ISSN 2072-8670 (Print) **НАУКА І ПРАВООХОРОНА**
NAUKA I PRAVOOKHORONA
DOI (Issue): https://doi.org/10.36486/np.2024.1(63) **Issue 1(63) 2024**

УДК 343.85:004-053.6

Лубенець Ірина Григорівна,
кандидат юридичних наук, старший дослідник, провідний науковий співробітник ДНДІ МВС України, м. Київ, Україна,
ORCID ID 0000-0003-2597-0356

ЗАГАЛЬНОСОЦІАЛЬНІ ЗАХОДИ ЗАПОБІГАННЯ ПРАВОПОРУШЕННЯМ СТОСОВНО ДІТЕЙ У ЦИФРОВОМУ СЕРЕДОВИЩІ

У статті розглянуто загальносоціальні заходи запобігання правопорушенням стосовно дітей у цифровому середовищі як узгоджену систему інформаційно-просвітницького, організаційно-технічного, соціального, правового, управлінського, виховного характеру, реалізація яких сприятиме зменшенню, нівелюванню, нейтралізації дії детермінант цих правопорушень. Такий широкий спектр дій спрямований на захист та забезпечення безпеки дітей в онлайн-середовищі.

Ключові слова: *безпека, діти, загроза, заходи запобігання, Інтернет, соцмережа, цифрове середовище.*

Невпинний процес еволюції у галузі цифрових технологій вплинув майже на всі сфери життя суспільства, надавши людству безліч можливостей для розвитку творчих здібностей, ведення бізнесу, розвитку медицини, трансформації науки, освіти, комунікації тощо. На тлі таких глобальних «цифрових перетворень» кількість інтернет-користувачів постійно зростає [1] (що підтверджується міжнародною статистикою), особливо за рахунок дітей, які є найактивнішими юзерами.

При всіх перевагах та позитивних рисах розвитку інформаційно-комунікаційних технологій, слід звернути увагу й на наявність негативної складової, зокрема, небезпек і загроз, що чатують на користувачів (особливо неповнолітніх) у цифровому середовищі. Необхідно відзначити, що суцільна цифровізація вплинула й на механізм скоєння окремих кримінальних правопорушень, зокрема, це стосується розповсюдження порнографії, збуту наркотичних чи заборонених в обігу товарів, розбещення, шахрайства, крадіжки коштів у Інтернеті тощо. Також з'явились нові склади кримінальних правопорушень, наприклад, домагання дитини для сексуальних цілей з використанням інформаційно-комунікаційних систем або технологій. Небезпечність криється в тому, що більшість правопорушень відносно дітей в цифровому середовищі залишаються поза увагою правоохоронних органів, що також підтверджується зарубіжними дослідженнями, зокрема, це відмічається у роботі пакистанських учених Pasha S.A., Ali S., Jeljeli R. «Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan» [2]. Отже, така трансформація правопорушень та їх висока латентність потребує ефективних заходів запобігання з метою забезпечення безпеки дитини в цифровому середовищі.

Необхідно зазначити, що питання запобігання правопорушенням у кіберпросторі та використання Інтернет-технологій для запобігання злочинності вивчали В.О. Біляєв та В.В. Клюс [3], Н.М. Гузела та М.В. Гузела [4], В.С. Березняк [5], S.A. Pasha, S. Ali, R. Jeljeli [2], M. Dorasamy [6] та ін. Особливо слід відзначити докторську дисертацію О.І. Бугери «Кримінологічні засади використання мережі Інтернет для запобігання злочинності» [7], у якій сформовано теоретичні аспекти використання Інтернет-технологій, моніторингу соціальних Інтернет-мереж, картографування кримінологічно значимої інформації для запобігання злочинності.

Проблему безпечного користування сучасними інформаційно-комунікаційними технологіями досліджували А.В. Пазюк [8], О.О. Черних [9], М.А. Снітко [10], О.А. Удалова [11], О.В. Швед, М.В. Євсюкова, О.В. Кузнецова, С.В. Колесникова, L. Dedkova та V. Mylek [12].

Питанню правового регулювання захисту дітей та запобіганню негативному впливу Інтернету присвятили свої роботи Н.В. Лесько [13], І.І. Припхан та І.І. Артемович [14], А.Ю. Нашинець-Наумова [15], К.Д. Кулик [16], С.О. Книженко [17], A. AlShabibi та M. Al-Suqri [18] та ін.

Попри значну кількість публікацій, присвячених різним аспектам безпеки в онлайн-середовищі, залишається актуальною потреба у науковому дослідженні шляхів попередження правопорушень стосовно дітей у цифровому середовищі, пошуку та удосконаленні заходів запобігання з метою усунення, нейтралізації, блокування їх детермінант.

На підставі вивчення вітчизняних та зарубіжних наукових джерел, нормативно-правової бази із вказаної тематики, аналізу результатів опитування учнів закладів загальної середньої освіти у м. Києві та Київській області[1] та з метою підвищення ефективності запобігання правопорушенням стосовно дітей у цифровому середовищі пропонується такий комплекс загальносоціальних заходів запобігання:

1. Підвищення рівня обізнаності дітей щодо навичок безпечної поведінки, можливих онлайн-загроз та їх наслідків у цифровому середовищі шляхом запровадження єдиного курсу з цифрової безпеки в межах навчальних програм школярів відповідно віку.

Проблема безпеки дитини в цифровому середовищі в останні десятиліття набуває все більшої актуальності. За цей час було напрацьовано чимало корисних матеріалів, розташованих на різних платформах, орієнтованих на певну цільову аудиторію – інтернет-користувачів загалом, дітей відповідного віку, батьків, вчителів тощо. Але вони часто мали фрагментарний характер, висвітлювали лише окремі аспекти онлайн-загроз. У результаті навчання школярів цифровій безпеці мало епізодичний та безсистемний характер, що не може забезпечити формування у них адекватного розуміння загроз, які їх очікують у цифровому середовищі, та вироблення навичок безпечної поведінки у ньому.

[1] Опитування було проведено фахівцями Державного науково-дослідного інституту МВС України у 2023 р. Генеральна сукупність – учні середніх шкіл м. Києва та Київської області віком від 11 до 17 років. Об'єм вибірки – 925 осіб. Серед проанкетованих – 364 (39,4 %) хлопців і 561 (60,6 %) дівчат.

Тому постає необхідність у запровадженні єдиного курсу з цифрової безпеки в межах навчальних програм школярів. Етапами реалізації цієї пропозиції мають бути:

1) розробка змісту курсу – визначення ключових тем, що слід включити до курсу (від створення складних паролів та основ медіаграмотності до уникнення кібербулінгу та переліку контактів, куди можна звернутися по допомогу у разі зіткнення з небезпеками в Інтернеті тощо) з періодичним їх оновленням відповідно до тенденцій розвитку цифрового середовища та виникнення нових онлайн-загроз;

2) адаптація курсу до інтернет-користувачів певного віку, тобто розроблення його різних версій для відповідних вікових груп (класів);

3) обов'язкове запровадження практичних занять, які дозволять дітям застосовувати набуті навички в конкретних ситуаціях та виявити прогалини у засвоєнні матеріалу;

4) залучення до проведення занять з окремих тем працівників Національної поліції (зокрема, кіберполіції, ювенальної превенції) з метою запобігання найбільш поширеним видам правопорушень у цифровому середовищі стосовно дітей та/або за їх участю з наведенням прикладів із практичної діяльності, обговоренням конкретних проблемних ситуацій та моделюванням відповідного алгоритму дій щодо того, як не стати жертвою посягань взагалі або як вийти зі «злочинної пастки». Для підвищення правової культури підлітків доцільно під час таких занять ознайомлювати їх із новелами законодавства у сфері відповідальності за правопорушення в цифровому середовищі.

Під час проведеного опитування школярів про необхідність упровадження таких практичних занять за участю працівників поліції заявили 60,2 % респондентів.

На користь такої взаємодії навчальних закладів із підрозділами поліції свідчить також позитивний зарубіжний досвід. Зокрема, з метою підвищення обізнаності школярів із приводу небезпек в Інтернеті у 38 департаментах Франції силами жандармерії проводяться спеціальні уроки для учнів останніх класів початкової школи (9–11 років). Їх мета – попередити молоде покоління про небезпеку мережі Інтернет. Упродовж 45 хвилин учням розповідають про те, що їх можуть примушувати до сексуальних зв'язків, зазивати в секти, підштовхувати до самогубств, показують відеоролики зі свідченнями однолітків – жертв агресії в Інтернеті. Наприкінці циклу таких уроків школярам пропонують скласти іспит на володіння правилами поведінки в мережі та видають Інтернет-посвідчення за аналогією до водійських прав [19].

Для забезпечення безпеки дитини в цифровому середовищі необхідно, щоб навчання дітей правилам безпечної поведінки в цифровому середовищі мало комплексний характер і відбувалось безперервно та систематично з обов'язковим відпрацюванням здобутих навичок на практиці.

Про необхідність запровадження комплексних широкомасштабних освітніх програм для дітей щодо кібербезпеки згадується у дослідженні AlShabibi A. та Al-Suqri M. «Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace» [18], де підкреслюється значний вплив поінформованості дітей щодо заходів безпеки у кіберпросторі на зменшення уразливості до онлайн-загроз. Автори наголошують, що обізнаність дітей у цій сфері є невід'ємною складовою захищеності дитини в онлайн-просторі.

2. Розроблення у навчальних закладах правил цифрової безпеки, затверджених установчими документами закладу освіти (статутом).

Окрім прав та обов'язків, визначених ст. 53 Закону України «Про освіту» [20], учні також можуть мати інші права та обов'язки, передбачені законодавством та установчими документами закладу освіти (ч. 1 ст. 20 Закону України «Про повну загальну середню освіту» [21]).

Установчими документами закладу загальної середньої освіти є рішення засновника (засновників) про його утворення та статут (ч. 1 ст. 33 Закону України «Про повну загальну середню освіту»). У цій же статті зазначається, що статут може містити інші положення з питань, що не врегульовані законодавством. Тому вважаємо за доцільне рекомендувати закладам освіти розробити правила цифрової безпеки як складової статуту навчального закладу.

Зміст та наповнення таких правил, що не суперечать чинному вітчизняному законодавству, визначатиме на свій розсуд навчальний заклад. Рекомендовано, щоб у правилах цифрової безпеки були окреслені:

вимоги (заборони) щодо користування мобільними пристроями у навчальному закладі;

вимоги (заборони) щодо проведення фото-/відеозйомок учасників освітнього процесу із зазначенням необхідності отримання згоди, зокрема, батьків, опікунів учнів, самих учнів, учителів, інших учасників освітнього процесу;

інші правила, спрямовані на запобігання кібербулінгу та порушенню прав учасників освітнього процесу під час використання цифрових засобів.

Вважається доцільним розробити також порядок реагування на інциденти, що виникають під час освітнього процесу та пов'язані з безпекою дітей, зокрема, у цифровому середовищі. Також з метою формування цілісного уявлення про наявні у навчальному закладі проблеми та тенденції, що вимагають уваги та втручання, необхідне впровадження процедури контролю та моніторингу порушень та інцидентів, пов'язаних із цифровою безпекою.

3. Доповнення системи оцінювання роботи закладів загальної середньої освіти показниками, які характеризують рівень роботи, спрямованої на забезпечення цифрової безпеки, а також встановлення переліку заохочень за успіхи в цій діяльності.

На наше переконання, таке заохочення в навчальних закладах стимулювало б розвиток ініціатив у межах школи з удосконалення виховного та організаційного процесу у сфері забезпечення цифрової безпеки учасників освітнього процесу, а також активізації роботи, що стосується обміну знаннями та найкращим досвідом з іншими навчальними закладами, органами, організаціями та установами з метою підвищення цифрових компетентностей вчителів, учнів і батьків.

4. Використання технічних засобів та новітніх технологій для створення безпечного середовища для дітей.

Забезпечення обов'язкової фільтрації шкідливого контенту в навчальних закладах та на комп'ютерах загального користування у позашкільних закладах, бібліотеках тощо.

Подібний досвід успішно реалізується за кордоном. Зокрема у США Закон «Про захист дітей в Інтернеті» (The Children's Internet Protection Act 2000 – CIPA [22]) зобов'язує школи та публічні бібліотеки, що отримують фінансування з федерального бюджету, при наданні дітям доступу до Інтернету встановлювати фільтри чи відповідне блокуюче програмне забезпечення.

Реалізація цього заходу може бути здійснена на рівні провайдера або шляхом встановлення на цифрові засоби, якими користуються учні в межах навчальної програми, відповідного програмного забезпечення для блокування доступу до небажаної інформації (контенту).

Популяризація встановлення на ґаджети, якими користується неповнолітній, програми «батьківський контроль».

За допомогою такого програмного забезпечення батьки можуть:

налагодити контент-фільтр, який блокуватиме доступ до шкідливого Інтернет-контенту;

встановити часові обмеження використання дітьми Інтернету;

відстежити місцезнаходження та активність пристрою за допомогою моніторингу геолокації.

Необхідно зазначити, що на ринку послуг є багато програм із зазначеними вище функціями, зокрема, ChildWebGuardianPro, Teentor, KidsControl, TimeBoss, «КіберМама» тощо. У браузерах також існують вбудовані інструменти для блокування шкідливого контенту. Наприклад, у Chrome та Opera це функція Adult Blocker, у Google можна активувати «Безпечний пошук». Ці сервіси проводять аналіз вебсторінок на наявність потенційно шкідливих слів та виразів і за необхідності блокують їх. У браузері Mozilla Firefox теж є кнопка «батьківського контролю», але в цьому браузері пропонуються додаткові інструменти, зокрема додатки Glubble for Families (надає доступ лише до сайтів, які дозволені батьками) та ProCon Latte (блокує сайти, які вносяться до чорного списку).

Періодичні перевірки налаштування профілю дитини в соцмережах, переконання її у необхідності зробити профіль закритим (приватним).

За результатами опитування переважна більшість дітей (88,9 %) уміють змінювати налаштування приватності профілю в соцмережах, але лише 34,6 % мають закритий профіль. Така легковажність з боку неповнолітніх інтернет-користувачів підвищує їх уразливість до онлайн-загроз особливо під час війни. Тому батькам необхідно контролювати налаштування приватності у соцмережах, де зареєстровані їхні діти. Зі свого боку вчителі під час навчально-виховного процесу (а батьки вдома) мають обговорювати з дітьми доцільність такого налаштування, а також можливі загрози, з якими діти можуть зіштовхнутись, у разі ігнорування елементарних заходів безпеки.

Контроль «маршруту» дітей у віртуальному просторі. Як свідчать результати опитування, більшість батьків не знають, чим діти займаються в Інтернеті. Перевірити, які сайти відвідувала дитина в Інтернеті, можна так: у браузері (правому верхньому кутку сторінки) потрібно натиснути на три крапки, після чого обрати рядок «Історія». Або ж можна скористатися комбінацією клавіш Ctrl+H.

Також ефективним засобом контролю підлітків, наприклад, у соцмережах, є використання хештегів. Хештег – це слово або група слів, перед якими стоїть знак решітки (#), який використовується для категоризації та пошуку розмов з певної теми. Хештег – це посилання на групу повідомлень, що використовує той же хештег.

Але слід пам'ятати, що діти, особливо підліткового віку, в питаннях новітніх технологій дуже розвинені та часто на крок попереду дорослих. Завдяки високому рівню цифрової компетентності нерідко школярі вміють відключати або змінювати зазначені функції контролю.

Для реалізації вказаних попереджувальних заходів необхідно створити систему постійного інформування батьків щодо зазначених та інших способів контролю за поведінкою дітей в Інтернеті. Ця функція може бути покладена на адміністрацію закладів навчального та просвітницько-розважального характеру, провайдерів Інтернет-послуг, продавців сучасних цифрових ґаджетів тощо.

5. Запровадження практики проведення інформаційної роз'яснювальної кампанії щодо новітніх способів скоєння протиправних діянь у цифровому середовищі та методів захисту від них, а також процедури звернення до правоохоронних органів.

У зв'язку з розвитком Інтернет-технологій та чи не щоденною появою нових викликів, пов'язаних з їх використанням, зокрема під час війни, постає необхідність у регулярному інформуванні користувачів на різних платформах (через ЗМІ, Інтернет тощо) про новітні небезпеки в цифровому середовищі: шахрайські «схеми»; методи соціальної інженерії, які часто використовуються кібершахраями; вірусні атаки, які поширюються е-поштою; ризики спілкування в соціальних мережах, зокрема, потрапляння до «груп смерті»; втягнення в злочинну діяльність, особливо під час війни тощо. Подібні інформаційні кампанії як з боку державних органів, так і недержавних організацій, проведення навчання, спрямованого на розширення свідомості інтернет-користувачів у згаданій сфері, є ключовими для підвищення безпеки в цифровому середовищі.

Одночасно необхідно проводити роз'яснювальну кампанію щодо дій громадян у разі, коли вони стикаються із кіберправопорушеннями. З цією метою, на наше переконання, доцільно залучати до співпраці операторів мобільного зв'язку, що дало б змогу поширювати через смс-повідомлення контакти (телефони «гарячих ліній», відповідні інтернет-адреси тощо), за якими діти або їх батьки чи особи, які їх замінюють, можуть звернутись по допомогу у разі зіткнення з інтернет-загрозами, отримати психологічну підтримку тощо.

Слід зазначити, що соціальні мережі сьогодні не тільки є засобом спілкування між людьми, а й самооновлюваною базою особистих даних, так як користувачі щоденно публікують особисту інформацію про себе та своїх рідних, рідко замислюючись про небезпеки та ризики, які виникають при цьому. На окрему увагу заслуговує питання щодо публікацій фотографій дітей. У середньому п'ятирічна дитина має близько 1 500 фотографій [23]. Такі дії порушують право дитини на приватність, а також створюють серйозну загрозу використання зазначених фото у протиправних цілях, таких як зловживання особистими даними, шахрайства та навіть використання дитячих фото для створення порноконтенту.

У якості заходу захисту від загроз у цифровому середовищі, на нашу думку, доцільно поширювати в ЗМІ, Інтернеті, у шкільних чатах, сайтах навчальних закладів, на батьківських зборах та класних годинах тощо рекомендації щодо безпечної поведінки в Інтернеті за кількома напрямами: 1) рекомендації щодо збереження персональних даних; 2) рекомендації для батьків (вчителів), що допоможуть уберегти дітей від Інтернет-загроз; 3) рекомендації для дітей, що допоможуть не стати жертвою протиправних діянь тощо.

6. Підвищення рівня взаємодії сім'ї та школи.

Налагодження партнерства між батьками та навчальними закладами з метою спільного виховання та навчання дітей толерантній комунікації, критичному мисленню, безпечній поведінці, у тому числі в цифровому середовищі.

Сім'я та школа – це два суспільних інститути, на які покладено обов'язок виховувати особистість. Сьогодні ситуація складається так, що кожен з них перекладає відповідальність за недоліки виховання та навчання один на одного: вчителі – на батьків, батьки – на вчителів. Однак досвід людства показує, що лише спільні зусилля сім'ї та школи можуть дати позитивні результати. При цьому має зберігатись пріоритетна роль сім'ї у вихованні та розвитку дитини, оскільки фундамент соціалізації та моральних якостей закладається саме в родині. І виховання навичок безпечного поводження в цифровому середовищі не має бути виключенням. Відповідно до дослідження чеських учених, батьківська участь у такому вихованні є невід'ємною частиною у процесі забезпечення безпеки дитини. Так зване, «батьківське онлайн-посередництво» є специфічною практикою виховання дітей, яка спрямована на максимізацію онлайн-можливостей і мінімізацію онлайн-ризиків, що забезпечується шляхом контролю та активною взаємодією дітей та батьків [12].

Однак нерідко батькам не вистачає відповідних знань у згаданій сфері, тому їм складно оцінити наявний рівень онлайн-загроз для дитини, а також запропонувати допомогу у разі необхідності та навчити безпечній поведінці в Інтернеті. Отже, батькам необхідно постійно підвищувати свій рівень цифрових компетентностей. Підтвердженням цьому є робота Dorasamy M., Kaliannan M., Jambulingam M., Ramadhan I., Sivaji A. «Parents' Awareness on Online Predators: Cyber Grooming Deterrence» [6], де зазначається, що «темний бік» Інтернету та соціальних мереж можна зменшити шляхом підвищення обізнаності та знань батьків про методи захисту та кібербезпеку.

З метою підвищення рівня цифрових компетентностей батьків, на наш погляд, є сенс у розробленні на базі сайтів навчальних закладів сторінки для батьків, де будуть розміщені рекомендації щодо способів контролю за поведінкою дітей в Інтернеті, запропоновано перелік ознак комп'ютерної залежності, предсуїцидальної поведінки та поведінки, характерної для жертв сексуального насильства, переслідування, цькування тощо, а також рекомендовано способи запобігання таким явищам і поради. Вважається за доцільне створити можливість дистанційного консультування батьків шкільним психологом.

Також необхідним є проведення роз'яснювальної роботи серед батьків під час батьківських зборів офлайн або онлайн з таких питань, як: «Що таке ґрумінг,

секстинг»; «Як запобігти правопорушенню відносно дитини в цифровому середовищі»; «Як розпізнати, що дитина стала жертвою певних правопорушень» тощо. З метою підвищення ефективності таких профілактичних бесід бажано запрошувати працівників ювенальної превенції та кіберполіції.

Основними складовими успішного педагогічного партнерства для забезпечення безпеки дитини, у тому числі в цифровому середовищі, є спілкування, взаємодія та співпраця між учителями, учнями, батьками та правоохоронцями.

Організація та проведення тижнів кібергігієни та медіаграмотності у навчальних закладах.

У межах проведення подібних тижнів можна залучати представників ІТ-компаній для інформування про нові засоби (програми, цифрові пристрої тощо) захисту ґаджетів від вірусних атак, способи фільтрації небажаного контенту, засоби захисту персональних даних тощо. За бажанням навчального закладу можливе проведення факультативних уроків, до яких батьки можуть підключатись дистанційно.

7. Підвищення ефективності суспільно-державного партнерства у сфері захисту користувачів від онлайн-загроз.

Взаємоінформування та співпраця між користувачами та провайдерами, а також сервісними службами хостингів, соцмереж, чатів тощо з метою зменшення кількості шкідливого контенту.

У зв'язку із значною поширеністю шкідливого контенту в мережі Інтернет постає необхідність у взаємоінформуванні користувачів і сервісних служб таких хостингів, як YouTube (Vimeo, Dailymotion, Smotri, Corbina.tv, Music.ivi тощо), Instagram, Tik-Tok тощо щодо виявленого шкідливого контенту (дописів чи коментарів) з метою його видалення.

Наприклад, якщо користувач у YouTube виявив будь-який шкідливий контент, то необхідно повідомити про це, натиснувши на три крапки під відео, а потім «Поскаржитись» й обрати відповідну категорію – «контент сексуального характеру», «шкідливі або небезпечні дії», «жорстоке поводження з дітьми», «пропаганда тероризму» тощо. Як стверджують розробники YouTube, відео буде видалено протягом 24 годин після того, як на нього поскаржаться. Також можливо поскаржитись на канал або користувача, обліковий запис якого може бути видалений.

Для подачі скарги в Instagram, Tik-Tok пропонується заповнити відповідні форми для подачі скарги. Чим більше інтернет-користувачі подають скарг, тим менше буде шкідливого контенту в Мережі. Тому батьками та вчителям обов'язково необхідно навчити дітей подавати відповідні скарги.

Провайдери мають максимально відповідально ставитись до змісту пакетів програмних послуг і не допускати розповсюдження в них суспільно небезпечної інформації, поширення якої визнається кримінальним правопорушенням згідно з кримінальним законодавством [24], зокрема, статтями 300, 301 Кримінального кодексу України [25].

У разі нереагування на вказані скарги користувача, останній має право звернутись із відповідним повідомленням до кіберполіції.

Запровадження громадського контролю за поширенням заборонених в обігу товарів (всі види наркотиків, зброї, кіно- та відеопродукції, комп'ютерних програм порнографічного характеру тощо) в мережі Інтернет, а також створення умов для активної участі громадськості у добровільному інформуванні правоохоронних органів про відомі їм випадки протиправних діянь у цифровому середовищі.

У період глобалізації та розвитку новітніх технологій світовий ринок змінюється, особливо це стосується заборонених у обігу товарів. Зокрема, наркотичні засоби зараз активно поширюються за допомогою Інтернету, через Мережу організовуються їх поставки, а за допомогою «закладок» вони розповсюджуються серед споживачів. Тобто сьогодні діє альтернативний, електронний ринок розповсюдження наркотиків. Було б доцільно заохочувати створення громадських груп, наприклад, журналістів, для моніторингу сайтів, соцмереж, блогів, чатів тощо з метою виявлення осіб, які пропонують наркотики чи інші заборонені товари або контент із подальшим повідомленням правоохоронних органів, зокрема, кіберполіції.

На сьогодні з метою виявлення таких фактів створені чат-боти (зокрема, «Стоп-наркотик»), за допомогою яких можна повідомити інформацію про поширення наркотиків за системою «закладок» та адрес, де розміщують інтернет-точки з продажем заборонених речовин з метою швидкого реагування. На нашу думку, для підвищення ефективності добровільного повідомлення про подібні правопорушення свідків необхідно заохочувати, наприклад, шляхом матеріальної винагороди або оформлення пільгового пакету інтернет-послуг чи абонементу у фітнес-клуб тощо. Для цього необхідно налагоджувати тісну взаємодію на взаємовигідних умовах між органами Національної поліції та підприємствами, організаціями, установами, що надають послуги населенню, і можуть погодитись бути спонсорами такого заходу.

Заохочення молоді до участі у виявленні та повідомленні правопорушень стосовно дітей у цифровому середовищі.

Сьогодні молодь значно краще володіє цифровими компетентностями, ніж дорослі, що підтверджено не тільки нашим опитуванням, а й іншими дослідженнями. Тому вважаємо за доцільне заохочувати найбільш талановитих, активних молодих людей, які пробують свої вміння у сфері цифрових технологій (зламуючи паролі, профілі, додаючись до закритих чатів тощо) до інформування відповідних органів у разі виявлення фактів протиправної діяльності стосовно дітей у Мережі або у разі встановлення певних уразливостей у захисті операційних систем тощо. Способи заохочення у разі успішної співпраці можуть бути різними.

Цифрове середовище – унікальний простір, якому немає аналогів у реальному світі. Це невід'ємна частина нашого повсякденного життя, оскільки виконує освітню, пізнавальну, інформаційну, розважальну, комунікаційну функції, долаючи географічні перешкоди. Тому діти проводять в Інтернеті все більше часу. Водночас, окрім позитивних сторін, віртуальне середовище приховує безліч ризиків і загроз для інтернет-користувачів, особливо неповнолітніх.

Тому розроблення та удосконалення заходів запобігання протиправним діянням стосовно дітей у цифровому середовищі є невід'ємною складовою існування безпечного

та захищеного онлайн-середовища для дітей, де вони можуть вільно користуватися Інтернетом, маючи мінімальні ризики стати жертвами протиправних діянь.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Internet World Stats. World internet usage and population statistics 2023 year estimates. URL: https://www.internetworldstats.com/stats.htm (дата звернення: 22.03.2024).

2. *Pasha S.A., Ali S., Jeljeli R.* Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan. *Human Arenas*, 2022. DOI 10.1007/s42087-022-00312-8.

3. *Біляєв В.О., Клюс В.В.* Перспективи використання Internet-технологій під час протидії екстремістським організаціям. Використання інноваційних технологій у попередженні злочинів: матеріали наук.-практ. семінару (м. Харків, 06 груд. 2012 р.) / МВС України, Харківський нац. ун-т внутрішніх справ. Харків: ХНУВС, 2012. С. 17–20.

4. *Гузела Н.М., Гузела М.В*. Проблема запобігання кримінальним правопорушенням в інформаційній сфері. *Вісник Національного університету «Львівська політехніка».* Серія: Юридичні науки. 2019. № 24. С. 139–143.

5. *Березняк В.С.* Запобігання шахрайству в Інтернеті. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2023. № 1. С. 190–196. DOI: 10.31733/2078-3566-2023-1-190-196.

6. *Dorasamy M., Kaliannan M., Jambulingam M. and other.* Parents' Awareness on Online Predators: Cyber Grooming Deterrence. *Qualitative Report.* 2021. Vol.26. Issue 11. P. 3683-3723. DOI 10.46743/2160-3715/2021.4914.

7. *Бугера О.І.* Кримінологічні засади використання мережі Інтернет для запобігання злочинності : автореф. дис. ... д-ра юрид. наук : 12.00.08. Київ, 2020. 36 с.

8. *Пазюк А.В.* Міжнародне інформаційне право: теорія і практика: моногр. Дніпропетровськ: Середняк Т. К., 2015. 447 с.

9. *Пазюк А.В., Черних О.О.* Дитина онлайн: як забезпечити безпеку і приватність (аналітичне дослідження). К.: ВАІТЕ, 2016. 74 с.

10. *Снітко М.А.* Соціально-педагогічні умови формування у підлітків безпечної поведінки в інтернет-мережі: автореф дис. ... канд. пед. наук. К., 2017. 22 с.

11. *Удалова О.А., Швед О.В., Євсюкова М.В. та ін.* Безпечне користування сучасними інформаційно-комунікативними технологіями: метод. рекомендації. К.: Україна, 2010. 72 с.

12. *Dedkova L., Mylek V.* Parental mediation of online interactions and its relation to adolescents' contacts with new people online: the role of risk perception. *Information Communication & Society.* 2023. Vol. 26. P. 3181-3198. DOI 10.1080/1369118X.2022.2146985.

13. *Лесько Н.В.* Правове регулювання захисту дітей від негативного впливу інтернету. 2017. URL: http://surl.li/svhxy (дата звернення: 22.03.2024).

14. *Припхан І.І., Артемович І.І.* Правовий механізм захисту неповнолітніх від негативного впливу інформації в мережі Інтернет. *Науковий вісник Ужгородського національного університету.* 2014, Серія «Право». Вип. 24. Т. 3, С. 104–108.

15. *Нашинець-Наумова А.Ю.* Інформаційна безпека: питання правового регулювання: монографія. Київ: Видавничий дім «Гельветика», 2017. 168 с.

16. *Кулик К.Д.* Запобігання розбещенню неповнолітніх з використанням мережі Інтернет. Міжнародні стандарти з кібербезпеки та їх застосування в Україні. 2016. Харків: Право, С. 72–75. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.nlu.edu.ua/jspui/bitstream/123456789/12138/1/Kulik_72-75.pdf (дата звернення: 22.03.2024).

17. *Книженко С.О.* Криміналістична характеристика створення та поширення контенту з вмістом дитячої порнографії з використанням інформаційно-телекомунікаційних систем або технологій. *Аналітично-порівняльне правознавство.* 2022. № 3. С. 227–231. DOI: https://doi.org/10.24144/2788-6018.2022.03.41.

18. *AlShabibi A., Al-Suqri M.* Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace. IEEE. 2021. 22nd International Arab Conference On Information Technology (ACIT). Muscat, Oman (Dec 21-23, 2021). P. 388-393. DOI 10.1109/ACIT53391.2021.9677117.

19. *Polevaya O., Boyer F.* L'école française face à ses problèmes. 2013. URL: http://rusoch.fr/fr/politique/problemy-francuzskoj-shkoly.html (дата звернення: 22.03.2024).

20. Про освіту: Закон України від 05.09.2017 № 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 22.03.2024).

21. Про повну загальну освіту: Закон України від 16.01.2020 № 463-IX.URL: https://zakon.rada.gov.ua/laws/show/463-20#Text (дата звернення: 22.03.2024).

22. The Children's Internet Protection Act 2000 (CIPA). URL: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act (дата звернення: 22.03.2024).

23. *Пилипів І.* Хочете зіпсувати майбутнє дитини? Публікуйте її фото в соцмережах. Як злочинці за допомогою ШІ руйнують життя. *Економічна правда.* 2023. URL: https://www.epravda.com.ua/publications/2023/08/10/703102/ (дата звернення: 22.03.2024).

24. Про розповсюдження в багатоканальних телемережах України програм іноземних мовників, які містять пропаганду війни, насильства, жорстокості, розпалювання національної, міжетнічної ворожнечі тощо: рішення Комітету ВРУ з питань свободи слова та інформації від 12.03.2014, протокол № 27. URL: https://zakon.rada.gov.ua/rada/show/v0027450-14 (дата звернення: 22.03.2024).

25. Кримінальний кодекс України від 05.04.2001 № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 22.03.2024).

REFERENCES

1. Internet World Stats. World internet usage and population statistics 2023 year estimates. URL: https://www.internetworldstats.com/stats.htm. (Date of Application: 22.03.2024) [in English].

2. *Pasha, S.A., Ali, S., Jeljeli, R.* (2022). Artificial Intelligence Implementation to Counteract Cybercrimes Against Children in Pakistan. *Human Arenas.* DOI: https://doi.org/10.1007/s42087-022-00312-8. [in English].

3. *Biliaiev, V.O., Klius, V.V.* (2012). Perspektyvy vykorystannia Internet-tekhnolohii pid chas protydii ekstremistskym orhanizatsiiam. Vykorystannia innovatsiinykh tekhnolohii u poperedzhenni zlochyniv. "Prospects for the use of Internet technologies during countermeasures against extremist organizations. Innovative technologies in crime prevention: scientific and practical materials". Seminar (December 6, 2012) / Ministry of Internal Affairs of Ukraine, Kharkiv National University of Internal Affairs. Kharkiv: KhNUVS. P. 17–20 [in Ukrainian].

4. *Huzela, N.M., Huzela, M.V.* (2019). Problema zapobihannia kryminalnym pravoporushenniam v informatsiinii sferi. "The problem of preventing criminal offenses in the information sphere". *Bulletin of the Lviv Polytechnic National University.* Series: Legal sciences. [in Ukrainian].

5. *Berezniak, V.S.* (2023). Zapobihannia shakhraistvu v Interneti. "Preventing Internet Fraud". *Scientific Bulletin of the Dnipropetrovsk State University of Internal Affairs.* No. 1. P. 190–196. DOI: https://doi.org/10.31733/2078-3566-2023-1-190-196 [in Ukrainian].

6. *Dorasamy, M., Kaliannan, M., Jambulingam, M., Ramadhan, I. and Sivaji, A.* (2021). Parents' Awareness on Online Predators: Cyber Grooming Deterrence. *Qualitative Report.* Vol. 26. Iss. 11. P. 3683–3723. DOI: https://doi.org/10.46743/2160-3715/2021.4914 [in English].

7. *Buhera, O.I.* (2020). Kryminolohichni zasady vykorystannia merezhi Internet dlia zapobihannia zlochynnosti. "Criminological principles of using the Internet to prevent crime": extended abstract of Doctor's thesis. Kyiv. 36 p. [in Ukrainian].

8. *Paziuk, A.V.* (2015). Mizhnarodne informatsiine pravo: teoriia i praktyka. Dnipropetrovsk. International information law: theory and practice: monograph. Dnipropetrovsk: 'Seredniak T.K.'. 447 p. [in Ukrainian].

9. *Paziuk, A.V., Chernykh, O.O.* (2016). Dytyna onlain: yak zabezpechyty bezpeku i pryvatnist (analitychne doslidzhennia). "Child online: how to ensure safety and privacy (analytical study)". K.: VAITE. 74 p. [in Ukrainian].

10. *Snitko, M.A.* (2017). Sotsialno-pedahohichni umovy formuvannia u pidlitkiv bezpechnoi povedinky v internet-merezhi. "Socio-pedagogical conditions for the formation of safe behavior in the Internet network among teenagers": Candidate's thesis. K. 22 p. [in Ukrainian].

11. *Udalova, O.A., Shved, O.V., Yevsiukova, M.V., Kuznetsova, O.V. and Kolesnykova S.V.* (2010). Bezpechne korystuvannia suchasnymy inforamtsiino-komunikatyvnymy tekhnolohiiamy: metodychni rekomendatsii. "Safe use of modern information and communication technologies": method. recommendations. K.: Ukraine. 72 p. [in Ukrainian].

12. *Dedkova L., Mylek V.* (2023). Parental mediation of online interactions and its relation to adolescents' contacts with new people online: the role of risk perception. *Information Communication & Society.* Vol. 26. P. 3181–3198. DOI: https://doi.org/10.1080/1369118X.2022.2146985. [in English].

13. *Lesko, N.V.* (2017). Pravove rehuliuvannia zakhystu ditei vid nehatyvnoho vplyvu internetu. "Legal regulation of the protection of children from the negative influence of the Internet". URL: http://surl.li/svhxy. (Date of Application: 22.03.2024) [in Ukrainian].

14. *Prypkhan, I.I.,* Artemovych, I.I. (2014). Pravovyi mekhanizm zakhystu nepovnolitnikh vid nehatyvnoho vplyvu informatsii v merezhi Internet. "The legal mechanism for the protection of minors from the negative impact of information on the Internet". Scientific Bulletin of the Uzhhorod National University. Series "Law". Iss. 24. Vol. 3. P. 104–108 [in Ukrainian].

15. *Nashynets-Naumova, A.Yu.* (2017). Informatsiina bezpeka: pytannia pravovoho rehuliuvannia: monohrafiia. "Information security: issues of legal regulation": monograph. Kyiv: Helvetica Publishing House. 168 p. [in Ukrainian].

16. *Kulyk, K.D.* (2016). Zapobihannia rozbeshchenniu nepovnolitnikh z vykorystanniam merezhi Internet. "Prevention of corruption of minors using the Internet". International Cyber Security Standards and their Application in Ukraine. Kharkiv: Pravo. P. 72–75. URL: chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://dspace.nlu.edu.ua/jspui/bitstream/123456789/12138/1/Kulik_72-75.pdf. (Date of Application: 22.03.2024). [in Ukrainian].

17. *Knyzhenko, S.O.* (2022). Kryminalistychna kharakterystyka stvorennia ta poshyrennia kontentu z vmistom dytiachoi pornohrafii z vykorystanniam informatsiino-telekomunikatsiinykh system abo tekhnolohii. "Forensic characteristics of the creation and distribution of content containing child pornography using information and telecommunication systems or technologies". *Analytical and Comparative Jurisprudence.* No. 3. P. 227–231. DOI: https://doi.org/10.24144/2788-6018.2022.03.41 [in Ukrainian].

18. *AlShabibi, A., Al-Suqri, M.* (2021). Cybersecurity Awareness and Its Impact on Protecting Children in Cyberspace // IEEE. 22nd International Arab Conference On Information Technology (ACIT). Muscat, Oman (Dec. 21–23, 2021). P. 388–393. DOI: https://doi.org/10.1109/ACIT53391.2021.9677117 [in English].

19. *Polevaya, O., Boier, F.* (2013). L'école française face à ses problèmes. URL: http://rusoch.fr/fr/politique/problemy-francuzskoj-shkoly.html. (Date of Application: 22.03.2024) [in French].

20. Pro osvitu. "On education": Law of Ukraine dated September 5, 2017 No. 2145-VIII. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text. (Date of Application: 22.03.2024) [in Ukrainian].

21. Pro povnu zahalnu osvitu. "On comprehensive general education": Law of Ukraine dated January 16, 2020 No. 463-IX. URL: https://zakon.rada.gov.ua/laws/show/463-20#Text. (Date of Application: 22.03.2024) [in Ukrainian].

22. The Children's Internet Protection Act 2000 (CIPA). URL: https://www.fcc.gov/consumers/guides/childrens-internet-protection-act. (Date of Application: 22.03.2024) [in English].

23. *Pylypiv, I.* (2023). Khochete zipsuvaty maibutnie dytyny? Publikuite yii foto v sotsmerezhakh. Yak zlochyntsi za dopomohoiu ShI ruinuiut zhyttia. "Do you want to spoil the child's future? Post her photo on social networks. How criminals destroy lives with the help of AI". *Economic Truth.* URL: https://www.epravda.com.ua/publications/2023/08/10/703102/. (Date of Application: 22.03.2024) [in Ukrainian].

24. Pro rozpovsiudzhennia v bahatokanalnykh telemerezhakh Ukrainy prohram inozemnykh movnykiv, yaki mistiat propahandu viiny, nasylstva, zhorstokosti, rozpaliuvannia natsionalnoi, mizhetnichnoi vorozhnechi toshcho. "On the distribution in multi-channel TV networks of Ukraine of programs of foreign broadcasters that contain propaganda of war, violence, cruelty, incitement of national and inter-ethnic enmity, etc.": decision of the VRU Committee on Freedom of Speech and Information dated March 12, 2014. Protocol No. 27. URL: https://zakon.rada.gov.ua/rada/show/v0027450-14. (Date of Application: 22.03.2024) [in Ukrainian].

25. Kryminalnyi kodeks Ukrainy. "Criminal Code of Ukraine". URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text. (Date of Application: 22.03.2024) [in Ukrainian].

UDC 343.85:004-053.6

Lubenets Iryna,
Candidate of Juridical Sciences, Senior Researcher, Leading Researcher,
State Research Institute MIA Ukraine, Kyiv, Ukraine,
ORCID ID 0000-0003-2597-0356

GENERAL SOCIAL MEASURES TO PREVENT OFFENCES AGAINST CHILDREN IN THE DIGITAL ENVIRONMENT

The advent of the latest communication tools and the digital environment has had a profound impact on all aspects of social life, to the extent that it is challenging to envisage a world without them. Moreover, the number of individuals utilizing the Internet is consistently on the rise, particularly among children, who represent the most active users.

For the majority of children in the current generation, digital technology has become an indispensable aspect of their everyday lives. They spend a considerable amount of time engaged with digital devices, which they use to communicate access information, pursue educational activities and engage in social interactions, as well as for leisure purposes. Nevertheless, despite the extensive range of possibilities and advantages offered by the digital environment, it also presents certain risks and dangers, particularly for children due to their age-specific vulnerabilities. Consequently, efforts to prevent violations concerning children in the digital environment remain pertinent, and preventive measures require periodic updating and improvement.

The article discusses general social measures to prevent violations concerning children in the digital environment as a system of legal, organizational, technical, social, managerial, and educational measures aimed at eliminating, blocking, and mitigating determinants that lead to unlawful behavior concerning children in the online environment. The most effective preventive measures in this area are: raising children's awareness of safe behavior on the Internet, using technical means to protect children from online threats, ensuring close cooperation between

family and school, conducting informational and explanatory work among the population, and improving public-state partnership in the field of protecting Internet users (including minors) from threats in the digital environment.

The digital environment is a unique space that has no analogues in the real world. It is an integral part of our everyday life, performing a multitude of functions, including educational, cognitive, informational, entertainment, and communication. It overcomes geographical barriers. It is clear that children are spending more and more time on the Internet. However, the virtual environment also poses significant risks and threats to Internet users, especially minors.

The implementation of the aforementioned measures will serve to mitigate the vulnerability of children in the digital environment and to reduce the likelihood of their becoming victims of relevant violations.

Keywords: security, children, threat, preventive measures, Internet, social media, digital environment.

Отримано 03.04.2024