Державна наукова установа «Інститут інформації, безпеки і права
Національної академії правових наук України»

Інститут цифровізації освіти
Національної академії педагогічних наук України

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ: ВИКЛИКИ СЬОГОДЕННЯ

ЗБІРНИК МАТЕРІАЛІВ

Київ–2025

Рекомендовано до друку:

Вченою радою
Державної наукової установи «Інститут інформації, безпеки і права Національної академії правових наук України», протокол № 5 від 24.06.2025 р.

Вченою радою
Інституту цифровізації освіти Національної академії педагогічних наук України, протокол № 10 від 26.06.2025 р.

З-38 **Захист персональних даних дітей: виклики сьогодення** : збірник матеріалів / Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»; Інститут цифровізації освіти НАПН України // Упорядн.: О.Г. Радзієвська, С.О. Дорогих, Н.В. Сороко. Київ : ІЦО НАПН України. 2025. 93 с.

УДК 004.738.5:342.7-053.2(082)
ISBN 978-617-8330-54-5
DOI: 10.33407/lib.NAES.id/eprint/746007

У збірнику матеріалів науково-методичного семінару «Захист персональних даних дітей у цифрову епоху» (29 травня 2025 р., місто Київ) висвітлено актуальні теоретико-правові та прикладні проблеми становлення і розвитку інформаційного суспільства, захисту інформаційних прав, свобод і безпеки дитини, приватності її життя та персональних даних в контексті вимог законодавства Європейського Союзу та євроінтеграції України. Також розглянуто низку правових, етичних і технічних аспектів захисту персональних даних дітей у цифровому середовищі, формування навичок безпечного використання цифрових технологій у навчальному процесі, а також впровадження ефективних практик забезпечення інформаційної безпеки дітей в умовах цифровізації освіти.

Видання розраховане на фахівців, експертів і вчених, науково-педагогічних працівників, представників органів державної влади та місцевого самоврядування, приватного сектору і громадянського суспільства, а також здобувачів вищої освіти.

Тези доповідей подано в авторській редакції.

ЗМІСТ

РЕКОМЕНДАЦІЇ УЧАСНИКІВ СЕМІНАРУ

Сучасне інформаційне суспільство характеризується стрімким розвитком інформаційних (цифрових) технологій, формуванням глобального інформаційного простору та цифровізацією усіх сфер життєдіяльності людини, суспільства, держави та міжнародної спільноти. Поряд з іншими суспільними трансформаціями суттєвих змін також зазнає освітянська сфера. Використання цифрових освітніх платформ в умовах цифрової трансформації постає актуальною складовою педагогічної сфери. Цифрові технології невідворотно змінюють спосіб спілкування, навчання, пошуку інформації, вираження думок.

Проте, надто швидке впровадження новітніх технологій в освітню сферу породжує низку вкрай важливих безпекових питань для дітей, як учасників освітнього процесу. Під загрозою постають їхній морально-психологічний стан та персональні дані. Серед основних викликів фахівці зазначають складності адаптації учасників освітнього процесу до нових освітніх можливостей та проблеми соціалізації дитини в цифрову епоху. Зокрема, це стосується знеособлення комунікації, поширення мови ворожнечі, кібербулінгу, маніпуляції, порушення права на приватність та права на захист персональних даних.

Як свідчать результати опитувань, більшість педагогічних працівників і батьків не знайомі з вимогами «Пакету захисту даних» ЄС (GDPR) та національного законодавства щодо захисту персональних даних, у тому числі даних учнів. Водночас особи, на яких покладено обов’язок щодо захисту безпеки дітей, не завжди розуміють ризики, пов’язані зі збором та обробкою персональних даних дітей, зокрема: з якою метою вони збираються, які механізми захисту передбачені, якими є терміни обробки і збереження даних, які існують системи контролю за дотримання норм права щодо захисту персональних даних тощо.

Наприклад, функції контролю за дотриманням правових норм щодо захисту персональних даних покладено на Уповноваженого Верховної Ради України з прав людини. Однак на практиці ця інституція не завжди володіє достатніми ресурсами і повноваженнями для системного моніторингу освітніх практик, де задіяні персональні дані дітей. Крім цього, чинний Закон України «Про захист персональних даних» не містить окремих положень, присвячених захисту даних дітей на відміну від Регламенту ЄС 2016/679 (GDPR). В українському законодавстві наразі не визначено мінімальний вік надання згоди на обробку персональних даних, не передбачено механізмів та процедури надання згоди на обробку персональних даних в освітньому процесі, не врегульовано питання щодо безпечного використання дитячих IoT-пристроїв та інші проблемні аспекти ефективного захисту персональних даних дитини.

Питання захисту інформаційної безпеки та персональних даних дітей суттєво актуалізується в умовах глобального інформаційного протиборства та поширення інформаційної агресії і насилля рф проти України.

Науково-практичний семінар *«Захист персональних даних дітей у цифрову епоху»*, проведений Державною науковою установою «Інститут інформації, безпеки і права Національної академії правових наук України» та Інститутом цифровізації освіти Національної академії педагогічних наук України об’єднав вчених, експертів і фахівців навколо проблем захисту інформаційних прав, свобод та безпеки дитини, її приватності та захисту персональних даних у цифровому середовищі.

В ході всебічного обговорення учасники науково-практичного семінару констатували необхідність системних змін з питань забезпечення інформаційної безпеки дитини в умовах цифрової трансформації, а також розробки нових механізмів захисту персональних даних дітей, зокрема в освітньому процесі.

Важливим аспектом обговорення було підвищення рівня цифрової грамотності та інформаційної культури учасників освітнього процесу,

зокрема шляхом системного навчання педагогів, учнів і батьків основам інформаційної та кібернетичної безпеки, конфіденційності та етики онлайн-спілкування, превентивних заходів щодо захисту даних, програмно-технічних і правових механізмів захисту персональних даних.

Учасники науково-методичного семінару за результатами обговорення виокремили напрями подальшого наукового пошуку і запропонували низку прикладних ***рекомендацій щодо захисту персональних даних дітей***, зокрема:

– провести експертне оцінювання і внести зміни до чинного законодавства з питань захисту персональних даних дітей в контексті євроінтеграції України та прийняття нового Закону України «Про захист персональних даних»;

– врахувати особливості захисту персональних даних дітей при врегулюванні діяльності державних та приватних інституцій у сфері надання освітніх послуг, охорони здоров'я, соціальній, правовій та інших сферах, пов'язаних із взаємодією з дітьми;

– опрацювати державну інформаційну політику в частині розвитку ефективних комунікацій з дітьми та іншими учасниками освітнього-виховного процесу з урахуванням сучасних викликів і загроз в інформаційній сфері;

– напрацювати ефективні програми і методики формування та підвищення цифрової грамотності та інформаційної культури громадян;

– забезпечити впровадження у навчальні плани початкової, базової та старшої школи освітні заходи щодо підвищення медіаграмотності, цифрової безпеки та захисту персональних даних;

– запровадити постійне оновлення методичних рекомендацій та навчальних матеріалів з питань інформаційної безпеки для вчителів, батьків і учнів;

– організувати проведення просвітницьких заходів для дітей, батьків, вчителів та інших учасників освітнього середовища для підвищення

обізнаності щодо захисту персональних даних;

– розробити і впровадити у закладах освіти практичні завдання для учнів на основі моделювання ситуацій, які можуть виникнути в цифровому просторі при навчанні, спілкуванні, розвагах (витоку даних, фішингу, небажаного онлайн-втручання тощо) та відповідні рекомендації для усунення можливих загроз;

– запровадити регулярні інформаційні кампанії щодо ризиків, які можуть виникати у цифровому середовищі: булінг, зловживання даними, секстинг (обмін повідомленнями інтимного характеру, зокрема фото та відео, за допомогою мобільних телефонів, електронної пошти або соціальних мереж), шахрайство та ін.;

– включити питання кібербезпеки та інформаційної гігієни у цифрову епоху у процес державної сертифікації електронних ресурсів, що використовуються в освіті;

– забезпечити доступність інструментів «відкликання згоди» щодо доступу до персональних даних дітей молодшого віку та інших категорій;

– запровадити міждержавний обмін, зокрема в межах програм *Horizon Europe, Digital Europe, Better Internet for Kids* та ін., з питань подальшого розвитку наукових і практичних заходів щодо захисту персональних даних дітей.

МІЖНАРОДНІ ПІДХОДИ ДО ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ: СУЧАСНІ ВИКЛИКИ. Овчарук О.В.

доктор педагогічних наук, професор,
Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0001-7634-7922

Захист персональних даних дітей у цифрову епоху є однією з актуальних проблем у сфері інформаційної безпеки та прав людини. Діти становлять особливо вразливу категорію користувачів, персональні дані яких часто обробляються без належної правової основи, що створює ризики зловживання, дискримінації та порушення приватності. В Україні, попри наявність загального закону про захист персональних даних, відсутній спеціалізований правовий механізм, який би регулював питання приватності дітей.

Цифровізація освіти в Україні, зокрема масове використання електронних журналів, онлайн-платформ (Google Workspace for Education, Microsoft Teams, Classtime та ін.), часто не супроводжується належним аналізом ризиків для приватності дітей. Дані учнів (включно з академічною успішністю, поведінкою, медичною інформацією) збираються і зберігаються з мінімальними гарантіями захисту (Новосад, 2021) [12]. Крім того, існує практика вимушеного збору даних без усвідомленої згоди батьків, що прямо суперечить міжнародному принципу «інформованої згоди» (Council of Europe, 1981)[1].

За результатами опитувань, більшість педагогічних працівників не знайомі з вимогами GDPR або національного законодавства щодо обробки персональних даних, зокрема даних учнів (UNICEF, 2023)[13]. Те саме стосується і батьків, які не завжди розуміють, як і з якою метою збираються дані їхніх дітей, та які ризики це несе. Функції контролю в цій сфері покладено на Уповноваженого Верховної Ради з прав людини, однак на

практиці ця інституція не має належних ресурсів і повноважень для системного моніторингу освітніх практик, що зачіпають персональні дані дітей (Омбудсман, 2023) [11].

Участь глобальних технологічних компаній у наданні освітніх послуг в Україні (Google, Facebook, Zoom) не супроводжується прозорими угодами про обробку даних. Часто дані українських учнів передаються за межі країни без зрозумілої юрисдикції захисту, що суперечить принципу обмеженого транскордонного обміну (OECD, 2013) [10]. Школи та місцеві органи управління освітою не мають стандартів впровадження принципу «конфіденційності за замовчуванням», що передбачає технічну та організаційну інтеграцію захисту приватності на етапі розробки будь-якого освітнього сервісу (Cavoukian, 2011) [7].

Сьогодні на міжнародному рівні діють основні документи, які дотичні до захисту персональних даних, які поширюються на органи влади, організації, інституції та осіб. Для усвідомлення, що таке персональні дані, слід звернутись до законодавства, де зазначено, що персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (абзац 10 статті 2 Закону України «Про захист персональних даних») [14]. Захист персональних даних став однією з ключових тем правового регулювання в умовах цифрової трансформації суспільства. Закон України «Про захист персональних даних» (2010) не містить окремих положень, присвячених захисту даних дітей. На відміну від Регламенту ЄС 2016/679 (GDPR), в українському законодавстві не встановлено мінімального віку, з якого дитина може самостійно давати згоду на обробку своїх персональних даних, а також не передбачено жодних особливих заходів щодо згоди батьків або опікунів (GDPR, 2016, Art. 8; Закон України, 2010) [14]. Це свідчить про невідповідність національного регулювання міжнародним стандартам і знижує ефективність правового захисту неповнолітніх в цифровому середовищі (Смокович, 2021) [12].

Зростання обсягів обробки персональної інформації потребує

системного нормативного забезпечення, яке базується як на міжнародних, так і на національних актах. Це акти міжнародних структур, зокрема Організації Об'єднаних Націй, ОЕСР, Ради Європи, Європейського Союзу та ін.

До основоположних міжнародних документів, що закладають основу для регулювання процедур захисту персональних даних можемо віднести Керівні принципи регламентації комп'ютеризованих картотек, що містять дані особистого характеру, ухвалені Резолюцією Генеральної Асамблеї ООН № 45/95 від 14 грудня 1990 р. (United Nations, 1990) [5]. Цей документ став першим та вміщує принципи та вимоги законності, обмеження мети збору, точності, збереження та безпеки обробки.

У 1980 р. Організація з економічного співробітництва та розвитку (ОЕСР) прийняла Базові принципи захисту недоторканності приватного життя і транскордонних потоків персональних даних, оновлені у 2013 р. (OECD, 2013) [10]. Документ визначив вісім основоположних принципів, зокрема обмеження збору, відкритість, безпеку даних, підзвітність обробників. Конвенція № 108 Ради Європи «Про захист осіб у зв'язку з автоматизованою обробкою персональних даних» від 1981 року (Council of Europe, 1981) стала першим обов'язковим міжнародним договором у сфері приватності. Вона регламентує основні права суб'єкта даних, обмеження обробки, а також питання транскордонної передачі.

Захист персональних даних дітей у ЄС має особливе значення, цьому питанню приділяється значна увага. Директива 95/46/ЄС Європейського Парламенту і Ради від 24 жовтня 1995 р. (European Parliament and Council, 1995) встановила правову базу захисту персональних даних у межах Європейського Союзу. Вона запровадила вимоги до згоди суб'єкта, інституційного контролю, повідомлення про обробку даних. Згодом її замінив Загальний регламент про захист даних (GDPR), що діє з 2018 р. [9].

У межах Загального регламенту про захист даних (GDPR) захист дітей визнається пріоритетним через їхню особливу вразливість. Відповідно до

статті 8 GDPR, дитина має бути не молодшою за 16 років, щоб самостійно надати згоду на обробку персональних даних у цифрових сервісах. Однак держави-члени ЄС можуть знизити цю межу до 13 років [2; 3]. Для дітей молодшого віку згода має надаватися або схвалюватися законними представниками.

Окрему увагу приділено таким принципам, як прозорість (надання зрозумілої та доступної інформації), мінімізація обсягу зібраних даних, обмеження автоматизованого прийняття рішень, а також заборона профілювання в комерційних цілях. У контексті освітніх закладів GDPR встановлює обмеження на передачу даних третім сторонам, зокрема EdTech-компаніям, без належної правової підстави.

Європейський Союз також розробляє етичні рамки проектування цифрових продуктів для дітей, подібні до Children's Code у Великій Британії. Ці ініціативи мають на меті підвищення стандартів конфіденційності для дитячої аудиторії в онлайн-середовищі (European Commission, 2023) [2].

Отже, Україна потребує оновлення правового регулювання захисту персональних даних дітей у відповідності до європейських норм. Це включає ухвалення спеціального підзаконного акту щодо захисту приватності дітей, запровадження вікових меж надання згоди, підвищення цифрової грамотності педагогів, посилення державного нагляду та стимулювання принципу «privacy by design» у школах.

Список використаних джерел

1. Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108)*. https://www.coe.int/en/web/data-protection/convention108

2. European Commission. (2023). *Children and the GDPR*. https://ec.europa.eu/info/law/law-topic/data-protection_en

3. European Parliament and Council. (1995). *Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046

4. OECD. (2013). *The OECD Privacy Framework*. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

5. United Nations. (1990). *Guidelines for the Regulation of Computerized Personal Data Files*. https://digitallibrary.un.org/record/92046
6. Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.
7. Cavoukian, A. (2011). *Privacy by Design: The 7 Foundational Principles*. Information and Privacy Commissioner of Ontario. https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf
8. Council of Europe. (1981). *Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data* (ETS No. 108). https://www.coe.int/en/web/data-protection/convention108-and-protocol
9. European Union. (2016). *Regulation (EU) 2016/679 (General Data Protection Regulation)*. https://eur-lex.europa.eu/eli/reg/2016/679/oj
10. OECD. (2013). *The OECD Privacy Framework*. Organisation for Economic Co-operation and Development. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf
11. Омбудсман. (2023). *Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан дотримання прав людини і громадянина*. https://ombudsman.gov.ua/files/Reports/Dopovid2023.pdf
12. Смокович, О. (2021). Захист персональних даних дітей у цифровому середовищі: міжнародні стандарти та національні виклики. *Інформаційне право України*, 4(36). С. 45-52.
13. UNICEF. (2023). *Діти в цифровому середовищі: аналітичний огляд*. https://www.unicef.org/ukraine/media/20203/file/digital-report-children-ukraine.pdf
14. Закон України «Про захист персональних даних», №2297-VI від 01.06.2010. https://zakon.rada.gov.ua/laws/show/2297-17#Text

ЗНАННЯ - ОДНА ІЗ ОСНОВ ЕФЕКТИВНОСТІ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ У ЦИФРОВУ ЕПОХУ.

Фурашев В.М.

кандидат технічних наук, с.н.с., доцент
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0001-7205-724X

Людство існує у суцільному інформаційному просторі, в якому кожна жива істота є інформаційною системою – елементарною (простою) або більш розвинутою (складною) та одночасно є джерелом і користувачем інформації.

Найскладнішою інформаційною системою в сучасному світі є саме людина.

З давніх часів зусилля людини, племені, суспільства концентрувалися, з одного боку, на отриманні необхідної інформації у будь-який спосіб, а з іншого – на недопущенні витоку визначеної інформації. З розвитком людства, налагодженням комунікативно-комунікаційних зав'язків в центрі всіх цих процесів завжди знаходилась інформація.

У цьому є як позитив, так і негатив розвитку людини й усього суспільства. Найгірше те, що з розвитком живих істот, інформація починає впливати на людину на рівні не тільки свідомості, а й підсвідомості, тобто, попри її волі. Інформація починає здійснювати домінуючий вплив на свідомість, поведінку людини та, відповідно, на суспільство в цілому. Таким чином, людина формується під впливом того інформаційного середовища, в якому вона знаходиться з моменту народження. Це, одночасно й добре, й небезпечно, як для людини, так і для суспільства.

Природними властивостями інформації, на наш погляд, є її спроможність впливу на людину як на рівні свідомості, так і на рівні підсвідомості та *подвійність* - неоднозначність трактування.

Штучними властивостями інформації слід вважати:

переконливість - ступінь сприйняття у порівнянні з іншою;

цінність - ступінь задоволення потреби, бажання, інтересів соціального суб'єкта (індивіда, групи людей суспільства);

корисність - міра задоволення, що отримує індивід від споживання інформації;

повнота – а) віддзеркалення вичерпного характеру відповідності одержаних відомостей цілям збору; б) достатність для розуміння ситуації та прийняття рішення; в) характеристика, яка визначає кількість інформації необхідної та достатньої для прийняття вірного рішення;

вчасність – а) ознака того, що вона є саме тією, яка потрібна на даний момент; б) важливість, істотність у певний момент часу;

вірогідність – а) віддзеркалення дійсності (істинного стану справ); б)

достовірність (міра наближеності інформації до першоджерела або точність передачі інформації);

конфіденційність - властивість захищеності інформації від несанкціонованого доступу та спроб її розкриття користувачем, що не має відповідних повноважень;

цілісність - показник того, що дані повні та не були змінені при виконанні будь-якої операції над ними, будь то передача, зберігання або представлення;

доступність - здатність забезпечення, при необхідності, своєчасного безперешкодного доступу до інформації, що цікавить;

санкціонованість розповсюдження - процес надання інформації споживачам , в рамках обумовлених повноважень.

Необхідно зауважити, що сама по собі неповна, невчасна, невірогідна або упереджена інформація, що використовується, у більшості випадків не завдає такої шкоди людині, що можна було б говорити про її небезпеку.

Людина кожну мить стикається з такою інформацією у повсякденному житті та під час її отримання, апріорі, вважає, що ця інформація є повною, своєчасною та вірогідною. Тільки через визначений час можна оцінити міру її повноти, своєчасності та вірогідності, чи взагалі не оцінити.

Ми живемо у часи коли цифрові технології вже стали частиною нашого життя. Сфери створення та використання цифрових технологій стрімко розширяться та проваджуються у все більше напрями та процеси і процедури забезпечення життєдіяльності як людської особистості, так і суспільства на всіх рівнях.

Формування суспільства, в якому соціальна, економічна та політична діяльність базується на використанні цифрових технологій та штучному інтелекті, значною мірою залежить від сприйняття сучасних цифрових новацій переважної більшістю громадян незалежно від віку.

Під поняттям «персональні дані» прийнято розуміти будь-яку інформацію, яка стосується будь-якої конкретно визначеної особи або особи,

що може бути конкретно визначеною («суб'єкта даних»). Тобто суб'єктом персональних даних може бути будь яка осіб незалежно від статі: чоловіча або жіноча, віку: дитя або доросла та ін. Коли говоримо про захист персональних даних дітей необхідно враховувати, що статтею 1 част. І Конвенції: про права дитини встановлено, що «Для цілей цієї Конвенції дитиною є кожна людська істота до досягнення 18-річного віку, якщо за законом, застосовуваним до даної особи, вона не досягає повноліття раніше розгляду» [1].

Враховуючи викладене вище можна стверджувати, що мова йде про розгляд захисту визначених даних засобами інформаційної безпеки та кібербезпеки. Чому ми говоримо одразу про два види безпеки – інформаційний та кібернетичний?

Інформаційна безпека – 1) створення умов запобігання та усунення несанкціонованого поводження з інформацією та інформаційними ресурсами на всіх етапах їх життєвого циклу; 2) стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації.

Кібербезпека – стан захищеності життєво важливих інтересів особистості, суспільства і держави в умовах використання комп'ютерних систем та/або телекомунікаційних мереж, за якого мінімізується завдання їм шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки функціонування інформаційних технологій; несанкціоноване поширення, використання і порушення цілісності, конфіденційності та доступності інформації.

Виходячи з сутності наведених понять можна встановити, що

кібербезпека є невід'ємною складовою інформаційної безпеки в умовах використання комп'ютерних систем та/або телекомунікаційних мереж.

Сутність кібербезпеки полягає у створенні умов забезпечення технологічної спроможності людини, суспільства і держави приймати рішення на основі отримання та оброблення повної, вчасної, актуальної та достовірної інформації. Крім того, кібербезпека має забезпечити технологічними засобами запобігання та уникнення негативного впливу інформації, насамперед такої, поширення якої заборонено законом.

У зв'язку з розглядом питання захисту персональних даних дітей у цифрову епоху, цілком природно виникає питання залежності цього захисту від віку суб'єктів даних.

Відповідь може бути наступною. В принципі технічні, технологічні програмно-апаратні засоби захисту персональних даних не залежать від віку суб'єктів даних.

Майже щодня ми ділимося інформацією про себе: де живемо, що купуємо, куди ходимо. Ми ділимося цим в соціальних мережах, месенджерах, при встановленні додатків на пристрій. Дезінформація — ще одна серйозна загроза. В інтернеті дуже легко поширювати неправдиві новини, які виглядають правдоподібно. Фейкові новини поширюються набагато швидше, ніж правдиві, бо часто вони більш сенсаційні та емоційні. Це може впливати на все: від вибору товарів до політичних поглядів і навіть рішень про здоров'я особливо. Залежність від цифрових пристроїв також становить ризик. Ми проводимо за екранами дедалі більше часу, що впливає на наше фізичне та психічне здоров'я. Також важливо налаштовувати параметри приватності на всіх платформах і використовувати надійні паролі та двофакторну автентифікацію. Цифрова епоха створює нам дуже багато можливостей, але вміння розпізнавати та уникати інформаційних ризиків стає необхідною навичкою для кожного. Особливу увагу необхідно приділяти підготовці дітей до свідомого розуміння та, цілком природно, поводження з інформацією, яка відноситься до персональних даних,

уникаючи, навіть випадкового розголошення персональних, конфіденційних та інших непублічних даних.

Реальне життя показує, що сучасні діти досить швидко починають «підходити» до відчуття дорослості завдяки ранньому використанню кіберпростору, але не розуміючи при цьому «можливостей та цілей» інформації, яку отримують.

На наш погляд вже з 3-го до 10-го – 11-го класів середньої школи необхідно, з врахуванням віку, можливостей сприйняття та доступною мовою, готувати наших громадян базовим основам у сферах розуміння природи інформації, інформаційної безпеки та кібербезпеки, тим більше, що наробок уже є багато. Крім того, з 24-го лютого 2022 року реальні події підказують теж саме.

Список використаних джерел:

1. Конвенція про права дитини: Конвенція ООН від 20.11.1989. // База даних Законодавство України / ВР України. URL: http://zakon3.rada.gov.ua/laws/show/995_021

ЦИФРОВИЙ СУВЕРЕНІТЕТ ДИТИНИ. Кронівець Т.М.

кандидат юридичних наук, доцент,
Вінницький державний педагогічний університет імені Михайла Коцюбинського
ORCID ID: 0000-0002-5506-3418

Сучасні процеси глобалізації, швидкий розвиток штучного інтелекту та життя в цифровому середовищі створюють значні виклики для молодого покоління, яке вже з раннього віку активно взаємодіє з цифровими технологіями. Діти використовують відповідні інструменти для навчання, спілкування, розваг і самовираження, що формує їхнє світосприйняття та впливає на розвиток особистості. Однак разом із новими можливостями

виникають і загрози, серед яких, приміром, порушення приватності та кібербулінг. У таких умовах формування культури відповідального споживання цифрового контенту та захист прав дітей у кіберпросторі, зокрема їхнього цифрового суверенітету, стали ключовим пріоритетом для міжнародної спільноти.

У нормативних актах Європейського Союзу (далі – ЄС) поняття «цифровий суверенітет» (digital sovereignty) не має єдиного офіційного визначення, проте воно активно використовується в політичних заявах та документах. Зокрема, Європейський парламент у 2021 році визначив цифровий суверенітет як «здатність Європи розробляти, надавати, захищати та зберігати критичні технології, необхідні для добробуту громадян та процвітання бізнесу, а також здатність діяти та приймати рішення незалежно в глобалізованому середовищі» [1, с. 15-16]. Натомість у звіті Європейської комісії про стан цифрового десятиліття, складеному у 2023 році, цей термін розглядається як «здатність діяти незалежно у цифровому світі» [1, с. 16].

У контексті забезпечення прав дитини, враховуючи наведені офіційні тлумачення інституцій ЄС, вважаємо, що під цифровим суверенітетом дитини загалом варто розуміти її право на контроль, захист та управління власною цифровою ідентичністю, даними та цифровими слідами. Реалізація цього права та формування комплексного захисту дітей у цифровому середовищі є наріжним каменем сучасної міжнародної політики.

Так, наприклад, пріоритетним напрямом Стратегії Ради Європи з прав дитини (2022-2027) «Права дітей у дії: від постійного впровадження до спільних інновацій» є саме забезпечення того, щоб голоси дітей були почуті в процесах прийняття рішень, що їх стосуються [2]. У межах цієї Стратегії підкреслюється, що розкриття потенціалу дітей вимагає не лише надання їм можливостей для розвитку, але й одночасного захисту від цифрових загроз та етичних викликів.

Разом з тим, концепція «цифрового суверенітету» дітей узгоджується також і з іншими європейськими документами, зокрема, Стратегією «Європа

2020» [3], Цілями сталого розвитку ЄС на 2030 рік [4], Молодіжною стратегією ЄС (2019-2027) [5], Програмою «Креативна Європа» (2021-2027) [6] та Загальним регламентом про захист даних (GDPR) [7], створюючи цілісний підхід до формування безпечного, інклюзивного та сприятливого простору для особистісного розвитку молоді.

Україна, як й інші країни Європи, давно надає пріоритет захисту прав дітей, впроваджуючи численні успішні ініціативи у національному правовому полі. Однак попри це, в нашій державі наявний фрагментований підхід до вивчення проблеми забезпечення цифрового суверенітету дітей. Вітчизняні науковці та практики приділяють обмежену увагу законодавству, стратегіям та методам ЄС у цій галузі, що ускладнює ефективну імплементацію найкращих практик та гальмує процес гармонізації національних підходів з європейськими стандартами.

Крім того, недостатньо дослідженими залишаються і питання, пов’язані з формуванням цифрових компетентностей у дітей, створенням безпечного цифрового контенту, а також із гарантуванням їхніх прав в освітньому процесі та творчому самовираженні. Відсутність системного бачення у цій сфері зумовлює недосконалість підходів до виявлення та нейтралізації цифрових ризиків, які здатні серйозно впливати на реалізацію цифрового суверенітету дитини як одного з фундаментальних принципів її захисту у віртуальному просторі.

Отже, все вищезазначене свідчить про наявність нагальної потреби в розробці цілісної, науково обґрунтованої та інтегрованої національної політики щодо забезпечення цифрового суверенітету дітей, яка має ґрунтуватися на кращих європейських практиках і бути адаптованою до соціально-правових реалій України, забезпечуючи дієвий, сталий і всебічний захист прав дитини в кіберпросторі.

Майбутнє України в ЄС, і саме молоде покоління стане рушійною силою, що відбудує країну після перемоги, сформувавши нове європейське суспільство, засноване на демократичних цінностях, етичному управлінні та

технологічних інноваціях. Відтак забезпечення цифрового суверенітету дітей є важливою передумовою цього процесу, адже саме в цифровому просторі сьогодні закладаються основи для їхнього розвитку.

Список використаних джерел:

1. Vogiatzoglou P. The EU's Quest for Digital Sovereignty: A Matter of Quantum Innovation? *Digital Society*. 2025. Vol. 4 (16). P. 4-16.

2. Strategy for the Rights of the Child (2022-2027). URL: https://surl.lu/khngir (дата звернення: 29.05.2025).

3. Europe 2020: A strategy for smart, sustainable and inclusive growth. *EUR-Lex*. URL: https://surli.cc/nxnfco (дата звернення: 29.05.2025).

4. Transforming our world: the 2030 Agenda for Sustainable Development. *United Nation*. URL: https://sdgs.un.org/2030agenda (дата звернення: 29.05.2025).

5. EU youth strategy (2019-2027). *EUR-Lex*. URL: https://surl.li/zsmzlk (дата звернення: 29.05.2025).

6. Creative Europe programme 2021-2027. URL: https://surl.li/bdwcez (дата звернення: 29.05.2025).

7. General Data Protection Regulation (EU GDPR). URL: https://gdpr-text.com/ (дата звернення: 29.05.2025).

ІНФОРМАЦІЙНА ГІГІЄНА ДІТЕЙ У ЦИФРОВУ ЕПОХУ.

Дорогих С.О.

кандидат юридичних наук,
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0002-2748-1938

Цифровізація стала ключовою рисою сучасного суспільства, трансформувавши всі сфери людської діяльності. Доступ до інформації

практично необмежений, а Інтернет став середовищем, у якому зростають нові покоління. Особливо актуальним це є у контексті дитинства — періоду формування світогляду, цінностей, критичного мислення. За умов інтенсивної інформаційної взаємодії, важливим постає питання інформаційної гігієни як складової цифрової безпеки та психічного здоров'я дитини.

Інформація сьогодні – це не лише знання, а й потужний чинник формування особистості. Фраза «людина є тим, що вона споживає» цілком справедлива не лише для харчування, а й для інформаційного простору. Контент, що надходить із різних джерел – новини, відео, соціальні мережі, блоги – впливає на емоційний стан, світогляд, поведінкові реакції. У дитячому віці цей вплив особливо глибокий, адже психіка ще не сформована, а здатність до критичного мислення лише розвивається. Таким чином, дитина, поглинаючи інформаційний потік, поступово формує уявлення про світ — часом спотворені або небезпечні.

Діти сьогодні починають користуватися гаджетами та взаємодіяти з Інтернетом ще до того, як опановують базові навички читання. Цифрові пристрої виконують функцію няні, ігрового майданчика, інструменту пізнання, а іноді – й замінюють спілкування з однолітками або батьками. В результаті формуються нові моделі комунікації, поведінки та навчання.

З одного боку, Інтернет надає безпрецедентні можливості для розвитку, доступу до знань і творчості. З іншого – загроза потрапляння до інформаційного середовища, яке дитина не здатна повністю осмислити та контролювати. Деструктивний контент, фейкова інформація, кібербулінг, онлайн-залежність – усе це реальні виклики, які ставлять під загрозу безпечне дитинство.

Орієнтація в цифровому просторі вимагає знань, навичок і постійного супроводу. Просте обмеження доступу до Інтернету або його заборона не вирішує проблему – натомість необхідно сформувати стійкі навички цифрової грамотності.

Перш за все, дитина повинна вміти розрізняти надійні джерела від фейкових, розуміти принципи функціонування соціальних мереж, алгоритми персоналізації контенту та небезпеки онлайн-спілкування. Також важливо навчити дитину емоційній саморегуляції у взаємодії з інформацією — вміння не піддаватися паніці, агресії або нав'язуванню чужої думки. Це завдання лежить як на школі, так і на батьках, адже тільки системний підхід забезпечить результат.

Поняття інформаційної гігієни включає в себе вміння захищати себе від шкідливого контенту, дозувати споживання інформації, зберігати емоційну стабільність та критичне мислення. Так само, як фізична гігієна є щоденною практикою догляду за тілом, інформаційна гігієна має стати звичкою, частиною культури поведінки у цифровому середовищі.

Для дітей така культура формується поступово: через освітні програми, приклади дорослих, інтеграцію тем цифрової безпеки у навчальні плани. Надзвичайно важливим є створення позитивного інформаційного середовища – з контентом, що сприяє розвитку, емпатії, творчості.

Інтернет, попри свій потенціал, містить велику кількість небезпечного, деструктивного контенту. Йдеться не лише про відверто насильницькі чи порнографічні матеріали, а й про тонку маніпуляцію, фейкові новини, пропаганду, культивування ворожнечі, мовою ворожнечі тощо.

Діти є вразливими до подібного контенту, оскільки не мають ще сформованих моральних фільтрів або знань для критичного аналізу. Ці загрози здатні викликати страх, агресію, відчуття безнадії або формування антисоціальної поведінки. Проблема ускладнюється також анонімністю в мережі, що унеможливлює оперативне реагування з боку батьків або вчителів.

Існує два основні методи протидії шкідливому інформаційному впливу на дітей. Перший – адміністративно-технічний: заборона, фільтрація, обмеження доступу до певних сайтів або контенту. Цей шлях є порівняно простим у реалізації, однак має суттєві недоліки. По-перше, будь-яку

заборону можна обійти – дитина швидко навчиться користуватися VPN, знайде альтернативні джерела. По-друге, заборонене, як відомо, приваблює. Тобто такий метод не вирішує проблему, а лише її відкладає.

Другий – більш складний, але дієвий – полягає в системному навчанні. З раннього віку дитина повинна отримувати знання про інформаційну гігієну, цифрову етику, безпеку в мережі. Це має бути послідовна політика на всіх рівнях освіти: від дитячого садка до старшої школи. Необхідна також підготовка педагогів, створення навчальних програм, адаптованих до віку дітей.

Висновки. Інформаційна гігієна у цифрову епоху – це питання, яке має стратегічне значення для розвитку особистості, захисту прав дитини та формування безпечного суспільства. Сучасні діти виростають у середовищі, де інформація впливає на всі аспекти їхнього життя. Тому лише завдяки поєднанню обізнаності, критичного мислення та освітніх стратегій можна забезпечити формування цифрово грамотного покоління, здатного протистояти загрозам інформаційного світу.

ШТУЧНИЙ ІНТЕЛЕКТ В ОСВІТІ І ЦИФРОВА БЕЗПЕКА ДИТИНИ: ТЕРМІНОЛОГІЯ ТА ОФІЦІЙНІ НАСТАНОВИ.

Пінчук О.П.

кандидат педагогічних наук, старший науковий співробітник,
Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0002-2770-0838

Штучний інтелект (ШІ) – «організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання шляхом використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час

роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань» [1, с.32]. У наукових джерелах, офіційних документах, освітніх і аналітичних матеріалах, публіцистичній літературі використовують як синоніми такі формулювання як: сервіси на основі штучного інтелекту, цифрові сервіси; інструменти зі штучним інтелектом; інтелектуальні сервіси та штучноінтелектні сервіси.

Рамкова конвенція Ради Європи про штучний інтелект та права людини, демократію та верховенство права [4] є першим в історії міжнародним юридично обов'язковим договором у цій галузі. Україна – один з підписантів цього документу. Одним із базових принципів Конвенція визначає повагу до приватного життя та захист персональних даних, що є критичним для захисту прав дітей у цифровому середовищі. Конвенція пропонує державам-учасницям два способи дотримання її принципів та зобов'язань під час регулювання: 1) ухвалити рішення бути безпосередньо зобов'язаними відповідними положеннями Конвенції, 2) вжити інших заходів для дотримання положень договору, повністю дотримуючись своїх міжнародних зобов'язань щодо прав людини, демократії та верховенства права.

Діти потребують особливого захисту в умовах цифрової трансформації суспільства. Тут доречно згадати дослідження [5] 2024 року, що проведене серед 12-17-річних дітей з різних європейських країн (7 тис. учнів з Німеччини, Греції, Португалії, Румунії, Іспанії, Туреччини та Великої Британії). Згідно з дослідженням, майже 74% підлітків у Європі вважають, що ШІ суттєво вплине на їхнє професійне життя. Але лише менше половини вірить, що школа їх до цього готує.

Ми вступаємо в еру, де ШІ вже не фантастика, а частина шкільного щодення: від текстових чатботів до рекомендацій у навчальних платформах. Але разом із можливостями приходить і відповідальність. У рекомендаціях [2]-[3], розроблених Міністерством цифрової трансформації та МОН

України, акцент робиться на прозорості алгоритмів, добровільній згоді та обмеженні дискримінаційного впливу. Зокрема, рішення, що впливають на освітню траєкторію особи, не повинні прийматися автоматизовано без участі людини (принцип «контроль з боку людини»).

Захист персональних даних дітей має бути невід'ємним елементом цифрової інфраструктури освітнього закладу. Це вимагає наявності чітких політик конфіденційності та технічного захисту при впровадженні ШІ в закладі освіти.

Перед використанням будь-яких цифрових платформ або ШІ-сервісів має проводитись правова та технічна експертиза щодо безпеки персональних даних, що особливо важливо у випадку неповнолітніх. Одна з ключових рекомендацій щодо цифрової безпеки: мінімізація введення чутливої інформації. Учні та вчителі, адміністрація закладу освіти не повинні вводити персональні, конфіденційні або таємні дані в будь-яку систему ШІ. Категорично заборонено вводити у системи ШІ імена учнів, контактні дані, інформацію про здоров'я, психологічний стан тощо без спеціального дозволу. Це положення має бути частиною кодексу поведінки та етичного навчання у сфері ШІ.

Безпека в цифровому середовищі має починатися з базової обізнаності про ризики та способи самозахисту. Учасники процесу мають володіти інструментами цифрової гігієни. При використанні інструментів на основі ШІ учитель повинен перевіряти їх на відповідність психоемоційним і віковим особливостям учнів, враховувати особливості сприйняття та емоційного розвитку дитини певного віку. Це особливо важливо при використанні генеративних інструментів у початковій школі. Для всіх без виключення учнів віком до 18 років потрібна згода батьків або законних представників.

Професійний розвиток педагогічних працівників у галузі ШІ-компетентності має ключове значення для забезпечення відповідального використання технологій. Це передбачає не лише технічну, а й етичну, юридичну та дидактичну підготовку.

Ми порівняли деякі аспекти настанов Міністерство освіти і науки України та Мінцифри [2]-[3] щодо захисту дітей у цифрову епоху.

Аспект	ЗЗСО, 2024 [3]	ЗВО, 2025 [2]
Захист персональних даних (ПД)	Наголос на забороні введення учнями персональних і конфіденційних даних у системи ШІ (с. 23).	Зазначено необхідність забезпечення легітимного доступу, згоди на обробку, надійного зберігання та якісного управління даними (с. 24-25).
Інформована згода	Необхідність інформування та отримання згоди батьків або їх законних представників (для учнів до 18 років) перед використанням ШІ (с. 11, 23).	Уточнюється вимога поінформованості здобувачів щодо збору й обробки їхніх даних у межах університетських політик, але згода пов'язана з повноліттям і самостійною відповідальністю.
Регламентація доступу до даних	Адміністрація має забезпечити відповідність сервісів законодавству про захист ПД (с. 10).	Впроваджуються політики конфіденційності на інституційному рівні: управління доступом, аудит, мінімізація використання чутливої інформації (с. 13, 24).
Ризики автоматизованого оцінювання	Автоматизоване оцінювання вважається високо ризиковим і має супроводжуватись людським контролем.	ШІ-системи для оцінювання мають містити механізми перегляду викладачами, що гарантує дотримання прав здобувачів (с. 11, 13).
Політики використання ШІ	Вимагається локальна регламентація і запобігання збору даних учнів без згоди.	Обов'язкове створення політик ШІ на рівні ЗВО, включаючи обмеження на обробку конфіденційної інформації та заборону несанкціонованого використання (с. 13, Дод. 6).

Етична складова	Містить рекомендації щодо виховання етичного ставлення до використання ШІ у школі (с. 24).	Запроваджуються принципи прозорості, підзвітності, уникнення дискримінації, дотримання конфіденційності (с. 11–12).

У підсумку варто зауважити, що обидва документи визнають обробку персональних даних у ШІ як вектор підвищеної загрози. У закладах загальної середньої освіти акцентовано на захисті дітей як уразливої категорії, у закладах вищої освіти – на інституційному управлінні та на внутрішніх політиках. Механізми інформованої згоди та обмеження збору даних більш строго прописані у документі для шкіл, де діти виступають як правові суб'єкти, що потребують додаткового захисту. Використання ШІ без людського контролю в оцінюванні розглядається як неприпустиме в обох документах, проте у [2] деталізовано механізми запобігання та зроблено більший акцент на автономії інституції та її політик, що врегульовують не лише захист даних, а й академічну доброчесність, етику, зокрема й авторське право.

Визнаючи відповідальність за використання автоматизованих інструментів, а також з метою сприяння утвердженню нових етичних норм у добу цифрових технологій маю зазначити, що задля стилістичної узгодженості тексту в окремих формулюваннях було використано інструмент ChatGPT, змістовне наповнення повністю ґрунтується на авторському дослідженні.

Список використаних джерел

1. Міністерство цифрової трансформації України. *Словник термінів у сфері штучного інтелекту*. Упоряд. Д. Чумаченко, Д. Мішкін, О. Андрієнко, О. Краковецький, О. Турута, О. Дубно, Д. Хрущова, А. Кобрін, Т. Авдєєва, І. Кравець, В. Герасимяк, О. Шабанов, А. Бистрицька. Київ, 2024. Дата звернення: 27 травня 2025. https://surl.li/ppgtki.

2. Міністерство цифрової трансформації України, та Міністерство

освіти і науки України. *Рекомендації щодо відповідального впровадження та використання технологій штучного інтелекту в закладах вищої освіти*. Київ, 2025. https://doi.org/10.33407/lib.NAES.id/eprint/745301

3. Міністерство освіти і науки України. *Інструктивно-методичні рекомендації щодо впровадження та використання технологій штучного інтелекту в закладах загальної середньої освіти*. Київ, 2024. https://mon.gov.ua/static-objects/mon/sites/1/news/2024/05/21/Instruktyvno.metodychni.rekomendatsiyi.shchodo.SHI.v.ZZSO-22.05.2024.pdf.

4. Council of Europe. *Framework Convention on Artificial Intelligence and Human Rights, Democracy and the Rule of Law*. Strasbourg: Council of Europe, 2024. https://www.coe.int/en/web/artificial-intelligence/the-framework-convention-on-artificial-intelligence

5. OECD. *Empowering Learners for the Age of AI: An AI Literacy Framework for Primary and Secondary Education*. Paris: OECD Publishing, 2025. https://ailiteracyframework.org/wp-content/uploads/2025/05/AILitFramework_ReviewDraft.pdf.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ В УМОВАХ ЦИФРОВІЗАЦІЇ ОСВІТИ: ПРАВОВІ ТА ІНФОРМАЦІЙНО-БЕЗПЕКОВІ АСПЕКТИ. Корж І. Ф.

доктор юридичних наук, старший науковий співробітник,
Державна наукова установа «Інститут інформації, безпеки і права НАПрН України»
ORCID ID: 0000-0003-0446-5975

Цифровізація освіти, яка значно посилилася під час пандемії COVID-19, спричинила широке використання електронних платформ, мобільних застосунків, відеозв’язку та електронних щоденників. Діти активно

взаємодіють у цифровому просторі, залишаючи значний обсяг персональної інформації. При цьому вони не завжди усвідомлюють наслідки її поширення в інформаційному просторі, що робить їх особливо вразливими до зловживань інформацією.

Основними загрозами для персональних даних дітей у даному випадку є:

– **технічні** – *кібератаки*, *фішинг* (від англ. Fishing – риболовля) – вид шахрайства, метою якого є виманювання в довірливих або неуважних користувачів мережі персональних даних клієнтів онлайнових аукціонів, сервісів із переказу або обміну валюти, інтернет-магазинів. Шахраї намагаються змусити користувачів самостійно розкрити конфіденційні дані – наприклад, надсилаючи електронні листи з пропозиціями підтвердити реєстрацію облікового запису, що містять посилання на сайт, зовнішній вигляд якого повністю копіює дизайн відомих ресурсів; *незахищені платформи* – наприклад UnityBase (full stack-платформа з відкритим вихідним кодом на основі JavaScript-рушію Mozilla, SpiderMonkey);

– **соціальні** – *кібербулінг* (англ. Cyberbullying – кіберзалякування), тобто умисне цькування щодо визначеної особи у кіберпросторі, як правило, впродовж тривалого проміжку часу. *Маніпуляції в мережі*. *Цифрове шахрайство* – окрім *фішингу*, це *вішинг* (телефонне шахрайство), це вид шахрайства, при якому зловмисники за допомогою **телефонного зв'язку** змушують людину повідомити їм свої конфіденційні банківські або персональні дані або стимулюють до здійснення певних дій зі своїм банківським рахунком або банківською картою; ***смішинг* (англ. smishing – sms+phishing, це SMS-шахрайство); *бейтінг* (шахрайство через зовнішні носії) –** техніка соціальної інженерії (метод маніпуляції діями людини), яку використовують зловмисники при якій жертві підкидають що-небудь, щоб вона почала діяти;

– **правові** – відсутність належної згоди батьків, нерегламентоване використання даних про дітей.

Зазначимо, що правову базу захисту персональних даних включає в себе відповідні закони [1,2] та інші закони в освітянській сфері, а також норми міжнародного права, зокрема Конвенцію ООН [3] про права дитини. Однак ці норми здебільшого потребують конкретизації та ефективного застосування в освітній практиці. Прикладом можуть слугувати вимоги Регламенту ЄС [4], які передбачають обов'язкову згоду батьків для обробки даних дітей до 16 років, прозоре інформування та право на видалення даних (право бути забутим).

Для забезпечення ефективного захисту персональних даних дітей в умовах цифровізації освіти вбачається доцільним впровадити наступні практики:

– прийняття політик конфіденційності в навчальних закладах;

– регулярне підвищення цифрової грамотності педагогів, учнів та батьків;

– обмеження доступу до персональних даних, застосування принципу мінімізації збору;

– використання шифрування, автентифікації (процес підтвердження того, що лише користувачі, служби і програми з належними дозволами можуть отримувати доступ до корпоративних ресурсів), захисту облікових записів;

– проведення аудитів інформаційної безпеки в школах.

Держава, у свою чергу, має забезпечити чіткі механізми моніторингу та контролю за дотриманням законодавства, а також підтримувати громадські ініціативи у сфері цифрових прав дітей.

О.А. Явор, В.Ф. Піддубна та О.О. Рубан, досліджуючи правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного законодавства та вимог GDPR зазначають [5, С. 32], що обробка персональних даних неповнолітньої особи мають відповідати певним вимогам: мова повинна бути зрозумілою для неповнолітньої фізичної особи; необхідно щоб неповнолітня особа розуміла зміст пропозиції і умови

договору після надання своїх персональних даних та згоди на укладення договору. Реалізація державних функцій має здійснюватися без примушування людини до надання згоди на обробку персональних даних. Така обробка персональних даних повинна здійснюватися в межах та на підставі законів і нормативно-правових актів України, враховуючи міжнародні договори в цій сфері.

Крім того, дослідники вважають, що до способів захисту персональних даних дітей можна віднести: отримання копії персональних даних як дітьми так і їх батьками, виправлення неточних персональних даних, заповнення неповних даних, користування правом бути «забутим» і мати право «стерти» особисті дані; визнання правочину недійсним; відшкодування майнової та моральної шкоди за незаконне використання персональних даних неповнолітнього. Якщо діє правило щодо обмеження обробки персональних даних неповнолітніх осіб за певних обставин, то діти віком з 14 до 18 років можуть заперечувати проти обробки персональних даних, яка здійснюється на законних підставах при реалізації суспільного завдання або інших законних інтересів. При цьому згадані технології не повинні бути безальтернативними й примусовими. Особи, які відмовилися від обробки своїх персональних даних, повинні мати альтернативу – використання інших традиційних методів ідентифікації особи згідно діючого вітчизняного законодавства.

У свою чергу Маркович Х.М., досліджуючи правові аспекти захисту даних неповнолітніх у цифровому середовищі, зокрема в Інтернеті [6, С. 202], зазначає, що важливими аспектами є забезпечення прозорості у використанні даних, контроль над тим, куди і кому передаються дані, а також можливість для батьків і дітей отримувати доступ до інформації та відкликати згоду. Однак, реалізація цих вимог часто стикається з практичними труднощами, що підкреслює необхідність постійного вдосконалення заходів захисту та підвищення обізнаності щодо безпеки персональних даних неповнолітніх. Водночас, необхідним вважаємо

дотримуватися балансу між захистом дитини і її свободою. Обмеження доступу до певної інформації або технологій, хоча й спрямоване на забезпечення безпеки, не повинно надмірно обмежувати можливості дітей щодо самовираження, навчання та соціалізації.

Знайти цей баланс – одне з головних завдань законодавця та суспільства загалом, адже свобода і захист не повинні взаємовиключати, а радше доповнювати одне одного в інтересах повноцінного розвитку дитини.

Овчарук О.В. і Гальперіна В.О., розглядаючи міжнародні підходи до захисту персональних даних дітей у цифровому освітньому середовищі [7, С.63-64] зазначають, що використання цифрових інструментів для захисту персональних даних дітей у цифровому освітньому середовищі потребує уваги освітян. З огляду на це міжнародні організації визначили основні підходи та принципи, що пов'язані з діяльністю освітніх інституцій різного рівня щодо забезпечення основних прав дітей на безпеку персональних даних та здійснення заходів у цьому напрямку. Особливу увагу приділяють підвищенню обізнаності освітян, батьків та структур, що збирають дані дітей про ризики, механізми захисту та можливості цифрових освітніх середовищ. Саме тому на часі є розроблення низки навчально-просвітницьких матеріалів та проведення низки заходів з питань захисту дітей у цифровому середовищі у контексті кращих світових та європейських практик.

І.І. Бочкова, К.М. Врублевська-Місюна і В.П. Тичина зазначають [8], що для зменшення ризиків, необхідно врахувати принципи Регламенту у національному законодавстві, зокрема прозорості та обмеження налаштувань, окрім того, важливо також підвищувати правову культуру громадян у сфері захисту персональних даних, сприяючи вдосконаленню нормативного середовища.

Таким чином, захист персональних даних дітей в освітньому середовищі, в умовах його цифровізації потребує комплексного, міждисциплінарного підходу. Йдеться не лише про юридичну відповідність, а й про етичну відповідальність усіх суб'єктів освітнього процесу.

Формування цифрової культури та інформаційної безпеки має стати пріоритетом державної політики у сфері освіти.

Список використаних джерел

1. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 10.05.2025).

2. Про освіту: Закон України від 5 вересня 2017 р. № 2145-VIII / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2145-19#Text (дата звернення: 10.05.2025).

3. Про права дитини: Конвенція ООН від 21 грудня 1995 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text (дата звернення: 11.05.2025).

4. Регламент Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 11.05.2025).

5. О. А. Явор, В. Ф. Піддубна, О. О. Рубан. Правові проблеми захисту персональних даних неповнолітніх осіб відповідно до вимог вітчизняного законодавства та вимог GDPR. Journal «Science Rise: Juridical Science». №3(25). 2023. С. 23-34. URL: file:///C:/Users/Admin/Downloads/286647-Article%20Text-663362-1-10-20230913.pdf (дата звернення: 11.05.2025).

6. Маркович Х.М. Правові аспекти приватності дітей в Інтернеті: баланс між захистом і свободою. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/70379/1/ 312972-Текст%20статті-724073-1-10-20241008.pdf (дата звернення: 11.05.2025).

7. Овчарук О.В. і Гальперіна В.О. Міжнародні підходи до захисту персональних даних дітей у цифровому освітньому середовищі. URL:

https://lib.iitta.gov.ua/id/eprint/727349/1/Овчарук%20О.%20Гальпєріна%20В.%20Збірник%20Імерсивні%20технології%20в%20освіті%202021.pdf (дата звернення: 11.05.2025).

8. І.І. Бочкова, К.М. Врублевська-Місюна, В.П. Тичина. Щодо необхідності врахування міжнародного досвіду правового регулювання у сфері захисту інформації про дитину. URL: http://journal-app.uzhnu.edu.ua/article/view/294671 (дата звернення: 11.05.2025).

ПРЕВЕНТИВНІ ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ В УМОВАХ ДІДЖИТАЛІЗАЦІЇ. Волобоєв А.О.

доктор філософії в галузі права,
Донецький державний університет
внутрішніх справ
ORCID ID: 0000-0002-7138-5847

Сучасний світ стрімко перетворюється на цифрову реальність, де діти, як найбільш незахищена категорія користувачів, стикаються з численними загрозами безконтрольного використання їхніх персональних даних. Цінність дитячої приватності закріплена не лише етичними міркуваннями, а й базовими правами, відображеними в міжнародному законодавстві, зокрема статтею 16 Конвенції ООН про права дитини [1]. Проблема захисту персональних даних дітей дедалі стає особливо актуальною з огляду розвитку штучного інтелекту, Big Data та Інтернету речей, що формують середовище для потенційно необмеженого збирання особистої інформації.

Вивченням захисту персональних даних, у тому числі й захисту даних дітей, займалися як вітчизняні, так і зарубіжні науковці: О. А. Баранов, В. М. Брижко, О. О. Золотар, А. В. Пазюк, В. Г. Пилипчук, А. М. Новицький, М. ван Дейк та інші. Попри існуючі дослідження, досі відсутнє єдине розуміння превентивних технологій захисту персональних даних дітей як у науковому, так і в практичному вимірах.

Так, сучасна теорія інформаційного права виділяє окрему категорію персональних даних – дані неповнолітніх осіб. Ця категорія потребує посиленого правового захисту [2] через особливості її власників: обмежену дієздатність, психологічну вразливість та нездатність повністю усвідомлювати наслідки розкриття особистої інформації.

Головна правова проблема полягає в суперечності регуляторних підходів, де захист інтересів дитини вимагає максимального захисту її даних, а розвиток особистої автономії та цифрових навичок передбачає поступове розширення контролю дитини над власними даними відповідно до вікових особливостей. Прогресивні правові системи розв'язують цю розбіжність через концепцію «поступової автономії», що передбачає гнучку модель захисту залежно від етапів розвитку дитини.

Однак сучасні загрози персональним даним дітей мають багатовимірний і динамічний характер. До ключових категорій ризиків слід віднести:

- алгоритмічну профілізацію – створення детальних поведінкових профілів на основі цифрового сліду дитини, що може призвести до маніпулятивного впливу;
- гіперексплуатацію даних – використання інформації з освітніх платформ, ігрових сервісів та соціальних мереж для комерційних цілей без належної прозорості;
- технологічну вразливість – недостатній рівень безпеки інформаційних систем, що призводить до витоків даних з освітніх установ та дитячих сервісів.

Особливе непокоєння виникає від явища «цифрового детермінізму» [3], коли рання цифрова історія може невиправдано впливати на майбутні можливості дитини через алгоритмічні рішення в освітній, соціальній та економічній сферах.

На нашу думку, під превентивними технологіями захисту персональних даних дітей слід розуміти системну діяльність уповноважених

суб'єктів з розробки, впровадження та використання комплексу технічних, організаційних та правових заходів для випереджального запобігання порушенням у сфері обробки персональних даних дітей та мінімізації відповідних ризиків. Таке визначення відображає багатогранний характер досліджуваного явища.

Слід зазначити, що превентивні технології захисту відрізняються від традиційних форм забезпечення приватності своєю методологією, цільовою спрямованістю та часовими рамками. Якщо класичні методи захисту даних переважно реагують на вже виявлені порушення, то превентивні технології зосереджуються на випереджальному виявленні потенційних загроз та проактивному реагуванні на можливі ризики.

У зв'язку з цим, комплексна модель превентивного захисту персональних даних дітей має базуватися на поєднанні правових, технологічних та освітніх інструментах, як-то на:

- технологічному вимірі, що реалізується через впровадження принципу «приватність за замовчуванням» у розробку цифрових продуктів для дітей. Це передбачає мінімізацію збору даних, локальне зберігання інформації, автоматичне видалення даних після визначеного терміну та застосування диференційованої приватності;
- правовому вимірі, що включає розвиток спеціалізованого регулювання дитячої приватності через механізми попередньої оцінки впливу на захист даних, диференційовані вимоги до отримання згоди залежно від віку та запровадження професійного представництва інтересів дітей у сфері захисту персональних даних;
- освітньому вимірі, що передбачає формування критичної цифрової грамотності, розвиток батьківських компетентностей щодо контролю за персональними даними дітей та впровадження спеціалізованих програм підготовки фахівців з дитячої цифрової безпеки.

Тобто, ефективний захист персональних даних дітей вимагає зміни концепції – від реагування до превенції, що передбачає випереджальну

ідентифікацію ризиків та їхню нейтралізацію. Багатосуб'єктний характер захисту потребує узгоджених дій законодавців, технологічних компаній, освітніх закладів, батьків та самих дітей.

У такому контексті перспективними напрямами подальших досліджень є:

- розробка практичної моделі превентивного захисту персональних даних дітей;
- дослідження методологічних основ превентивних технологій, особливо прогностичних методів та технологій запобігання ризикам;
- аналіз стратегічних аспектів превентивного захисту в контексті формування інформаційної політики держави;
- дослідження практичних форм взаємодії всіх зацікавлених сторін для створення цілісної системи превентивного захисту персональних даних дітей.

Отже, сучасне розуміння сутності превентивних технологій захисту персональних даних дітей виходить за межі традиційних уявлень про інформаційну безпеку і потребує комплексного переосмислення її теоретичних засад. Формування цілісної системи превентивного захисту сприятиме кращому забезпеченню прав дітей у цифровому просторі та вдосконаленню інформаційної безпеки України в умовах глобальної діджиталізації.

Список використаних джерел

1. Конвенція про права дитини. ООН; Конвенція, Міжнародний документ від 20.11.1989. *Вебпортал Верховної ради України.* URL: https://zakon.rada.gov.ua/laws/show/995_021#Text.

2. Софіюк Т. О. Право на захист персональних даних в системі поколінь прав людини. *Dictum Factum : юридичний збірник.* Вип. № 2. Київ : ДУІТ, 2018. URL: https://df.duit.in.ua/index.php/dictum/article/view/43/36.

3. Chandler D. Technological or Media Determinism. *Інформаційна сторінка.* URL: http://visual-memory.co.uk/daniel//Documents/tecdet/tecdet.html.

ПРАВОВІ МЕХАНІЗМИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ДИТИНИ В ПРОЦЕДУРІ МЕДІАЦІЇ. Головко О.М.

кандидат юридичних наук., ст. дослідник
Державна науково установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0001-8963-6598

У цифрову епоху питання захисту персональних даних неповнолітніх потребує додаткової деталізації з огляду на виклики, які постають, зокрема в контексті процедур, що передбачають опрацювання чутливої інформації про дитину. Інформація про конфлікт, в якому опиняється дитина цілком передбачувано набуває чутливого характеру, тому процедура медіації за участі неповнолітніх вимагає ще більшої чіткості та прозорості механізмів захисту персональних даних неповнолітніх.

Медіація це добровільна, конфіденційна, структурована процедура, яка застосовується як один із способів альтернативного способу вирішення спорів. В період пандемії більшого поширення набула онлайн-медіація, яка спричинила чимало викликів для медіаторів по всьому світу.

Закон України «Про медіацію» прямо встановлює принцип конфіденційності як один із обов'язкових принципів проведення процедури. Він передбачає нерозголошення відомостей, що стали відомі в процесі врегулювання спору, за винятком випадків, прямо передбачених законом. Особливої уваги конфіденційність набуває у справах, де стороною або учасником медіації є неповнолітня особа, адже йдеться не лише про збереження приватності, а й про захист персональних даних у широкому сенсі – включаючи дані, що стосуються сімейних обставин, емоційного стану, освітнього середовища та інших чутливих аспектів.

Відповідно до п. 2 ч. 1 ст. 70 ЦПК України, особи, які за законом зобов'язані зберігати в таємниці відомості, що були довірені їм у зв'язку з

наданням послуг медіації, про такі відомості не можуть бути допитані як свідки. Це положення фактично дублюється в ч. 5 ст. 6 Закону України «Про медіацію», де зазначено, що медіатор не може бути допитаний як свідок у справі (провадженні) щодо інформації, яка стала йому відома під час підготовки до медіації та проведення медіації. Такі законодавчі положення створюють фундамент для забезпечення медіатором безпечного простору в процедурі, в тому числі, щодо неповнолітніх, які можуть виступати як сторонами, так і іншими учасниками медіації.

Важливо зазначити, що межі конфіденційності в процедурі визначають самі сторони, а також вони можуть бути деталізовані в угоді. Наприклад, Кодексом професійної етики медіатора Національної асоціації медіаторів України передбачено, що медіатор дотримується принципу конфіденційності без обмежень у часі, якщо інше не визначено сторонами. В той же час, коли йдеться про залучення дитини, то це накладає додаткові обмеження щодо диспозитивної поведінки сторін щодо конфіденційності в медіації.

Пропонуємо розглянути деякі аспекти захисту персональних даних дитини і процедурі медіації, з урахуванням викликів, які постають у цифрову епоху, та які гарантії має забезпечити медіатор і сторони процедури для ефективного дотримання прав дитини. У процедурі медіації персональні дані дитини – це будь-яка інформація, що прямо чи опосередковано стосується її особистості, життєвих обставин, стану здоров’я, думок, сімейних обставин або ідентифікаторів (включно з технічними), яка обробляється у процесі комунікації, документування, або збереження в цифровому або паперовому вигляді. Медіатор фактично виступає контролером або процесором таких даних.

Відповідно до положень статті 38 Загального регламенту щодо захисту даних в ЄС (далі – GDPR), діти вимагають специфічного захисту щодо своїх персональних даних, оскільки можуть бути менш обізнаними про ризики, наслідки та свої права, включно під час користування послугами, що пропонуються безпосередньо дитині [1]. Це специфічний захист викликаний

двома ключовими факторами: рівнем усвідомлення дитиною наслідків наданої інформації та тим, що дані, розкриті у дитячому віці, можуть переслідувати особу в майбутньому, створювати так званий ефект цифрового сліду.

Найпоширенішими ситуаціями, де дитина бере участь в медіації є сімейні відносини, відновне правосуддя (кримінальні правопорушення) та шкільна медіація.

Кодексом професійної етики Асоціації сімейних медіаторів України (далі – АСМУ) передбачено, що «медіація за участю дитини проводиться медіатором, що пройшов спеціалізоване навчання по роботі з дітьми в медіації, за згодою батьків та дитини» [2]. Вважаємо доцільним включити в програму такого навчання обов'язкову частину щодо персональних даних дитини. При проведенні медіації під час розлучення надважливим є врахування інтересів дитини. Дитина може безпосередньо зустрітись з медіатором (за згодою батьків) для врахування її думки під час прийняття рішень батьками [3]. Така зустріч може відбуватись онлайн, особливо якщо мова йде про транскордонні сімейні спори, де один з батьків не має можливості перетинати кордон.

Медіація є одним із заходів реалізації Національної стратегії розбудови безпечного і здорового освітнього середовища у новій українській школі. Шкільна медіація, безперечно, є пріоритетним напрямом подолання конфліктів серед однолітків. В той же час, важливо враховувати ризики, які можуть виникати через відсутність чітких правил та заходів дотримання конфіденційності всіма учасниками.

Окрім цього, в Україні діє програма відновного правосуддя, розроблена на основі рекомендацій Комітету міністрів Ради Європи та Організації об'єднаних націй (ООН) [4]. Додатком 2 до цього наказу передбачено підписання згоди на участь у Програмі відновного правосуддя за участю неповнолітніх, які є підозрюваними, обвинуваченими у вчиненні кримінального правопорушення, та обробку персональних даних. Згода

надається на обробку персональних даних та передання їх до центру з надання БПД. Окрім цього, потерпілим в таких категоріях справ теж може бути неповнолітня особа. Таку згоду також підписують законні представники неповнолітніх, без чого медіатор не має права розпочинати взаємодію зі сторонами та їх законними представниками. Також, ця згода розповсюджується на онлайн-формат медіації. Важливо враховувати специфіку кримінально-процесуальних відносин, яка накладає певні особливості на порядок забезпечення конфіденційності в процедурі.

Загальним коментарем №12 (2009) Комітету ООН з прав дитини роз'яснено зміст статті 12 Конвенції про права дитини. Зазначено, що «дитина має право на участь у рішеннях, що її стосуються, з урахуванням її віку та зрілості» [5]. Таким чином, що медіатор в онлайн процедурі має: поінформувати дитину у доступній формі, що її участь відбувається в цифровому форматі, та наслідки цього, зокрема, щодо обробки даних; забезпечити безпечний цифровий простір, що може передбачати підтримку або навпаки, відсутність дорослого, використання аватарів або аудіо замість відео – якщо дитина просить про це.

Відповідно до Рекомендації РЄ щодо дітей у цифровому середовищі, держави та оператори повинні мінімізувати збір і зберігання даних дітей [6]. Отже, медіатором має бути мінімізовано збір відомостей щодо дитини. Всі документи, записи, угоди повинні містити мінімум персональних даних дитини – лише ті, що є абсолютно необхідними. Використання умовних ідентифікаторів під час ведення записів або аналітики (для внутрішньої статистики, звітності медіатора) є пріоритетним.

Додати прозорості до медіаційних та постмедіаційних механізмів захисту дозволяють заходи письмового інформування сторін про порядок зберігання та знищення даних, надання контактної особи або інституції, куди можна звернутись у разі витоку або порушення конфіденційності.

Отже, обробка персональних даних в процедурі медіації щодо неповнолітніх, включно з онлайн форматом процедури, повинна бути

прозорою та заснованою на взаємній довірі між учасниками. Це передбачає механізм їх збереження та захисту від несанкціонованого доступу, а також порядок їх збереження або знищення після завершення процедури незалежно від факту підписання сторонами угоди за результатами медіації. Доступ медіатора до конкретних персональних даних має бути обумовлений межами його/її ролі та обов'язків, а також метою даної процедури. Учасники мають право знати, які дані обробляються та для яких цілей, вимагати видалення даних, якщо вони більше не потрібні.

В питанні захисту персональних даних дитини в процедурі медіації в цифрову епоху опорою мають стати такі правові конструкти як «найкращі інтереси дитини» та «чутлива інформація» про дитину. Вважаємо, що варто лишити простір для подальших дискусій з цієї тематики. Специфіка захисту персональних даних дітей в медіації, особливо, якщо вона проводиться онлайн, дає змогу глибше побачити етичні, правові й технологічні виклики для професійної спільноти.

Список використаних джерел

1. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC // EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj (дата звернення: 27.05.2025).

2. Кодекс професійної етики АСМУ / Асоціація сімейних медіаторів України. URL: https://www.afmu.org.ua/_files/ugd/4a26bd_5c817c71b2074c94a39c403de33eecf7.pdf (дата звернення: 23.05.2025).

3. Медіація під час розлучення та врахування інтересів дитини / Асоціація сімейних медіаторів України. URL: https://drive.google.com/file/d/1SJPApnxCdkGCpHw57AIwlB6MmYq3pgXO/view (дата звернення: 24.05.2025).

4. Наказ Міністерства юстиції, МВС, Офісу Генпрокурора від 22.07.2024

№ 2176/5/501/176 "Про реалізацію пілотного проєкту «Програма відновного правосуддя за участю неповнолітніх» / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/z1116-24 (дата звернення: 19.05.2025).

5. General comment No. 12 (2009): The right of the child to be heard, CRC/C/GC/12 / Office of the United Nations High Commissioner for Human Rights (OHCHR). URL: https://www2.ohchr.org/english/bodies/crc/docs/advanceversions/crc-c-gc-12.pdf (дата звернення: 23.05.2025).

6. Recommendation CM/Rec (2018)7 of the Committee of Ministers: Guidelines to respect, protect and fulfil the rights of the child in the digital environment / Council of Europe. URL: https://rm.coe.int/children-digital-environment-guidelines-en/16808d881a (дата звернення: 30.05.2025).

ВІДПОВІДАЛЬНІСТЬ ВЧИТЕЛЯ ЗА БЕЗПЕКУ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ В ЦИФРОВУ ЕПОХУ.

Кравчина О.Є.

Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0002-3903-0835

Відповідальність вчителя за безпеку персональних даних дітей залишається надзвичайно важливою, особливо, з огляду на те якими темпами відбувається цифровізація освіти. Використання онлайн-платформ, освітніх додатків, хмарних сервісів та інших цифрових інструментів стало невід'ємною частиною навчального процесу, в якому учителі працюють з чутливими персональними даними учнів (такі як імена, дати народження, контакти, оцінки чи медична інформація), що збільшує ризик витоку даних. Водночас кібератаки, фішингові схеми, витоки інформації й інші загрози активно впливають на освіту. Оскільки дані дітей є особливо вразливими й можуть стати об'єктом маніпуляцій, шахрайства або кібербулінгу, на

вчителів покладається відповідальність за їхній надійний захист. Учителі мають бути прикладом у створенні безпечного цифрового простору, захищаючи інформацію про учнів та навчаючи їх основам цифрової грамотності, що допомагає дітям орієнтуватися у світі технологій і уникати шкідливих ситуацій в інтернеті. Нажаль не всі вчителі мають належний рівень знань у сфері кібербезпеки чи законодавчих вимог щодо роботи з персональними даними. Це доводить важливість інтеграції відповідних програм підвищення кваліфікації для вчителів.

У багатьох країнах законодавство регулює процедури зберігання та обробки персональних даних дітей. В Україні ухвалено кілька документів, які визначають норми захисту персональних даних у сфері освіти. У «Концепції виховання дітей та молоді в цифровому просторі» сформульовано стратегічні напрями розвитку в цифровому середовищі, одним із ключових принципів якого є забезпечення конфіденційності та безпеки [1]. Професійний стандарт «Вчитель закладу загальної середньої освіти» акцентує увагу на інформаційно-цифровій компетентності педагогів. У ньому зазначено, що викладачі мають володіти навичками захисту персональних даних учнів, використовувати безпечні інформаційні системи та дотримуватись етичних норм при роботі з конфіденційною інформацією. [2]. Освітній омбудсмен підкреслює важливість дотримання закладами освіти принципів захисту персональних даних, особливо під час використання електронних журналів, відеоконференцій та цифрових платформ. [3]. Основний нормативний акт, який регулює процеси збору, зберігання та обробки персональних даних, — це Закон України «Про захист персональних даних». У ньому уточнюється поняття персональних даних, порядок їх обробки, а також передбачені наслідки за порушення цього закону [4]. Недотримання законодавчих норм може призвести до накладення штрафів згідно зі статтею 188-39 Кодексу України про адміністративні правопорушення. [5]. Учителям необхідно суворо дотримуватися цих правил, адже їх ігнорування загрожує не лише штрафами, а й серйозною юридичною відповідальністю.

У сучасну цифрову епоху персональні дані учнів потрапляють у зону підвищеного ризику через численні загрози, характерні для віртуального середовища. Насамперед існує ймовірність несанкціонованого доступу до інформації, що може статися внаслідок хакерських атак на освітні платформи або електронні журнали, витоку облікових даних користувачів чи використання спільних акаунтів без належних механізмів автентифікації. Іншою проблемою є неконтрольована передача або зберігання даних. Це може проявлятися через передачу персональної інформації третім сторонам без отримання згоди, а також унаслідок розміщення даних на незахищених пристроях чи в хмарних сервісах без належного рівня шифрування. Особливо небезпечним є неправильне використання зображень учнів. До таких випадків належить публікація фотографій або відео в соціальних мережах чи на сайтах навчальних закладів без належної згоди, а також поширення відеозаписів онлайн-уроків без відповідного контролю та регламентації. Додаткову загрозу становить використання ненадійного або недостатньо перевіреного програмного забезпечення. Освітні додатки без захищеної політики конфіденційності, прихований збір даних чи порушення норм GDPR або українського законодавства несуть потенційну небезпеку для приватності учнів. До цього додається людський фактор, коли помилки персоналу стають причинами витоку даних. Це може проявлятися як недбале поводження з паролями, випадкове надсилання особистої інформації стороннім особам або обговорення конфіденційної учнівської інформації у невідповідних умовах – наприклад, у відкритих публічних чи неформальних просторах. Суттєву роль у створенні загроз також відіграє відсутність чітких політик захисту даних у закладах освіти. Недостатньо сформульовані процедури обробки персональної інформації або невизначеність щодо відповідальності за їх порушення суттєво підвищують рівень уразливості. Окрему категорію загроз представляє соціальна інженерія. Фішингові атаки, спрямовані на вчителів чи учнів для отримання доступу до конфіденційної інформації, стають ще однією поширеною небезпекою у цифровому

просторі.

Обов’язки та відповідальність вчителів у сфері захисту персональних даних учнів регулюється законодавством, етичними стандартами та практичними рекомендаціями, спрямованими на збереження конфіденційності, цілісності та безпеки інформації учнів при використанні сучасних технологій. Основні напрями діяльності вчителів у цьому контексті включають такі аспекти:

1. Виконання норм законодавства. Українське законодавство, зокрема Закон України «Про захист персональних даних», встановлює чіткі вимоги щодо обробки особистої інформації. Вчителі повинні:

- збирати, обробляти, зберігати та передавати персональні дані лише за умови дотримання правових підстав, таких як письмова згода батьків або інших законних представників;
- уникати поширення даних без дозволу, за винятком випадків, що передбачені законом, наприклад, запити правоохоронних органів;
- дотримуватись норм щодо термінів зберігання та умов обробки інформації згідно із чинним законодавством.

2. Забезпечення безпеки даних. Основна роль вчителя полягає у захисті даних учнів від несанкціонованого доступу та можливого витоку особистої інформації. Тривалий захист забезпечується такими заходами, як:

- використання перевірених навчальних платформ замість особистих месенджерів або інших ненадійних каналів зв’язку;
- налаштування складних паролів, шифрування інформації та впровадження двофакторної автентифікації;
- регулярне оновлення програмного забезпечення для уникнення вразливостей системи;
- відмова від застосування сервісів із низьким рівнем захисту даних.

3. Контроль доступу до інформації. Ефективний контроль доступу допомагає зменшити ймовірність неправомірного використання даних.

Вчителі повинні:

- обмежувати доступ до персональної інформації виключно уповноваженим працівникам навчального закладу;
- не передавати дані через небезпечні комунікаційні канали, як-от незашифровані електронні листи або публічні Wi-Fi мережі;
- забезпечувати фізичний захист документів та інших носіїв інформації від неправомірного доступу.

4. Розвиток культури цифрової безпеки у школярів. Одним із ключових обов'язків вчителя є формування в учнів розуміння важливості захисту власних даних. Ця робота включає:

- проведення уроків із цифрової грамотності, де роз'яснюються принципи створення надійних паролів, загроз фішингу і правила безпечного користування мережею;
- інформування про ризики публікації особистої інформації в соціальних мережах чи месенджерах;
- просвітницьку діяльність для підвищення обізнаності щодо ризиків у цифровому середовищі.

5. Дії у разі виявлення порушень безпеки даних. При підозрі або факті витоку персональної інформації вчителі повинні:

- одразу повідомити адміністрацію школи про ситуацію;
- за необхідності звернутися до відповідних органів, таких як Уповноважений з прав людини, що контролює дотримання законодавчих норм у сфері захисту персональних даних;
- сприяти розслідуванню інциденту та брати участь у заходах щодо мінімізації його наслідків.

В умовах стрімкого розвитку цифрових технологій обізнаність і дотримання стандартів захисту персональних даних є важливою частиною професійної діяльності сучасного вчителя. Це допомагає не лише забезпечити правовий захист дітей, але й створити безпечний освітній

простір для всіх. Недотримання вимог щодо обробки та зберігання цих даних може призвести до серйозних юридичних, дисциплінарних, етичних і фінансових наслідків. У сучасному академічному дискурсі відповідальність учителів трактується як комплекс обов'язків, що базуються на нормах чинного законодавства, внутрішніх регламентах освітніх закладів й етичних стандартах. Подальший аналіз розглядає ключові аспекти такої відповідальності з точки зору правового і професійного підходів.

1. Юридична відповідальність педагогів за порушення у сфері захисту персональних даних регламентується нормами законодавства України та може набувати кількох форм:

- Адміністративна відповідальність відповідно до статті 188-39 Кодексу України про адміністративні правопорушення, неналежна обробка персональних даних, зокрема їх незаконне збирання, використання чи розголошення, тягне за собою накладення штрафів. Розмір цих штрафів визначається залежно від характеру та обсягу порушення.
- Кримінальна відповідальність, оскільки умисне розголошення конфіденційної інформації, яке завдало шкоди учням або їхнім родинам, підпадає під статтю 182 Кримінального кодексу України, що передбачає покарання за порушення недоторканності приватного життя. Такі дії можуть каратися штрафами, обмеженням волі або іншими санкціями згідно із законом.
- Цивільна відповідальність, коли у випадках шкоди, спричиненої витоком персональних даних, вчитель чи освітній заклад можуть бути зобов'язані відшкодувати матеріальні або моральні збитки згідно із нормами Цивільного кодексу України. Така компенсація може включати як порушення права на конфіденційність, так і інші пов'язані втрати.

2. Дисциплінарна відповідальність, коли порушення внутрішніх правил школи щодо роботи з персональними даними може тягнути за собою застосування дисциплінарних санкцій. Невиконання положень статуту

навчального закладу або внутрішніх інструкцій може стати причиною винесення догани, тимчасового усунення від виконання обов'язків чи навіть звільнення відповідно до норм Кодексу законів про працю України. Міра дисциплінарної відповідальності залежить від важкості скоєного правопорушення, його наслідків та політики управління в межах закладу освіти.

3. Етична відповідальність вчителя має фундаментальне значення, адже захист персональних даних учнів є важливою частиною професійної етики вчителя. Одним із ключових чинників є збереження довіри учнів та їхніх батьків до педагогічного персоналу і навчального закладу загалом. Порушення конфіденційності здатне підірвати авторитет учителя та репутацію школи, а також створити несприятливу психологічну атмосферу. Моральний обов'язок вчителя передбачає дотримання принципу поваги до приватного життя учнів та їхніх сімей і відповідальне ставлення до використання довіреної їм інформації в межах освітньої діяльності.

4. Фінансові наслідки визвані необережністю дотримання норм захисту даних для самого вчителя, так і для закладу освіти. У випадку судових позовів з боку батьків або опікунів постраждалих учнів освітній заклад або його представники можуть бути зобов'язані сплатити компенсації за матеріальні чи моральні збитки.

У контексті зростаючої цифровізації освітнього процесу захист персональних даних учнів є критично важливим завданням для вчителів. Для забезпечення відповідності законодавчим вимогам, етичним стандартам і практичним потребам пропонується низка рекомендацій, спрямованих на підвищення безпеки даних та мінімізацію ризиків їх компрометації. Ці рекомендації базуються на сучасних підходах до кібербезпеки та практичного досвіду роботи з інформаційними системами в освіті. Практичні поради вчителям шодо **захисту персональних даних учнів наведені на рис.1.**

Рис. 1. Практичні поради вчителям шодо **захисту персональних даних учнів**

Захист персональних даних учнів у сучасній цифровій епосі вимагає від вчителів системного підходу, що включає підвищення кваліфікації, використання безпечних технологій, зменшення обсягу збирання даних і тісну співпрацю з адміністрацією. Реалізація таких практичних рекомендацій допоможе створити безпечніше цифрове середовище, зменшити ризики порушення конфіденційності та підвищити довіру до освітньої системи. Постійне вдосконалення цифрових навичок і дотримання етичних стандартів є важливими для ефективного захисту даних у сучасних умовах.

Список використаних джерел

1. Концепція виховання дітей та молоді в цифровому просторі. Національна академія педагогічних наук України. 2021. 52 с. Режим доступу:

https://ipv.org.ua/wp-content/uploads/2021/08/Kontseptsiia-vykhovannia-ditey-ta-molodi-v-tsyfrovomu-prostori.pdf

2. Професійний стандарт «Вчитель закладу загальної середньої освіти». Наказ Міністерства освіти і науки України від 29 серпня 2024 р. № 1225. м. Київ Режим доступу: https://mon.gov.ua/npa/pro-zatverdzhennia-profesiinoho-standartu-vchytel-zakladu-zahalnoi-serednoi-osvity

3. Права учасників освітнього процесу та дії закладу освіти. Освітній омбудсмен України. Режим доступу: https://eo.gov.ua/

4. Закон України «Про захист персональних даних». від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481. Режим доступу: https://zakon.rada.gov.ua/laws/sho.

5. Кодекс України про адміністративні правопорушення від 07.12.1984 № 8073-X // Відомості Верховної Ради УРСР. 1984.Додаток до № 51.Ст. 1122.Режим доступу: https://zakon.rada.gov.ua/laws/show/80731-10#Text

НАВЧАННЯ В ОБ'ЄКТИВІ: EDTECH ТА ТІНЬОВИЙ ПРОФАЙЛІНГ. Дубняк М.В.

кандидат юридичних наук,
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0001-7281-6568

Цифровізація освіти стрімко трансформує способи здобуття знань, водночас створюючи нові ризики для приватності та безпеки дітей. Освітні технології (EdTech) дедалі активніше інтегрують штучний інтелект, аналітику великих даних, адаптивне навчання та інші інструменти, що дозволяють здійснювати приховане збирання, обробку та використання персональних даних учнів — від академічних результатів до емоційних реакцій, стилів навчання, поведінкових патернів тощо.

Профайлінг — означає будь-яку форму автоматизованого опрацювання

персональних даних, що складається із використання персональних даних для оцінювання окремих персональних аспектів, що стосуються фізичної особи, зокрема, для аналізу або прогнозування аспектів, що стосуються продуктивності суб'єкта даних на роботі, економічної ситуації, здоров'я, особистих переваг, інтересів, надійності, поведінки, місцезнаходження або пересування; (GDPR (ст. 4(4)) [1]. Явище «**тіньового профайлінгу** (shadow profiling) — *це практики збору та обробки персональних, неперсональних та поведінкових даних, з метою доповнення чи створення нового цифрового профілю користувача без його повного усвідомлення, інформування чи прямої згоди. Такий профіль формується на основі як власної активності користувача (зокрема, метаданих, рухів курсора (click paths), cookie-файли та інших технологій збору даних), так і поведінки інших осіб, пов'язаних із ним у цифровому середовищі (наприклад, через спільне використання платформ, соціальні графи або групову взаємодію). Результатом тіньового профайлінгу можуть бути алгоритмічні рішення, що впливають на доступ до освітніх можливостей, оцінювання, психологічну характеристику або прогнозування кар'єрної траєкторії, часто без можливості оскарження чи контролю з боку користувача.*

Наприклад, Proctoring-системи в онлайн-тестуванні, використовують технології розпізнавання облич, аналіз міміки, рухів очей та фонових звуків, порушуючи право дитини на приватність та фізичну недоторканність [2]. EdTech-платформи (наприклад, Google Classroom, ClassDojo, «Мрія») збирають не лише освітні, а й поведінкові метадані які формують персональні «рейтинги поведінки» учнів, що можуть зберігатися та передаватися без контролю батьків, та школи [3,4].

Хоча EdTech платформи для навчання містять «Політики збору та обробки даних» на виконання як національних, так і міжнародних нормативних актів, таких як GDPR, COPPA, FERPA, проте деякі дані збираються «завуальовано» для цілей платформи «надання або покращення освітніх послуг», проте саме з цих даних здійснюється тіньовий профайлінг.

Ми вважаємо, що перелік таких даних є надмірно широким. Для доведення цієї думки проаналізуємо «Політики обробки даних» інтерактивної платформи ClassDojo, яка збирає та обробляє такі дані: *(пронумеровано автором)*: 1. ідентифікатор облікового запису; 2. час активності користувача; 3. аудіофайли, фотографії, відео; 4. тип браузера користувача; 5. рухи курсора і кліків (click paths); 6. дані про поведінку студента; 7. контактна інформація про користувача; 8. інформація про cookie-файли; 9. інформація про технічний пристрій (наприклад, операційну систему, версію апаратного забезпечення, налаштування пристрою); 10. прямі повідомлення та чати в додатку платформи; 11. публікації на сторінці відгуків (включно з текстом, посиланнями, зображеннями); 12. висновки, зроблені платформою щодо споживача/користувача, 13. точні дані геолокації користувача; 14. URL-адреси переходів користувача [3].

Узагальнено, платформа збирає такі дані:

1. Ідентифікаційні дані (п.1, 4, 7, 8, 9, 13, 14);

2. Поведінкові та аналітичні дані (п.2, 5, 6, 12);

3. Особисту та контекстну інформацію (п.3, 10, 11,).

Аналогічною є ситуація з збором та обробкою персональних даних на вебсторінці (державного) освітнього додатка «Мрія» [4].

Отже, зібрані категорії даних дозволяють будувати інтегровані тіньові профілі користувача: наприклад, оцінювати зосередженість (через дані про рухи курсором); комунікативність (через активність у чатах); інтереси (через URL-переходи та дані про поведінку); навіть емоційні характеристики (через фото-аудіо-ведіо та функції Proctoring-системи з технологіями штучного інтелекту, забезпечують аналіз емоційного стану учня — користувача платформи).

Відповідно до принципу мінімізації даних «персональні дані необхідно вважати достатніми і відповідними та обмежити їх мірою необхідності в них з огляду на цілі опрацювання» (ст. 5(1)(c) GDPR [3]. Так викликає сумнів, необхідність збору таких даних як: час активності, cookie-файли, рухи

курсором, точна геолокація, URL-адреси переходів (*показник, який фіксує, чи було переміщення уваги учня (наприклад в процесі виконання контрольних чи домашніх завдань*) на інші веб-сайти *(п.п. з авт.класифікації №: 2, 5, 6, 8, 12, 13, 14)*. Більшість цих даних перевищують обсяг, необхідний для навчання, і можуть бути використані вторинно – для аналітики, комерційних або автоматизованих рішень. Власне, на виконання вимог GDPR, політики «Збору та обробки даних» чітко вказують ці вторинні цілі: для прямого маркетингу, покращення персоналізації, історичних досліджень, встановлення ідентичності, для надання послуги, на яку користувач зареєструвався, розробки нових продуктів [3].

Оскільки, EdTech платформа ClassDojo виступає обробником персональних даних, зібраних у зв'язку з використанням у школі, і тому не приймає рішення за визначення правової підстави згідно зі статтею 6 «Законність опрацювання» GDPR. Таку правові підстави визначає контролер даних (школи, коледжі, університети, інші заклади освіти) [3].

Хоча згідно з GDPR Контролер (школа) – відповідає за мету та правові підстави обробки, а Обробник (платформа) – лише виконує інструкції. Проте на практиці школи часто не мають: достатньої компетентності оцінювати наслідки профайлінгу, ресурсів для проведення Data Protection Impact Assessment (DPIA), контролю над реальними алгоритмами платформи, механізмів впливу на обсяг збору даних платформою. Послуга надається в цілому, без можливості встановлення заборон, до збору певних наборів даних.

Отже, маємо ситуацію з формальною відповідальністю закладів освіти, які при виборі онлайн платформ не сприяють захисту прав дитини. В частині управління даними (наприклад видалення певних категорій даних) ситуація виглядає ще гірше. Згідно Політик – користувач (власник облікового запиту, дитина) може подавати запити про видалення інформації з детальним описом наборів даних, які потрібно видалити. Таке завдання є не реальним для виконання ні для дитини, ні для закладів освіти, адже обсяг даних дуже

великий. А запит «видалити все» може стосуватись конкретного облікового акаунту учня, проте не прогнозних висновків (п. 12), який є результатом аналітичної роботи платформи, того самого результату формування тіньового профілю.

Висновки: У сучасних умовах стрімкої цифрової трансформації освітнього процесу, використання цифрових освітніх платформ є не лише неминучим, а й необхідним елементом сучасної педагогіки. Щодня з'являються нові EdTech-рішення, які в межах автономії суб'єктів освітньої діяльності активно впроваджуються у шкільне й позашкільне навчання – як приватними особами, так і державою. Зокрема, навіть офіційна національна освітня платформа «Мрія» не є винятком, оскільки базові проблеми збору, обробки та захисту даних є спільними для більшості EdTech платформ – незалежно від їхнього походження чи статусу.

Список використаних джерел

1. Загальний регламент про захист даних (GDPR). URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 26.05.2025).

2. Nigam, A., Pasricha, R., Singh, T., & Churi, P. (2021). A systematic review on AI-based proctoring systems: Past, present and future. *Education and Information Technologies*, *26*(5), 6421-6445.

3.ClassDojo Information transparency data poilicy. URL: https://www.classdojo.com/uk-ua/transparency/ (дата звернення: 26.05.2025).

4. Повідомлення про обробку персональних даних на веб-сторінці додатка Мрія. URL: https://mriia.gov.ua/policy.(дата звернення: 26.05.2025).

ВРАЗЛИВОСТІ ДИТЯЧИХ IoT-ПРИСТРОЇВ (РОЗУМНІ ГОДИННИКИ, ІГРАШКИ): ЯК ДАНІ ПОТРАПЛЯЮТЬ ДО ТРЕТІХ ОСІБ? ЧИ БЕЗПЕЧНІ ДИТЯЧІ GPS-ТРЕКЕРИ?

Маринкевич О.

Харківськи національнио університет
внутрішніх справ
ORCID: 0009-0004-2670-7925

Сучасний розвиток дитячих IoT-пристроїв потребує комплексного підходу до підвищення їх безпеки, особливо щодо захисту конфіденційних даних дітей. Перспективним напрямом є перехід на сучасні стандарти шифрування даних, зокрема обов'язкове впровадження WPA3 для Wi-Fi з'єднань та Bluetooth 5.2+ для бездротового зв'язку [1, с. 1-3].

Такі технології забезпечують значно вищий рівень захисту від перехоплення даних порівняно з застарілими протоколами, що досі використовуються у багатьох пристроях. Особливу увагу слід приділити розробці спеціалізованих алгоритмів шифрування, адаптованих саме для дитячих гаджетів, які поєднуватимуть високу продуктивність із максимальним рівнем безпеки [2, с. 1-5].

Важливим кроком у підвищенні безпеки є впровадження обов'язкового наскрізного шифрування (E2EE) для всіх типів переданих даних, включаючи геолокаційну інформацію, голосові повідомлення та відеопотоки. Це дозволить виключити можливість доступу до даних третіх осіб, включаючи самих виробників пристроїв. Паралельно необхідно розвивати інфраструктуру локальних серверів для зберігання даних у юрисдикції країни, де використовується пристрій, що особливо актуально для України. Такі сервери повинні відповідати міжнародним стандартам безпеки та проходити регулярні незалежні аудити [3, с. 2-3].

Законодавче регулювання потребує суттєвого вдосконалення для ефективного захисту дитячих даних. Україні необхідно розробити спеціальні норми, що регулюватимуть вимоги до безпеки дитячих IoT-пристроїв,

враховуючи досвід ЄС у рамках GDPR. Це передбачає встановлення чітких стандартів щодо збору, зберігання та обробки даних, зобов'язання виробників проводити публічні аудити безпеки, а також запровадження суворих санкцій за порушення. Особливу увагу слід приділити регулюванню міжнародної передачі дитячих даних, що потребує узгодження з міжнародними правовими нормами [4, с. 2].

Для підвищення кібербезпеки необхідно розвивати спільні ініціативи виробників, регуляторів та громадськості. Перспективним напрямом є створення єдиного реєстру сертифікованих безпечних пристроїв для дітей, розробка навчальних програм для батьків та вчителів, а також сприяння розвитку вітчизняних розробок у цій сфері. Важливим елементом має стати система оперативного попередження про вразливості та механізми їх усунення, що дозволить оперативно реагувати на потенційні загрози [5, с. 1-2].

Реалізація таких заходів дозволить створити ефективну систему захисту дитячих даних у IoT-пристроях, що поєднуватиме передові технологічні рішення з сучасним правовим регулюванням. Це забезпечить безпеку дітей у цифровому середовищі та сприятиме розвитку інноваційних рішень у сфері дитячих технологій, що відповідають міжнародним стандартам безпеки та конфіденційності [6, с. 4-5].

Список використаних джерел

1. Безпека WiFi: історія небезпеки WEP, WPA і WPA2, URL: https://e-server.com.ua/uk/poradi/bezpeka-wifi-istoriia-nebezpeki-wep-wpa-i-wpa2?srsltid=AfmBOopxDgJYn0aV3NJFKtDNlwy8GhMoLYV584Tlq4rgmp3U7Dky9a9t (дата звернення 21.05.2025).

2. У пошуках безпечного месенджера. URL: https://kr-labs.com.ua/blog/top-secure-and-privacy-messaging-apps (дата звернення 21.05.2025).

3. Відстежуйте текстові повідомлення за допомогою програмного

забезпечення для відстеження SMS, URL: https://spyera.com/uk/ (дата звернення 21.05.2025).

4. Обдурити, відключити GPS трекер – чому це актуально? URL: https://totalapi.io/2024/11/27/obduriti-abo-vidkljuchiti-gps-treker-i-sistemu-monitoringu-ce-mozhlivo/ (дата звернення 21.05.2025).

5. 5 найкращих додатків для зберігання вашої інформації у хмарі. URL: https://www.rbc.ua/rus/styler/naykrashchi-dodatki-zberigannya-vashoyi-informatsiyi-1713394303.html (дата звернення 21.05.2025).

6. Захист персональних даних дитини: на що треба звернути увагу батькам? URL: https://www.radiosvoboda.org/a/zahyst-personalnyh-danyh-dytyny/31603271.html (дата звернення 21.05.2025).

ШЛЯХИ ЦИФРОВІЗАЦІЇ ІНФОРМАЦІЙНОГО СУСПІЛЬСТВА В УКРАЇНІ. Лихоступ С.В., Мороз А.О.

кандидат економічних наук, старший науковий співробітник,
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»;
Державне підприємство «Інформаційні судові системи»

Масове проникнення комп’ютерних технологій у всі сфери життєдіяльності та у побуті потреби сучасного розвитку людства на протязі тривалого часу обумовило у світі появу цифрової трансформації. Етапи еволюції цифрових технологій в Україні включає декілька етапів : перший етап (1990–2000 рр.) – **формування** інфраструктури з метою широкого доступу до Інтернету, використання отриманої інформації для ознайомлення, а не для комунікації чи ведення бізнесу; другий етап (20002010 рр.) – це створення та захист інформаційних електронних ресурсів, упровадження електронного документообігу, оновлення швидкими темпами комп’ютерної

техніки; третій етап (2010–2020 рр.) – впровадженням електронного урядування та наданням публічних електронних послуг, початок розбудова інформаційного суспільства в Україні; четвертий етап розпочався у 2020 році, – використання штучного інтелекту, хмарних технологій, дронів, Інтернету речей та послуг, опрацювання великих масивів даних, застосуванням систем «розумне місто» та «розумне підприємство».

3 березня 2021 року Кабінет Міністрів України затвердив своєю Постановою Національну економічну стратегію на період до 2030 року, у якій вказується на необхідність подальшого розвитку ефективної цифрової сервісної держави та компактних державних інститутів (розвиток цифрової економіки як одного із драйверів економічного зростання України) [2]. Також 3 березня 2021 року Кабінет Міністрів України своїм розпорядженням схвалив Концепцію розвитку цифрових компетентностей і затвердив план заходів щодо її реалізації. Ухвалення цієї Концепції – стратегічний крок вперед у побудові цифрової держави [3, с. 8].

В останні роки Україна стрімко рухалася в напрямку повної цифрової трансформації держави, але через повномасштабну війну пріоритети частково відкоригували. Кабінет Міністрів України уточнив сьогоднішні пріоритети для України і визначив їх як спільний безпечний кіберпростір, відновлення інфраструктури і телекомунікацій та інвестиції в діджиталізацію економіки. Тому останнього часу основні напрямки розвитку цифрових технологій визначають реалізацію програми «Держава в смартфоні», протистояння агресору у кіберпросторі, сприяння розвитку IT-сектора, організація ефективної взаємодії між органами публічної влади, населенням, українськими військовими, інститутами громадянського суспільства.

В теперішніх умовах Україна продовжує інтегруватися в європейський цифровий простір. Під час Конференції EURODIG 2025 яка відбулося в м. Страсбург, Франція Україна приєдналася до Рамкової конвенції Ради Європи про штучний інтелект (ШІ), права людини, демократію та верховенство права. Документ визначає принципи, яких держава має

дотримуватися у формуванні законодавства та застосуванні ШІ-продуктів у публічному секторі: повага до людської гідності, прозорість, недискримінація, захист приватності, надійність і безпека. Принципи Конвенції опосередковано опиратимуться на бізнес: держава створюватиме ініціативи для приватного сектору, які допоможуть компаніям адаптувати принципи в розробку власних продуктів. Конвенція набере чинності після її ратифікації Верховною Радою України. Раніше Конвенцію підписали 15 урядів, серед яких Велика Британія, США, Канада, ЄС, Ізраїль, Японія та інші технологічні держави.

Отримання переваг від поширення цифровізації потребує виваженого підходу до впровадження цифрових технологій в усіх сферах, з урахуванням особливостей процесів цих процесів та ще й проблем і недоліків, які існують сьогодні, як, наприклад, низький рівень цифрової грамотності населення, недостатньо розгалужена ІТ-інфраструктура, недостатня кількість відповідних фахівців та інше.

Список використаних джерел

1. Баран М. Взаємодія громадянського суспільства та органів влади: сучасний стан, проблеми, перспективи / *Державне управління: удосконалення та розвиток.* 2013. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=645:

2. Національна економічна стратегія на період до 2030 року: схв. постановою Кабінета Міністрів України від 03 березня 2021 р. № 179. URL: https://www.kmu.gov. ua/npas/pro-zatverdzhennya-nacionalnoyi-eko-a179.

3. Хаустова М.Г. Поняття цифровізації: національні та міжнародні підходи. *Право та інновації.* № 2 (38). 2022. С. 7-18.

4. Київська школа економіки. Понад $54 млрд – збитки житлового фонду України внаслідок повномасштабної війни на кінець травня 2023 року. 2023. 26 червня. URL: http://surl.li/iuvhz

5. What is Digital Transformation? Theagileelephant.com. website. URL: http://www.thea-gileelephant.com/what-is-digital-transformation (the date of

application: 27.03.2021).

6. Мельник Л.Г., Карінцева О.І., Кубатко О.В., Сотник І.М., Завдоєва Ю.М. Цифровізація економічних систем та людський капітал: підприємство, регіон, народне господарство. *Mechanism of Economic Regulation.* 2020, No 2. С. 9-28.

7. Оцінка соціальних ризиків в регіонах України як підстава для прийняття управлінських рішень щодо їх подолання. URL: http://old.niss.gov.ua.

8. Оцінка соціальних ризиків в регіонах України як підстава для прийняття управлінських рішень щодо їх подолання. URL: http://old.niss.gov.ua.

ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНИХ ПРАВ ТА БЕЗПЕКИ ДИТИНИ В УКРАЇНІ. Радзієвська О.Г.

кандидат юридичних наук, старший дослідник,
Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0003-3813-3987

Розвиток інформаційно-комунікаційних технологій та їх швидке впровадження у виробничу, фінансову, управлінську, освітню та інші сфери діяльності сучасного суспільства призводить до цифровізації суспільних процесів та суттєвих змін у житті людей. Будь-яка діяльність нині нерозривно пов’язана з інформацією, інформаційними технологіями та інформаційним простором. Відповідно, складова інформаційної безпеки сьогодні набуває дедалі більшого значення і стосується усіх без виключення сфер діяльності як на індивідуальному, так і на державному чи міжнародному рівнях.

Зважаючи на те, що серед пріоритетів національних інтересів України у рамках забезпечення національної безпеки поряд із захистом прав, свобод і законних інтересів громадян є суспільний розвиток та розвиток людського капіталу України, зокрема через модернізацію освіти і науки, охорони здоров'я, культури, соціального захисту, подальша трансформація та цифровізація цих сфер діяльності неминуча. Посилення ролі електронних комунікацій у повсякденному спілкуванні, роботі та навчанні підвищує ступінь вразливості процесів обробки інформації, створює додаткові ризики для захисту чутливої інформації, особливо персональних даних людини. Це створює необхідність як для держав, так і для бізнесу розроблення та впровадження додаткових механізмів та заходів для належного функціонування і захисту інформаційних ресурсів та систем.

Актуалізація та загострення інформаційного протистояння на регіональному, державному та міжнародному рівнях, зміщення акцентів у веденні воєнних конфліктів на комплексне використання воєнних і невоєнних інструментів принципово змінює характер трансформаційних процесів у сучасному суспільстві та провокує виникненням новітніх викликів та загроз для людини, суспільства, держави. Загрози в інформаційній сфері стають все більш небезпечними, а негативний інформаційний вплив на індивідуальну та суспільну свідомість дедалі суттєвішими.

Особливу небезпеку інформаційні загрози становлять для дитини, як суб'єкта суспільних відносин, який потребує особливого захисту і піклування з боку держави та суспільства відповідно до законодавства України і норм міжнародного права. Сучасні трансформаційні процеси в інформаційній сфері суттєво впливають на формування свідомості дитини та її сприйняття навколишнього світу, а інформація негативного змісту здатна викривляти світогляд дитини, підмінювати її морально-етичні цінності, заважати формуванню цілісної та гармонійної особистості. Широке використання дитиною цифрового простору для реалізації освітніх, комунікативних та розважальних потреб ставить під загрозу її приватність, а також

правомірність використання її персональних даних та конфіденційної інформації. Це стосується:

- правомірності збору персональних даних та конфіденційної інформації про особу, особливо в мережі Інтернет, та соціальних медіа;
- правомірності використання персональних даних та конфіденційної інформації про особу;
- належного захисту персональних даних при зберіганні та обробці.

Про це свідчать дані щорічних доповідей про стан додержання та захисту прав і свобод людини і громадянина в Україні Уповноваженого Верховної Ради України з прав людини у 2022, 2023, 2024 роках [1; 2; 3]. Зокрема, 60% звернень до Уповноваженого Верховної Ради України з прав людини в інформаційній сфері за 2022 рік пов'язано з незаконною обробкою персональних даних, 12% – стосувалися порушення процедури обробки персональних даних суб'єктами владних повноважень [1].

Необхідність ідентифікації на різних платформах та у додатках змушує дитину надавати персональні дані для реєстрації. Крім того відбувається автоматичний збір даних про особу. Великі дані (BIG DATA), або автоматично сформовані дані про користувача, його вподобання, інтереси, зібрані методом аналізу його діяльності в мережі, разом з поширеною ним же інформацією про себе, у тому числі фото, відео, становлять живий інтерес для бізнесу, політики, соціальних та комерційних проектів. Ця інформація стає надзвичайно цінним ресурсом знань для будь-якої компанії, у тому числі й для створення персоналізованої (таргетованої) реклами. Наприклад, інноваційні підходи сучасного маркетингу передбачають використання великих даних при створенні цифрового профілю об'єкта для подальшого використання у просуванні товарів і послуг у мережі.

З іншого боку великі дані є незамінним інструментом в інформаційному протистоянні та інформаційних війнах. Маніпулювання з інформаціє збільшує об'єми недостовірної та викривленої інформації в інформаційному просторі, підвищує кількість негативних та маніпулятивних

впливів на свідомість громадян. Такі дії порушують право особи на захист від маніпулювання свідомістю, право на захист від недостовірної інформації, а також ставить під загрозу повноцінність реалізації ним права вибору. Правомірність використання даних, зібраних про користувача в мережі, є сумнівною, оскільки не відображена в національному законодавстві. Крім того використання великих даних для проведення спеціальних інформаційних операцій з метою отримання переваг також може призвести до завдання суттєвої шкоди суспільству і державі та становить реальну загрозу для безпеки самої дитини.

Постають суттєві питання щодо захисту персональних даних та правомірності їх автоматичного збирання та використання в мережі. Правовою підставою для використання персональних даних у контексті продажу й просування в Інтернеті є згода суб'єкта персональних даних відповідно до Закону України «Про захист персональних даних» [4]. Необхідною умовою для отримання згоди суб'єкта персональних даних на обробку його персональних даних, відповідно до Закону, є інформування його про порядок обробки даних, зокрема, про володільця персональних даних, склад і зміст зібраних персональних даних, права, мету збору, а також про осіб, яким буде передано персональні дані. При зміні мети обробки персональних даних необхідним є повторне отримання згоди суб'єкта персональних даних на обробку його персональних даних. Однак на практиці надана інформація про порядок обробки персональний даних, зібраних за допомогою файлів cookies, є недостатньою, а повторний запит на згоду суб'єкта персональних даних взагалі не здійснюється.

Крім того, інформація, зібрана про особу з використанням автоматичних можливостей мережі, жодним нормативним документом в Україні офіційно не визнана персональними даними. Тоді як в Європейському Союзі інформація, зібрана з допомогою файлів cookies, вважається персональними даними відповідно до Загального регламенту щодо захисту даних 2016/679 (GDPR) [5] та Директиви про обробку

персональних даних та захист конфіденційності в секторі електронних комунікацій 2002/58/EC (ePrivacy Directive) [6].

Низка проблем залишається й у питаннях реалізації права громадян на приватність у цифровому вимірі, зокрема у соціальних мережах, мережі Інтернет, при здійсненні відеоспостереження у громадських місцях.

Впровадження ШІ, який сьогодні демонструє властивості швидкого самонавчання, без належного контролю може нести загрозу всьому людству. ШІ дуже швидко саморозвивається, на що людський мозок не здатний через біологічні особливості організму, зокрема через неможливість швидко передавати, а від так, і опрацьовувати інформацію та не має миттєвого доступу до всіх даних, які мітить глобальна мережа. Системи з використанням ШІ викликають занепокоєння щодо їх безпеки без належного правового регулювання та необхідного контролю зі сторони людства за надто швидким процесом саморозвитку. Спонтанне та неконтрольоване впровадження нових технологій призведе до відсутності узгодженості у діяльності між новими системами з використанням ШІ та тими, що існували раніше, що унеможливить їх нормальне функціонування. Відсутність належного рівня правого забезпечення розробки, впровадження та використання сучасних технологій створить підґрунтя для зловживань і протиправного використання їх можливостей. У кінцевому рахунку ці чинники суттєво впливатимуть на можливість безперешкодної реалізації прав дітей в інформаційному суспільстві та призведе до зниження рівня їх захищеності.

Певні складності під час війни спостерігаються і у питаннях реалізації права особи на доступ до інформації. Зокрема, це стосується:

- обмеження доступу до публічної інформації;
- обмеження доступу до суспільно важливої інформації;
- обмеження доступу до інформації навчального характеру та порушення права на освіту на окупованих територіях.

Великою проблемою, яка очікує на нашу державу у найближчому майбутньому є інформаційна реінтеграція дітей з окупованих територій. Сьогодні маємо чотири основні категорії дітей, які потребують окремих підходів та особливих стратегій реінтеграції в інформаційно-ідеологічне поле нашої держави, а саме:

- діти, які знаходяться на окупованих територія з 2014 року;
- внутрішньо переміщені особи;
- діти, які виїхали за кордон;
- діти, яких насильно вивезли на територію РФ.

Основні напрямки державної політики щодо інформаційної реінтеграції тимчасово окупованих територій сьогодні стосуються Донецької і Луганської областей та Автономної Республіки Крим. Вони викладені у Стратегії інформаційної реінтеграції Донецької та Луганської областей [7] та Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя [8], а також деталізовані у Планах щодо їх реалізації, розроблених Урядом України. Зважаючи на значне розширення окупованих територій, а також враховуючи кількість дітей, які вимушено виїхали за межі України, чи були примусово вивезені на територію РФ, необхідно напрацьовувати нові напрями та підходи у питаннях інформаційної реінтеграції. Подальших системних напрацювань потребують не лише питання інформаційної реінтеграції дітей з окупованих територій в українське суспільство, але й підтримка та повернення в Україну тих, хто опинився в силу обставин за межами країни.

Це далеко не повний перелік актуальних проблемних питань, які постають перед суспільством сьогодні через впровадження нових інноваційних технологій, цифровізації суспільства і новітніх безпекових загроз у світі та в Україні. Аналіз сучасного стану забезпечення інформаційної безпеки в Україні дає підстави стверджувати, що система захисту інформаційної безпеки дитини в Україні залишається недостатньо ефективною і такою, що потребує кардинальної трансформації відповідно до

сучасних викликів і загроз в інформаційній сфері. Правове забезпечення інформаційної безпеки дитини розвивається фрагментарно, ситуаційно, за відсутності системного підходу та єдиної інформаційної політики держави, що знижує ефективність протидії інформаційним викликам і загрозам та ускладнює організацію превентивних заходів з їх упередження. Як приклад, відсутність єдиної державної інформаційної політики практично залишає без важелів впливу центральні та місцеві органи виконавчої влади щодо профілактики інформаційних викликів і загроз. Тоді як питання захисту інформаційної безпеки дитини в сучасному інформаційному суспільстві у коротко- і довготривалій перспективі буде залишатися вкрай важливою складовою системи забезпечення інформаційної безпеки держави та одним із ключових елементів забезпечення національної безпеки України.

З огляду на зростання рівня небезпек для дитини в інформаційному суспільстві, виникає необхідність використання правового моделювання у правотворчій та правозастосовній практиці, що надасть можливість запобігти дії негативних інформаційних впливів на її свідомість та забезпечити безпеку. Розроблення превентивної правової моделі у цій сфері є можливим за умови використання методів правового моделювання розвитку суспільних процесів, що ґрунтуються на всебічному аналізі та прогнозуванні реальних і потенційних загроз інформаційній безпеці людини, суспільства та держави. Для цього необхідним є створення інтегрованої системи оцінки інформаційних загроз. Актуальним у цьому питанні видається опрацювання і впровадження в Україні розробленої Європолом системи оцінювання загроз організованої злочинної діяльності в мережі Інтернет (IOCTA). Також доцільно проаналізувати практику держав - членів НАТО у питаннях створення і розвитку інститутів, що відповідають за інформаційно-психологічну безпеку.

При розбудові та забезпеченні функціонування системи захисту прав та безпеки дитини в інформаційному просторі необхідно зважати на те, що згідно із законодавством України відповідальність за її реалізацію лежить не

лише на державі та її інституціях, які повинні створювати відповідні умови цієї протидії, але й на кожному громадянинові України, а убезпечення дитини в інформаційному просторі законодавчо покладається на батьків або осіб, що їх замінюють і на державні органи та інституції, на які покладено функції по охороні дитини. Тому вагомою складовою системи захисту інформаційної безпеки дитини є удосконалення професійної підготовки у сфері інформаційної безпеки, впровадження загальнонаціональних освітніх програм з інформаційної та медіакультури, інформаційної грамотності із залученням громадянського суспільства і бізнесу та відповідного відображення зазначеного у національному законодавстві.

Список використаних джерел:

1. Щорічна доповідь про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2022 році Уповноваженого Верховної Ради України з прав людини URL: https://ombudsman.gov.ua/report-2022/informatsiini-prava#doctup-do-informatsii

2. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2023 році. URL: https://ombudsman.gov.ua/storage/app/media/uploaded-files/Щорічна_доповідь_Уповноваженого_за_2023_рік.pdf

3. Щорічна доповідь Уповноваженого Верховної Ради України з прав людини про стан додержання та захисту прав і свобод людини і громадянина в Україні у 2024 році. URL: https://www.ombudsman.gov.ua/storage/app/media/uploaded-files/Щорічна_доповідь_Уповноваженого_2024_році.pdf

4. Про захист персональних даних: Закон України від 1 червня 2010 р. № 2297-VI / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text

5. Регламент Європейського парламенту і Ради (ЄС) 2016/679 про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про

вільний рух таких даних, та про скасування Директиви 95/46/ЄС (Загальний регламент про захист даних) від 27 квітня 2016 р. / Верховна Рада України. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

6. Директива Європейського Парламенту і Ради (ЄС) № 2002/58 від 12 липня 2002 року «Про обробку персональних даних та захист таємниці сектора електронних комунікацій». URL: http://zakon3.rada.gov.ua/laws/show/994_b34

7. Про схвалення Стратегії інформаційної реінтеграції Донецької та Луганської областей: Кабінету Міністрів України, Розпорядження, Стратегія від 26.07.2018 № 539-р. URL: https://zakon.rada.gov.ua/laws/show/539-2018-%D1%80#top

8. Про схвалення Стратегії інформаційної реінтеграції Автономної Республіки Крим та м. Севастополя: Кабінету Міністрів України, Розпорядження, Стратегія від 27.12.2018 № 1100-р. URL: https://zakon.rada.gov.ua/laws/show/1100-2018-%D1%80#Text

КІБЕРБУЛІНГ: ЯК ПРОТИСТОЯТИ. Сороко Н.В.

кандидат педагогічних наук,
Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0002-9189-6564

Активний розвиток інформаційно-комунікаційних технологій викликав суттєву проблему суспільства як кібербулінг. У документах UNICEF це поняття визначається як «агресивні дії з використанням цифрових технологій: соцмереж, месенджерів, ігор чи електронної пошти для залякування, приниження чи переслідування людини» [1]. Він може проявлятися у вигляді образ, погроз, поширення фейкової інформації або розголошення приватних даних.

За даними Департамент кіберполіції Національної поліції України,

основними видами кібербулінгу є [2]:

- систематичні погрози, в тому числі у месенджерах та соціальних мережах (часто анонімні);

- цілеспрямований злам облікових записів потерпілого для подальшого використання отриманої особистої інформації для шантажу або морального насильства;

- сталкінг (від англ. Stalking – переслідування) – небажана нав'язлива увага до людини, що може проявлятися, зокрема, у відстежуванні жертви та її онлайн-активності, погрозах та залякуванні;

- хепіслепінг (від англ. happy slapping – «веселі ляпаси») – насильницькі дії щодо людини під запис з можливим подальшим розміщенням в інтернеті або поширенням таких записів серед знайомих постраждалої особи;

- розповсюдження принизливої, інтимної або неправдивої інформації або інтернет-контенту про жертву;

- умисне розміщення провокативних повідомлень для розпалювання конфліктів між учасниками онлайн-спільнот;

- грумінг (від англ. grooming – залицяння) – встановлення дорослими довірливих стосунків з неповнолітніми, в тому числі через Інтернет, для подальшого вступу з ними в інтимний зв'язок, вчинення сексуального насильства, шантажування або залякування.

Це питання почало розглядатися з 1999 року [3]. Значне зростання досліджень з приводу кібербулінгу полягає на період з 2015 року по 2023 рік. Науковці пояснюють його соціальними, технологічними та політичними факторами. Так, після 2015 року смартфони стали доступнішими для дітей і підлітків у всьому світі. Крім цього соціальні мережі (Instagram, Snapchat, TikTok) почали активно заміщати традиційні засоби спілкування, що створило нові ризики для кібернасильства. У 2015-2017 роках багато країн прийняли спеціальне законодавство проти кібербулінгу (наприклад, Італія, Франція, Фінляндія); стало більше національних і міжнародних грантів на

дослідження цієї теми (наприклад, EU Horizon 2020, Erasmus+, UNICEF програми).

Серед ініціатив щодо запобіганню кібербулінгу слід звернути увагу на проєкт Safety Net, що заснований у межах програми EU Horizon 2020 [4].

В Україні постійно діє Інтернет-Асоціація України (ІнАУ) [5], яка є партнером європейської ініціативи щодо безпечного Інтернету та організатором Дня безпечного Інтернету в Україні. Вона координує кампанії з профілактики кібербулінгу та поширює матеріали серед шкіл, батьків і молоді.

Крім вищезазначеного в Україні діє служба гарячої лінії з приводу кібербулінгу, куди можна звернутися зі скаргою на кібербулінг та отримати поради: за електронною адресою callcenter@cyberpolice.gov.ua, або за номером телефону 0 800 505 170.

Отже, варто зазначити, що першим кроком щодо протистояння кібербулінгу є звернення за допомогою до когось, кому молода особа довіряєте, наприклад, до батьків, близького члена родини або іншої дорослої людини, яка має її довіру. Якщо цькування відбувається на соціальній платформі, можна заблокувати цькувача та офіційно повідомити про його поведінку на самій платформі. Компанії соціальних мереж зобов’язані забезпечувати безпеку своїх користувачів.

Активна діяльність керівництва школи, вчителів, батьків, державних установ та ін. проти кібербулінгу є важливим щодо підтримки здоров’я молоді країни.

Список використаних джерел

1. UNICEF. Cyberbullying: What is it and how to stop it. URL: https://www.unicef.org/end-violence/how-to-stop-cyberbullying.

2. Департамент кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/article/kiberpolicziya-informuye-pro-vidpovidalnist-za-vchynennya-riznyx-vydiv-bulingu-800/

3. Arti Singh, Abderahman Rejeb, Hunnar Nangru, Smriti Pathak (2024).

Global research trends on cyberbullying: A bibliometric study, Computers in Human Behavior Reports, 16, 100499. https://doi.org/10.1016/j.chbr.2024.100499.

4. Safety Net. URL: https://www.saferinternet.org

5. Інтернет-Асоціація України. URL: https://inau.ua/

ЦИФРОВА ВРАЗЛИВІСТЬ НЕПОВНОЛІТНІХ ПІД ЧАС РОЗСЛІДУВАННЯ ДОМАШНЬОГО НАСИЛЬСТВА.

Шаповал К.А.

доктор філософії у галузі права,
Харківський національний університет внутрішніх справ
ORCID ID: 0000-0003-1826-5261

У період активної цифровізації та впровадження цифрових технологій у різні сфери життя захист прав і свобод дитини, особливо потерпілої від домашнього насильства, набуває нових викликів. Науковці звертають увагу на формування нового виміру дитячої вразливості, яка охоплює не лише фізичні чи психологічні загрози, але й цифрові ризики – зокрема, витік, поширення чи зловживання персональними даними в межах досудового розслідування.

У сучасних умовах діти можуть ставати не лише жертвами домашнього насильства, а й суб'єктами цифрової віктимізації – через витік персональних даних, кібербулінг, переслідування у соціальних мережах, месенджерах, хмарних сервісах тощо. Така вразливість має комплексний характер – вона зумовлена одночасно правовими, психологічними та технічними чинниками.

Відповідно Закону України «Про захист персональних даних», персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована [1]. На міжнародному рівні питання захисту персональних даних дітей регламентуються, зокрема: ст. 16 Конвенції ООН про права дитини, яка

гарантує право на приватне життя [2]; Регламентом європейського парламенту і ради (ЄС) 2016/679 (Загальний регламент про захист даних – GDPR), ст. 38 якого передбачає спеціальні гарантії щодо обробки даних дітей.

Під час дії особливих правових режимів, у тому числі воєнного стану й ураховуючи загальний стресовий стан (психологічне напруження) населення, фіксується зростання кількості випадків домашнього насильства, зокрема щодо дітей. За таких обставин вважаємо за необхідне наголосити на деяких його особливостях розслідування:

– значна кількість доказів має цифрову природу (листування, відеозаписи, фотоматеріали, записи з камер, повідомлення в месенджерах тощо);

– дитина може стати об'єктам цифрового нагляду, контролю або шантажу з боку кривдника;

– сліди насильства іноді поширюються в мережі інтернет, що може спричинити повторну травматизацію.

У підтвердження поширення цифровізації доказової бази слід наголосити, що для захисту своїх прав, порушених унаслідок домашнього насильства в цифровому середовищі, постраждала особа повинна самостійно фіксувати факти протиправної поведінки. Зокрема, зберігати електронне листування (на електронній пошті, у месенджерах, соціальних мережах), дописи, робити скриншоти екранів/моніторів гаджетів, записувати розмови тощо, тобто зафіксувати факт учинення насильства. Надалі така інформація може бути використана як доказ факту вчинення насильства і використана у ході досудового розслідування та судового розгляду [3, с. 540].

У процесі досудового розслідування може виникнути ризик розкриття конфіденційної інформації про дитину, зокрема під час допиту, судово-психологічної експертизи, вилучення цифрових носіїв або моніторингу онлайн-активності. Поширення такої інформації може мати травмуючий вплив на дитину, сприяти соціальному цькуванню, висміюванню, погрозам

або іншій повторній віктимізації. Відсутність чітко прописаних алгоритмів конфіденційної обробки персональних даних лише ускладнює захист прав неповнолітніх.

Поняття цифрової вразливості, на нашу думку, охоплює сукупності загроз, зумовлених:

– низьким рівнем цифрової грамотності;

– неусвідомленням дитиною ризиків поширення персональних даних;

– високим рівнем залежності від цифрових платформ (соціальні мережі, ігри, освітні платформи тощо);

– відсутностю ефективних правових механізмів реагування на цифрову шкоду в реальному часі.

Ця вразливість особливо посилюється у випадках, коли дитина стає учасником (особливо – потерпілим) у кримінальному провадженні, що стосується домашнього насильства. У такому випадку скоординована взаємодія слідчого, прокурора, психолога, соціального працівника, медика чи представника освітнього закладу має забезпечувати баланс між доказовою цінністю інформації та захистом особистих даних дитини, конфіденційністю її джерела.

У межах кримінального процесу ці засади реалізуються через:

– вимоги кримінально-процесуальної форми;

– обмежений доступу до матеріалів провадження;

– особливості умов проведення слідчих (розшукових) дій за участю дітей.

Так, вважаємо необхідним зазначити про найбільш поширену СРД – допит та його особливості. Отже, під час проведення допиту неповнолітнього в ході досудового розслідування кримінальних правопорушень пов’язаних з домашнім насильством, слід виділити наступні аспекти:

– процесуальний – суворе дотримання вимог закону щодо підготовки, проведення та фіксації допиту;

– психологічний – урахування вікових (чи вміє самостійно висловлювати думку, можливо запропонувати зобразити малюнок), гендерних особливостей, соціально-психологічної характеристики (яка включає визначення рівня трагедії, що сталася для допитуваного, рівень освіти), темпераменту допитуваного;

– етичний – високоморальна, тактовна поведінка слідчого (прояв співчуття);

– педагогічний (виховний) – допит проводять на основі індивідуального підходу, вияві чуйності до особистості неповнолітнього;

– тактичний – використання тактичних прийомів допиту залежно від ситуації, що складається [4, с. 151].

Також ураховуючи вищезазначене, вважаємо необхідним доповнити цей перелік ще одним аспектом:

інформаційно-безпековий – забезпечення цифрової захищеності персональних даних неповнолітнього, що передбачає: конфіденційність аудіо-відео записів СРД; контроль доступу до цифрових носіїв, недопущення витоку, поширення чи використання інформації.

Зокрема, інтерв'ювання дітей рекомендовано здійснювати в умовах «Зеленої кімнати» або за моделлю «Барнахус». Необхідним є створення в органах досудового розслідування внутрішніх регламентів з обмеженим доступом до цифрових даних неповнолітніх (журнали доступу, аудити, шифрування), а також використання спеціальних форматів цифрової фіксації (анонімізація, візуальні/звукові фільтри під час відеодопиту тощо).

До основних принципів організації досудового розслідування з урахуванням цифрової вразливості слід віднести:

принцип мінімізації втручання, тобто залучення дитини до процесу розслідування лише за наявності аргументованої необхідності, використання зафіксованих свідчень (ст.ст. 224, 226 КПК України);

принцип анонімізації та конфіденційності, а саме обмеження доступу до персональних даних дитини, використання псевдонімів, технічних засобів

захисту, проведення допиту не в приміщенні правоохоронного органу тощо;

принцип технічної безпеки даних – шифрування, обмежений доступ, аудит інформаційних систем;

принцип міжвідомчої взаємодії – участь психологів, соціальних працівників, медиків у межах моделі «Барнахус» або «Зеленої кімнати».

З метою недопущення спричинення шкоди неповнолітнім через недбале використання цифрових технологій необхідним є проведення навчань для слідчих щодо етичної та правової роботи з персональними цифровими даними дітей та запровадження спеціальних цифрових інструментів (реєстри, хмарні сховища, електронні кейс-менеджери) для роботи з вразливими категоріями потерпілих.

Таким чином, організація досудового розслідування має враховувати не лише доказову цінність цифрових слідів, а й уникати вторинної віктимізації дитини. У кримінальних провадженнях щодо домашнього насильства варто враховувати не лише фізичну й психологічну вразливість дитини, а й її цифрову беззахисність.

Лише поєднання криміналістичної доцільності, правозахисного підходу та цифрової обізнаності може забезпечити як ефективність, та і законність слідчих (розшукових) дій у таких провадженнях. Документування фактів домашнього насильства повинно здійснюватися з дотриманням принципів дитиноцентризму, тобто орієнтування на дитину, пропорційності та цифрової безпеки. Розробка національних стандартів захисту цифрової інформації про неповнолітніх у кримінальному процесі є одним з пріоритетних напрямів сучасної криміналістичної науки та практики.

Список використаних джерел

1. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI. *БД «Законодавство України»* / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2297-17#Text (дата звернення: 26.05.2025).

2. Конвенція про права дитини від 20.11.1989. *БД «Законодавство*

України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/995_021#Text (дата звернення: 26.05.2025).

3. Шаповал К. А. Особливості використання цифрових технологій у розслідуванні кримінальних правопорушень, пов'язаних із домашнім насильством. *Актуальні питання судової експертології, криміналістики та кримінального процесу :* мат-ли VI міжнар. наук.-практ. конф. (Київ, 20.12.2024) / за заг. ред. Н. В. Нестор. – Київ : Видавництво Ліра-К, 2024. С. 538-542. URL:

4. Шаповал К. А. Методика розслідування вбивств, вчинених у зв'язку з домашнім насильством : дис. … докт. філософії : 081 Право. Харків, 2023. 224 с.

ЦИФРОВА ЕРА І ФІЛОЛОГІЧНА ВІДПОВІДАЛЬНІСТЬ: ФОРМУЄМО КУЛЬТУРУ МОВЛЕННЯ І БЕЗПЕЧНОЇ ПОВЕДІНКИ В МЕРЕЖІ. Ющенко В.В.

ВСП «Фаховий коледж транспорту та комп'ютерних технологій Національного університету «Чернігівська політехніка»

Цифрові технології невідворотно трансформували наше повсякдення: спосіб спілкування, навчання, пошуку інформації, вираження думок. Разом з цим постали нові виклики: знеособлення комунікації, поширення мови ворожнечі, кібербулінг, маніпуляції, порушення права на приватність. Особливо вразливою категорією в цьому контексті залишаються діти та молодь – ті, хто проводить у мережі значну частину свого життя, часто не усвідомлюючи всіх ризиків.

Філолог, який працює у закладі фахової передвищої освіти, сьогодні вже не лише провідник у світ слова й літератури, а й медіаграмотний педагог, здатний сформувати в здобувачів освіти навички безпечного й відповідального мовлення в цифровому просторі.

Уміння чітко і відповідально формулювати думки, дотримуватися норм

етикету онлайн-спілкування, виявляти емпатію й уникати агресії – усе це елементи мовної культури, яка стає основою цифрової безпеки. Нерідко здобувачі освіти не вважають публікацію світлини в соцмережі або коментар у чаті чимось особливо важливим. Проте кожен допис – це елемент цифрового сліду, який формує особистий образ і впливає на безпеку, репутацію, взаємини.

Під час обговорення теми «Мова в інтернеті: стиль, відповідальність, ризики» один зі здобувачів поділився історією, як його невдалий жарт у коментарі під фото викликав шквал критики й образ. Такий випадок став точкою відліку для глибшого осмислення: що ми пишемо в мережі – важить.

Заняття з української мови та літератури дають чудову можливість не тільки розвивати мовні компетентності, а й виховувати медіакультуру. Наприклад, аналізуючи публіцистичні тексти, рекламні гасла, блоги, можна навчати здобувачів розпізнавати маніпулятивні техніки, фейки, мовну агресію.

Працюємо над критичним мисленням через завдання:

- проаналізуй емоційне забарвлення заголовків новин;
- напиши відповідь на провокативний коментар, зберігаючи доброзичливий тон;
- сформулюй правила безпечного мовлення в соцмережах для підлітків.

Такі завдання не лише розвивають мовлення, а й стимулюють відповідальне ставлення до публічної комунікації.

Питання захисту персональних даних – не лише технічне чи правове, а й мовне. Адже все починається зі слів: що і як ми про себе повідомляємо, які згоди даємо, чи читаємо умови використання сервісів. На заняттях доречно аналізувати формулювання угод користувача, онлайн-опитувань, типових запитів чат-ботів, акцентуючи: коректність мови, прозорість намірів.

Наприклад, після обговорення теми «Особиста інформація в інтернеті» здобувачі освіти виконували практичне завдання: укласти пам’ятку для

однолітків під назвою «10 фраз, які не варто писати в соцмережах». Під час роботи групи обговорювали не лише мовне оформлення висловлювань, а й ризики, які вони можуть нести для безпеки, репутації чи емоційного стану. У результаті до переліку потрапили такі приклади фраз:

- «Я вдома один/одна»
- «Ми з родиною поїхали у відпустку на тиждень»
- «Ось фото мого нового паспорта/студентського»
- «Мені набридло жити. Ніхто мене не розуміє»
- «Пишіть у приват – скину номер картки»
- «Це він/вона винен(-на), що в нас так сталося!»
- «Я сьогодні не піду на пари – викладач усе одно нічого не пояснює»
- «Не люблю, коли до нас приходить інспектор – він такий...»
- «Давайте його зацькуємо – він того заслужив!»
- «Якщо ти не з нами – ти проти нас».

Після презентації роботи здобувачі дійшли висновку, що мовна необачність у цифровому просторі може мати реальні наслідки: від витоку особистих даних до морального тиску чи навіть кримінальної відповідальності. Це завдання дало змогу поєднати знання з мови, етики та цифрової грамотності.

Філолог у цифрову епоху виконує місію, що значно ширша за традиційне мовне навчання. Ми не лише вчимо правильно писати й говорити – ми вчимо відповідально бути в публічному просторі. Слово має силу: і лікувати, і ранити, і захищати.

Цифрова епоха диктує нові вимоги до професійної ролі філолога: сьогодні він не лише викладач мови та літератури, а й провідник у світ свідомої комунікації, медіаграмотності та цифрової етики. Формуючи мовну культуру здобувачів освіти, ми не просто вчимо грамотно висловлюватися – ми вчимо мислити критично, дотримуватися моральних орієнтирів і бути відповідальними в онлайн-просторі.

Інтеграція тем цифрової безпеки, захисту особистої інформації та етичного мовлення в освітній процес з української мови й літератури є не лише доречною, а й необхідною. Такі міжпредметні акценти допомагають молоді орієнтуватися в інформаційному світі, оберігати власні кордони, з повагою ставитися до інших і розуміти силу слова – не лише в літературному, а й у соціальному вимірі.

Отже, філологічна відповідальність у цифрову добу – це про людяність, осмисленість і захист через слово.

Список використаних джерел

1. Ворон А.А. Культура фахового мовлення. К.: ВЦ «Академія», 2007. 254 с.

2. Про захист персональних даних : Закон України від 01.06.2010 № 2297-VI // Відомості Верховної Ради України. 2010. № 34. Ст. 481.

3. Український інститут медіа і комунікації. Дослідження цифрової грамотності українців. URL: https://mediacom.org.ua/digital-literacy (дата звернення: 20.05.2025).

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ДІЯЛЬНОСТІ ВІДЕОБЛОГЕРІВ У КРАЇНАХ ЄС. Заславська Л.В.

Державна наукова установа «Інститут інформації, безпеки і права Національної академії правових наук України»
ORCID ID: 0000-0001-6951-2627

Сьогодні більша половина людства не уявляє себе без цифрових пристроїв, які покращують та забезпечують їм комфортний рівень життя. Не лише дорослі, а й діти та підлітки, що є соціально незахищеною частиною населення, споживають різноманітний контент з інтернету, соцмереж, телеграм каналів, тощо. Звичні нам раніше медіа (радіо, телебачення, журнали, книги) стають все менш популярними, а їм на заміну приходять

різного роду відеоблогери, що несуть інформацію в маси. Відеоблогери активно взаємодіють із аудиторією, створюють контент, співпрацюють з брендами та впливають на суспільну думку. Відеоблогерство у сучасному цифровому просторі стало не лише способом самовираження, а й важливим сегментом економіки та медіаіндустрії. Проте з розвитком цієї діяльності постає питання правового регулювання, яке гарантує дотримання норм етики, авторського права, захисту персональних даних, а також рекламних стандартів.

Європейський Союз, як один із провідних регіонів у сфері цифрової політики, запроваджує комплекс правових норм для регулювання діяльності відеоблогерів. Основні законодавчі акти, такі як Директива про аудіовізуальні медіапослуги (AVMSD) [1], Загальний регламент про захист даних (GDPR) [2] та законодавство про авторське право, встановлюють загальні правила, що впливають на блогерів та платформи, на яких вони працюють. Проте перш ніж порівнювати конкретні кроки з регулювання, варто звернути увагу на різні підходи у розумінні того, хто власне може вважатись відеоблогерами (інфлюенсерами, ютуберами), та в чому полягає характер їх діяльності, а також як саме їх діяльність може кваліфікуватися за Директивою про аудіовізуальні медіапослуги (AVMSD) [1].

Юридичного поняття як відеоблогер не закріплено жодним правовим актом. На думку ERGA [3] (Європейської групи регуляторів аудіовізуальних медіапослуг: органу, що складається з керівників та представників європейських національних регуляторів, та консультує Європейську комісію щодо реалізації Директиви та інших питань, пов’язаних з аудіовізуальними медіа) у таких випадках слід використовувати загальноприйняте розуміння цього терміну, а саме – особу, яка створює відеоблоги (тобто блоги, які складаються з відео) та публікує їх в інтернеті, на платформах спільного доступу до відео, де вони стають доступними для широкої публіки [4].

Термін «блогер» та «інфлюенсер» використовуються як синоніми, але існує різниця між ними. Блогер створює контент, а інфлюенсер має реальну

здатність змінювати уявлення та смаки своєї аудиторії, оскільки є публічною особою. Кембриджський словник так трактує термін «інфлюенсер» – це той, хто справляє вплив. Людина, яка має значний вплив на думки і поведінку інших людей у медіапросторі, формує тренди, створює нові течії та активно взаємодіє з аудиторією [5]. Часто це блогери, артисти, громадські діячі.

Відеоблогери зазвичай використовують платформи обміну відео (VSP), як правило, YouTube, для розповсюдження свого контенту, з цієї причини їх також іноді називають «ютуберами» або каналами «YouTube».

Одним із регулюючих документів діяльності відеоблогерів є Директива про аудіовізуальні медіапослуги (AVMSD) – встановлює правила для платформ спільного доступу до відео, таких як YouTube, включаючи вимоги щодо реклами, захисту користувачів та контентних обмежень. AVMSD визнає набір основних суспільних цінностей, що застосовуються до всіх аудіовізуальних медіапослуг, таких як збереження людської гідності, захист неповнолітніх та заборона мови ворожнечі.

Відповідно до пункту 18 Преамбули AVMSD аудіовізуальні медіапослуги не повинні містити публічних провокацій до вчинення терористичного злочину. У 19 пункті Преамбули йдеться про те, що глядачі, включаючи батьків та неповнолітніх, повинні мати можливість приймати обґрунтовані рішення щодо контенту для перегляду, необхідно, щоб постачальники медіапослуг надавали достатню інформацію про контент, який може негативно вплинути на фізичний, розумовий чи моральний розвиток неповнолітніх. Це можна зробити, наприклад, за допомогою системи дескрипторів контенту, акустичного попередження, візуального символу або будь-яких інших засобів, що описують характер контенту. В пунктах 20, 21 Преамбули AVMSD йдеться про підвищення рівня захисту неповнолітніх та особливого захисту щодо обробки їх персональних даних. «Найбільш шкідливий контент, який може зашкодити фізичному, психічному або моральному розвитку неповнолітніх, але не обов’язково є кримінальним злочином, повинен підлягати найсуворішим заходам, таким як шифрування

та ефективний батьківський контроль, без шкоди для прийняття державами-членами суворіших заходів» [1].

Загальний регламент про захист даних (GDPR) [2] – регулює обробку персональних даних, що важливо для блогерів, які взаємодіють із аудиторією та збирають інформацію.

Слід відзначити ще один важливий документ, прийнятий Регламентом Європейського Парламенту та Ради 2022/2065 від 19 жовтня 2022 року про єдиний ринок цифрових послуг і внесення змін до Директиви 2000/31/ЄС2 (Закон про цифрові послуги (DSA) [6]. Цей документ розширює зону відповідальності інфлюенсерів, блогерів за розміщення контенту, який не відповідає встановленим вимогам. Насамперед, DSA спрямований на захист інтернет-користувачів шляхом встановлення нових функцій для онлайн-платформ, відповідно до яких великі компанії (поки що це 19 платформ), наприклад, Google, Meta (Facebook) тощо, нестимуть відповідальність за незаконний та шкідливий контент. Окрім цього, онлайн-платформи повинні: ділитися інформацією про те, як працюють їх алгоритми; впроваджувати процеси для швидкого видалення незаконних товарів і контенту; боротися з користувачами, які розповсюджують дезінформацію.

Слід зазначити, що в пунктах 69 та 95 Преамбули Закону про цифрові послуги йдеться про заборону таргетованої реклами вразливим категоріям населення, зокрема дітям, оскільки це може мати особливо серйозні негативні наслідки. Тому платформи Snapchat, TikTok, Google і YouTube від Alphabet, а також Instagram і Facebook від Meta перестануть показувати таргетовану рекламу користувачам підліткового віку.

Відповідно до положень DSA інфлюенсери та блогери як творці контенту повинні прийняти більшу відповідальність за вміст, який вони публікують в Інтернеті. Вони також повинні переконатися, що їхній вміст є відповідним і не вводить в оману чи не є незаконним. Що стосується онлайн-платформ соціальних медіа, які розміщують контент інфлюенсерів, то вони повинні бути більш чіткими та прозорими щодо того, як працюють їх

алгоритми вмісту. Вони повинні мати кнопку, яка дозволяє користувачам повідомляти про незаконний контент, опублікований впливовою особою, і швидко реагувати після повідомлення. Нарешті, вони зобов'язані самостійно стежити за публікаціями та видаляти їх у разі необхідності або навіть призупиняти облікові записи [7].

В підсумку зазначимо, що країни Європейського союзу мають у своєму законодавстві достатні важелі для врегулювання суспільних та юридичних відносин у відносно новій цифровій сфері медіа. Важливими аспектами є захист авторських прав, захист персональних даних, відповідальність блогерів за контент, регулювання діяльності великих онлайн платформ. Враховуючи виклики цифрової епохи, в подальшому необхідно буде вдосконалення нормативної бази ЄС. Особливу увагу необхідно буде приділити механізмам захисту прав відеоблогерів, забезпеченню справедливої монетизації контенту та врегулюванню питань відповідальності за дезінформацію.

Список використаних джерел

1. Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32018L1808 (дата звернення 02.06.2025 р.)

2. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance) URL: https://eur-lex.europa.eu/search.html?lang=en&text=GDPR&qid=1748864745901&type=quic

k&scope=EURLEX&locale=en (дата звернення 02.06.2025 р.)

3. Consistent implementation and enforcement of the new AVMSD framework URL: ERGA-SG1-2021-Report-Vloggers.pdf (дата звернення 02.06.2025 р.)

4. Правдниченко А. Директива про аудіовізуальні медіапослуги і відеоблоги: досвід європи і перспективи для України URL: https://dslua.org/wp-content/uploads/2024/02/EU-Regulation-on-Vloggers.pdf (дата звернення 02.06.2025 р.)

5. Influencer. Definition of influencer from the Cambridge Advanced Learner's Dictionary & Thesaurus. URL: https://dictionary.cambridge.org/dictionary/english/influencer (дата звернення 02.06.2025 р.)

6. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance) URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065 (дата звернення 02.06.2025 р.)

7. Influencers: obligations and responsibilities in Europe. URL: https://www.europe-consommateurs.eu/en/shoppinginternet/influencers.html (дата звернення 02.06.2025 р.)

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ: СУЧАСНІ ЗАКОНОДАВЧІ ТА ПРОСВІТНИЦЬКІ ІНІЦІАТИВИ В ПОЛЬЩІ. Іванюк І.В.

кандидат педагогічних наук, старший дослідник,
Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0003-2381-785X

Захист персональних даних дітей є пріоритетним завданням для всіх

країн. Діти є однією з найуразливіших категорій користувачів цифрових сервісів. З розвитком інформаційних технологій також зростає обсяг особистої інформації, яку збирають та обробляють онлайн-платформи. Особливу стурбованість викликає комерційна експлуатація даних неповнолітніх, кібербулінг, викрадення ідентичності та порушення права на приватність. Польща, реагуючи на ці виклики, послідовно впроваджує європейські нормативи в національне законодавство, адаптуючи їх до локального контексту. Розглянемо які нормативно-правові та просвітницькі ініціативи впроваджуються на практиці в Польщі.

Одним з документів, що регламентують цифрове середовище в країнах Європейського Союзу в нормативно-павовому полі, є «Регламент (ЄС) 2022/2065 Digital Services Act (DSA)» [1]. DSA забороняє використання таргетованої реклами на основі персональних даних неповнолітніх, що зменшує ризик комерційної експлуатації дітей через соціальні мережі, відеоплатформи та мобільні додатки [2].

Міністерство цифрових справ Польщі ініціює розробку та впровадження технологічних рішень для розвитку систем вікової верифікації користувачів [3]. Для цього вивчається і розглядається досвід Великої Британії (Age Appropriate Design Code) як модель для забезпечення безпеки дітей в інтернеті [4].

Спрямований на посилення захист прав дітей «Закон Камілки», викликав суперечливу реакцію з боку Польського управління з питань захисту персональних даних. Управління зазначило, що деякі його положення суперечать принципам загальному регламенту захисту даних щодо пропорційності, законності та обмеженості обробки [5].

Польське управління з питань захисту персональних даних здійснює просвітницькі ініціативи у співпраці з іншими партнерами. Наприклад, спільно з Омбудсменом з прав дитини вони ініціюють і проводить освітні заходи, спрямовані на посилення цифрової грамотності дітей та молоді, зокрема, наукові конференції, навчальні курси для вчителів [6]. А у

партнерстві з Фондом Orange Польське управління з питань захисту персональних даних опублікувало посібник «Зображення дитини в інтернеті. Публікувати чи ні?», який надає поради батькам та освітянам щодо безпечного розміщення фото та відео дітей у цифровому просторі [7].

У Польщі реалізується загальнонаціональна освітня програма «Твої дані – твоя справа» [8], спрямована на підвищення обізнаності дітей щодо ризиків цифрового середовища. У межах програми проводяться інтерактивні заняття, конкурси та інформаційні кампанії у закладах загальної середньої освіти.

Здійснене дослідження дозволяє зробити висновки, що Польща демонструє комплексний підхід до захисту персональних даних дітей, поєднуючи регуляторні механізми ЄС, національне законодавство та просвітницькі програми.

Список використаної літератури:

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). URL: http://data.europa.eu/eli/reg/2022/2065/oj (дата звернення 20.05.2025)

2. Traple Konarski Podrecki &Partners. New technologies law - the most important legislative developments in 2023 in EU and Poland. URL: https://www.lexology.com/library/detail.aspx?g=2231a86f-1ec7-42f0-97c4-6cad152bf428 (дата звернення 20.05.2025)

3. Better Internet for Kids. Poland: Policy Monitor - Country Profile. URL: https://better-internet-for-kids.europa.eu (дата звернення 20.05.2025)

4. Age appropriate design: a code of practice for online services. URL: https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/childrens-information/childrens-code-guidance-and-resources/age-appropriate-design-a-code-of-practice-for-online-services/ (дата звернення 20.05.2025)

5. UODO. The Act on the Protection of Minors (known as Kamilek's Law) needs corrections. URL: https://uodo.gov.pl/en/553/1783 (дата звернення

20.05.2025)

6. UODO. Issues of children's data processing in the modern world. URL: https://uodo.gov.pl/en/553/1667 (дата звернення 20.05.2025)

7. UODO.The right to privacy and images of children on the internet. Handbook. https://uodo.gov.pl/en/553/1720

8. UODO. Children want to know how to protect personal data in the era of new technologies. URL: https://uodo.gov.pl/en/553/1783 (дата звернення 20.05.2025)

ПОЛІТИКА ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ШКОЛЯРІВ У ВЕЛИКІЙ БРИТАНІЇ. Малицька І.Д.

Інститут цифровізації освіти НАПН України
ORCID ID: 0000-0003-1598-0120

У сучасному цифровому світі одним із ключових елементів забезпечення прав людини стає питання захисту персональних даних. Дані дітей, які є вразливою категорією населення, потребують особливої уваги. У Великій Британії шкільна система зобов'язана дотримуватися суворих норм щодо збору, зберігання та обробки персональної інформації учнів.

Захист даних дітей у школах регулюється низкою законодавчих актів, серед яких головну роль відіграють UK GDPR, який базується на основних положеннях Загального регламенту захисту даних (GDPR - *General Data Protection Regulation*), прийнятим Європейським Союзом [1]. Документ містить принципи обробки персональних даних, які застосовуються у всіх сферах, включно з освітою за принципами: законності, справедливості і прозорості; обмеженню обробки та зберігання даних, їх мінімізації та точності, цілісності і кофеденційності, а також підзвітності [2].

Крім цього у 2018 році був прийнятий *Закон про захист даних,* в якому

уточнюються положення UK GDPR і конкретизуються правила щодо обробки даних дітей. У ньому передбачено, що обробка персональних даних дітей до 13 років може бути надана тільки батьками або опікунами. Також зазначено, що освітні установи зобов'язані призначати відповідальних осіб, які відповідають за захист даних [3].

Для забезпечення безпеки даних, що зберігаються, у школах Великої Британії використовується спеціалізоване програмне забезпечення – системи управління інформацією (MIS – Management Information System), як-от: Arbor, Bromcom, RM Integris. Такі системи зберігають інформацію про учнів: ім'я та прізвище, дата народження, адреса, інформація про навчальні досягнення, особливі потреби. Програмне забезпечення має вбудовані функції безпеки: шифрування, контроль доступу, історію змін [4, 5].

Особлива увага приділяється кібербезпеці, запобіганню витокам даних школи. З цією метою впроваджується: антивірусне програмне забезпечення (Sophos, ESET); міжмережеві екрани (фаєрволи); системи виявлення вторгнень (IDS); резервне копіювання даних. Такі заходи допомагають захистити інформацію від хакерських атак, які останнім часом стають все частішими – зокрема, в 2024 році понад 300 шкіл у Британії зазнали кіберзлому [6].

Крім цього проводиться постійний моніторинг активності учнів, їх цифрової поведінки. Для виявлення потенційно небезпечних запитів, фільтрації вебконтенту та захисту від шкідливих програм використовується програмне забезпечення таке як: Smoothwall Monitor [7], Impero [8], Securus [9]. NetSupport DNA [10]. Системи дозволяють школам блокувати доступ до небезпечних сайтів і виявляти підозрілу активність у мережі, наприклад, спроби несанкціонованого доступу до даних учнів.

Школи у Великій Британії зобов'язані мати чіткі політики щодо захисту даних, які оприлюднюються на їхніх вебсайтах. Політики освітньої установи включають процедури збору, зберігання та використання даних, а також механізми реагування на порушення безпеки. Управління

інформаційного комісара (Information Commissioner's Office, ICO) є головним регулятором, який стежить за отриманням всіх норм [11].

Згідно з законом, кожна школа повинна мати посадову особу з питань захисту даних (DPO Data Protection Officer), яка контролює дотримання політик, проводить перевірки, взаємодіє з батьками та державними органами. Виконання таких обов'язків може виконувати як працівник, призначений адміністрацією школи, так і зовнішній консультант [12].

Регулярна підготовка вчителів та адміністрації учбового закладу з цифрової безпеки є обов'язковою вимогою та контролюється місцевими освітніми органами. Для запобігання випадковому витоку даних шкільний персонал проходить навчання з кібергігієни, тренінги з основ GDPR, інструктажі з обробки конфіденційної інформації.

Захист персональних даних дітей у британських школах – це комплексне завдання, яке охоплює юридичні, технічні та організаційні аспекти. Законодавство Великої Британії забезпечує високий рівень контролю за обробкою інформації, а школи впроваджують сучасні інструменти для збереження конфіденційності учнів. Водночас з розвитком цифрових технологій зростають і загрози, тож система захисту даних потребує постійного вдосконалення. Важливим є не лише дотримання нормативів, але й створення культури поваги до приватності учнів.

Список використаних джерел

1. Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation – GDPR). 2016. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

2. UK General Data Protection Regulation (UK GDPR). 2016. URL: https://www.legislation.gov.uk/eur/2016/679/contents

3. Data Protection Act 2018. UK Public General Acts. 2018. URL: https://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

4. Arbor Education – MIS for schools and MATs. URL: https://arbor-

education.com

5. Bromcom. URL:https://bromcom.com/

6. 330 UK schools hacked – pupil data sold on dark web. The Sun. 2024. URL: https://www.thesun.co.uk/news/27831561/pupil-images-sold-paedos-school-data-hack/

7. Smoothwall Monitor. URL: https://smoothwall.com/solutions/monitor

8. Impero. URL: https://www.imperosoftware.com/

9. Securus. URL: https://www.securus-software.com/

10. NetSupport DNA. URL: https://www.netsupportdna.com/

11. Data protection in schools / GOV.UK. 2023. URL: https://www.gov.uk/guidance/data-protection-in-schools.

12. Data protection policies and procedures. GOV.UK. 2023. URL: https://www.gov.uk/guidance/data-protection-in-schools/data-protection-policies-and-procedures

НАУКОВЕ ВИДАННЯ

Матеріали надруковані в авторській редакції. За достовірність фактів, посилань, стилістичне та орфографічне оформлення відповідальність несуть автори публікацій.

ЗАХИСТ ПЕРСОНАЛЬНИХ ДАНИХ ДІТЕЙ:
ВИКЛИКИ СЬОГОДЕННЯ

ЗБІРНИК МАТЕРІАЛІВ

Упорядники: О.Р. Радзієвська, С.О. Дорогих, Н.В. Сороко,

Формат: PDF.

Обсяг даних 1516 Кб

Інститут цифровізації освіти
Національної академії педагогічних наук України
м. Київ, вул. Максима Берлінського, 9
Свідоцтво про державну реєстрацію:
серія ДК №7609 від 23.02.2022 р.
електронна пошта (E-mail): iitlt@iitlt.gov.ua