УДК 343.8:343.9: 342.7
DOI https://doi.org/10.24144/2788-6018.2024.06.131

НАПРЯМИ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ ТА ВДОСКОНАЛЕННЯ ПРАВОВОГО РЕГУЛЮВАННЯ ЗАХИСТУ ПРАВ ЛЮДИНИ У КІБЕРПРОСТОРІ

Сперкач Н.А.,
кандидат юридичних наук,
доцент кафедри кримінального права та процесу
Державного податкового університету
ORCID: 0000-0001-6579-126X
e-mail: natali.sperkach@gmail.com

Ковбасюк В.С.,
здобувачка вищої освіти першого (бакалаврського) рівня
Державного податкового університету
ORCID: 0009-0000-0672-7241
e-mail: kovbasiukviktoriia@gmail.com

Сперкач Н.А., Ковбасюк В.С. Напрями запобігання кіберзлочинності та вдосконалення правового регулювання захисту прав людини у кіберпросторі.

Дослідження спрямоване на визначення основних проблем реалізації захисту прав людини у кіберпросторі та розробку сучасних і дієвих напрямів вдосконалення правового регулювання, щодо підвищення рівня захищеності користувачів в мережі Інтернет та зміцнення довіри громадян до цифрового середовища. Проаналізовано та запропоновано напрями запобігання кіберзлочинності, однією з найсерйозніших проблем сучасного кіберпростору, особливо в контексті постійних кібератак.

Особливу увагу приділено аналізу сучасних загроз і проблем, пов'язаних із порушенням прав людини у кіберпросторі в умовах постійних кібератак, що значно активізувалися після повномасштабного вторгнення рф. Передусім, було проаналізовано основні національні та міжнародні нормативно-правові акти, що регулюють захист прав людини у кіберпросторі. Виявлено, що наявна нормативно-правова база, якою керується Україна є дещо неактуальною в сучасних умовах, оскільки не повною мірою охоплює нові загрози, які виникають у процесі розвитку інформаційних технологій. Надано мотивовані пропозиції щодо внесення змін до чинного національного законодавства України, що стосуються вдосконалення механізмів захисту прав людини у кіберпросторі. Також порушено питання захисту персональних даних, зокрема, проаналізовано концепцію «права бути забутим», яка є особливо актуальною в умовах швидкого розповсюдження інформації в Інтернеті.

Окремо розглянуто проблеми захисту прав дітей у кіберпросторі, зокрема такі явища, як кібербулінг, грумінг і надмірний вплив насильницького контенту. Акцентовано увагу на важливості запровадження спеціальних заходів захисту для дітей, зокрема, шляхом посилення контролю за доступом до небезпечних вебресурсів, а також активізації роботи з підвищення рівня обізнаності батьків і освітян щодо загроз у цифровому просторі. Також проаналізовано заходи юридичної відповідальності за кібербулінг у США та Канаді. Крім цього, у статті детально регламентовано та обґрунтовано доцільність розробки Стратегії інформаційної безпеки дітей у кіберпросторі та Стратегії цифрового громадянства. Наголошено на необхідності впровадження в Україні інституту майнової відповідальності за кібербулінг. Зроблено висновок про необхідність комплексного підходу до вдосконалення правового регулювання кіберпростору.

Ключові слова: кіберпростір, права людини, кіберзлочинність, кібербулінг, запобігання злочинності, кримінальна відповідальність, цифрове громадянство.

Sperkach N.A., Kovbasiuk V.S. The areas of cybercrime prevention and improvement of legal regulation of human rights protection in cyberspace.

The article is devoted at identifying the main problems of human rights protection in cyberspace and developing modern and effective ways to improve legal regulation, increase the level of protection of users on the Internet and strengthen public confidence in the digital environment.

The author analyzes and proposes ways to prevent cybercrime, one of the most serious problems of modern cyberspace, especially in the context of constant cyberattacks.

Particular attention is paid to the analysis of current threats and problems related to human rights violations in cyberspace in the context of constant cyberattacks, which have significantly intensified after the full-scale invasion of russia. First of all, the authors analyzed the main national and international legal acts regulating the protection of human rights in cyberspace. It is found that the existing legal framework governing Ukraine is somewhat irrelevant in the current environment, as it does not fully cover new threats arising from the development of information technologies. Motivated proposals were made to amend the current national legislation of Ukraine to improve the mechanisms for protecting human rights in cyberspace. The authors also raised the issue of personal data protection, in particular, analyzed the concept of the «right to be forgotten», which is particularly relevant in the context of the rapid dissemination of information on the Internet.

The problems of protecting children's rights in cyberspace, including such phenomena as cyberbullying, grooming and excessive exposure to violent content, are separately considered. The article emphasizes the importance of introducing special protection measures for children, in particular, by strengthening control over access to dangerous web resources, as well as intensifying efforts to raise awareness of parents and educators about threats in the digital space. The authors also analyzed measures of legal liability for cyberbullying in the United States and Canada. In addition, the article regulates in detail and substantiates the feasibility of developing a Strategy for Information Security of Children in Cyberspace and a Strategy for Digital Citizenship. The authors emphasize the need to introduce the institution of property liability for cyberbullying in Ukraine. The article concludes that a comprehensive approach to improving the legal regulation of cyberspace is needed.

Key words: cyberspace, human rights, cybercrime, cyberbullying, crime prevention, criminal liability, digital citizenship.

Постановка проблеми. Захист прав людини у кіберпросторі сьогодні набуває надзвичайно важливого значення. Враховуючи те, що користувачем глобальної мережі Інтернет може бути будь-яка особа, особливу увагу слід звернути на ризики і загрози, які можуть бути причиною порушень прав людини в кіберпросторі. Адже разом зі зростанням важливості інтернету та цифрових технологій зросли й ризики, пов'язані з порушенням прав людини у кіберпросторі. З початком повномасштабного вторгнення рф, кіберпростір став ще одним бойовим фронтом. Окрім широкомасштабних руйнувань та людських жертв, наша держава зіштовхнулась з безпрецедентною кількістю кібератак з боку рф.

Постійні виклики та загрози потребують вчасного реагування органів державної влади, зокрема і на появу нових технологій та загроз, що виникають у глобальній мережі. Таким чином, усі ці фактори спричиняють потребу дослідження та встановлення конкретних механізмів щодо захисту прав людини у кіберпросторі та відповідності потребам користувачів. Тож, відсутність узгоджених підходів до захисту прав людини у кіберпросторі призводить до недостатньої ефективності існуючих механізмів та потребує детального дослідження та виокремлення напрямів його вдосконалення.

Мета дослідження полягає у вивченні сучасного стану захисту прав людини у кіберпросторі, визначенні основних проблем реалізації цього захисту та обґрунтуванні сучасних напрямів вдосконалення правового регулювання захисту прав людини у кіберпросторі.

Стан опрацювання проблематики. В українській правничій науці у сфері кіберзахисту, науковці зосереджуються здебільшого на проблематиці нормативно-правового регулювання кіберзахисту (Л.С. Гнатюк [1], В.В. Пахомов, І.В. Каріх, Д.А. Рєпін [12]). Деякі праці вітчизняних науковців присвячені окремим порушенням прав людини у кіберпросторі, зокрема, дослідження О.М. Лисенка [10], Я.Г. Худолєя, Н.А. Загребельної [16]. У зарубіжній правовій доктрині, особливу увагу слід звернути на наукові праці щодо кіберзахисту осіб в глобальній мережі інтернет таких науковців: Дж. Ауслуса [17] та К. Джайшанкара [18], які досить ґрунтовно досліджують концепцію права «бути забутим».

Виклад основного матеріалу. У сучасному світі кіберпростір став невід'ємною частиною повсякденного життя людей. Інтернет та цифрові технології суттєво змінили спосіб комунікації, здійснення комерційних операцій, надання освітніх та адміністративних послуг. З кожним роком кількість користувачів інтернету зростає, а разом із цим збільшується обсяг даних, що передаються та зберігаються у цифровому форматі.

Так, відповідно до пункту 11 статті 1 Закону України «Про основні засади забезпечення кібербезпеки України»: «кіберпростір – це середовище (віртуальний простір), яке надає можливості для здійснення комунікацій та/або реалізації суспільних відносин, утворене в результаті функціонування сумісних (з'єднаних) комунікаційних систем та забезпечення електронних комунікацій з використанням мережі Інтернет та/або інших глобальних мереж передачі даних» [14].

Частиною другою статті 19 Міжнародного пакту про громадянські та політичні права закріплено свободу вільного висловлювання і поширення думок та поглядів, а також пошуку та поширення інформації [11].

Відповідно до статті 34 Конституції України, кожному гарантується право на свободу думки і слова, на вільне вираження своїх поглядів і переконань. У цій же статті закріплюється право на інформацію. Статтями 31 та 32 Конституції гарантується право «на приватність» [8].

Незважаючи на наявність міжнародних та національних нормативно-правових актів у сфері кіберзахисту, вважаємо, що реалізація захисту прав людини у кіберпросторі все ще є недосконалою, адже більшість документів не відповідають вимогам сучасного часу – вони не врегульовують деякі актуальні проблеми, із якими наразі зіштовхуються користувачі. Розглянемо основні з них.

Кіберзлочинність є однією з найсерйозніших проблем сучасного кіберпростору, особливо в контексті постійних кібератак рф. За даними Департаменту кіберполіції у 2023 році було виявлено понад 3600 випадків кіберзлочинів[1], натомість у 2022 році таких кримінальних правопорушень було зареєстровано понад дві тисячі[2], а у 2021 році – всього 147 кіберінцидентів[3]. Як бачимо, з початком повномасштабного вторгнення, кіберзлочинність стрімко зростає, що вимагає посиленої уваги та ***вдосконалення заходів для її стримування***.

Основоположним документом, який регламентує правові засади запобігання кіберзлочинам є Конвенція про кіберзлочинність. У Конвенції виокремлено 4 групи правопорушень у сфері кіберпростору [7]. Варто зазначити, що 28.01.2003 р. було підписано Додатковий протокол до даної Конвенції, й виокремлено ще одну, п'яту групу злочинів [2].

В.В. Пахомов, І.В. Каріх та Д.А. Рєпін наголошують, що зважаючи на те, що Конвенція про кіберзлочинність була створена в період, коли рівень розвитку інформаційно-комунікаційних технологій (далі – ІКТ) був низьким і багато типів загроз у мережі ще не існували, то саме тому у Конвенції відсутні типові для сучасної кіберсфери дефініції, як до прикладу, «ботнети», «фішинг», «спам» та інші [12, с. 271].

Похідною від кіберзлочинності, та не менш серйозною є проблема *незаконного збору та використання персональних даних.* Це явище набуло широкого розмаху через комерціалізацію персональних даних, коли компанії збирають, обробляють і продають інформацію про користувачів без їх згоди. Наприклад, у нашій державі досить проблемною є ситуація із онлайн-казино, які часто використовують дані про своїх клієнтів для таргетованої реклами та інших комерційних цілей, що, безумовно, загрожує приватності користувачів[4].

У Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних, учасницею якої є Україна, наведено 8 основних принципів захисту даних. Особливу увагу слід зосередити на принципі 2 – персональні дані повинні бути зібрані та оброблені сумлінно, законно, точно, адекватно та не надмірно, *зберігатися лише для визначених цілей,* оновлюватися за потреби, і зберігатися лише протягом необхідного часу [6].

Діяльність з обробки персональних даних регулюється Законом України «Про захист персональних даних». Проте, як слушно зазначають Я.Г. Худолєй та Н.А. Загребельна, в умовах воєнного стану, коли права громадян зазнають обмежень, ситуація у гіперсфері потребує розробки детального плану дій щодо захисту персональних даних [16, с. 77]. Передусім, слід визначити чіткі межі та повноваження осіб на всіх рівнях щодо обробки персональних даних, а також конкретизувати всі законні підстави передачі даних від їх власників до інших осіб.

На наше переконання, кожен, хто має доступ до персональних даних, повинен чітко розуміти свої обов'язки та обмеження. Необхідно регламентувати й розмежувати правила окремо для державних службовців, військових, правоохоронних органів та інших осіб, залучених до обробки персональних даних. Також доцільною буде розробка детальних інструкцій, які б визначали, коли і за яких обставин персональні дані можуть бути передані третім особам.

В контексті удосконалення правового регулювання, не можна оминути увагою Загальний регламент про захист даних (далі – GDPR). Як зазначає, С.Л. Гнатюк, основний акцент у Регламенті зроблено на наданні громадянам більшого контролю над використанням їхніх особистих даних, що досягається шляхом вдосконалення адміністративних процедур, розширення прав громадян і посиленням контролю та відповідальності компаній-операторів у справах захисту та обробки персональних даних [1, с. 93].

Важливість даного документу, на нашу думку, полягає у тому, що Регламент розширює перелік прав осіб-власників персональних даних,

---

[1] За 2023 рік кіберполіція виявила понад 3600 кіберзлочинів. *Суспільне Новини*. URL: https://suspilne.media/673484-za-2023-rik-kiberpolicia-viavila-ponad-3600-kiberzlociniv/).

[2] У 2022 році в Україні зареєстрували 2194 кіберінциденти – Держспецзв'язку. *Суспільне Новини*. URL: https://suspilne.media/397220-u-2022-roci-v-ukraini-zareestruvali-2194-kiberincidenti-derzspeczvazku/.

[3] "41 млн підозрілих подій та 147 кіберінцидентів", – річний звіт ДЦКЗ. *Державна служба спеціального зв'язку та захисту інформації України*. URL:https://cip.gov.ua/ua/news/321f4bf8).

[4] Див: Карти, гроші, витік даних. Чи можна робити ставку на анонімність в онлайн-казино? : Свідомі. URL: https://svidomi.in.ua/page/karty-hroshi-vytik-danykh-chy-mozhna-robyty-stavku-na-anonimnist-v-onlain-kazyno (дата звернення: 29.04.2024).

зокрема, закріплено «право бути забутим», що дозволяє громадянам легше видаляти свої дані з баз даних із забороною подальшого їх використання без законних підстав (ст. 17) та «право на мобільність», що передбачає вільний доступ до власних персональних даних у будь-яких базах даних, а також спрощену процедуру передачі даних від одного постачальника послуг до іншого, що сприяє конкуренції серед постачальників послуг (ст. 20) [3]. Таким чином, положення Регламенту містять важливі норми щодо міцних та узгоджених засад захисту даних, які можна перейняти і для вдосконалення нашого законодавства, що стосується гарантування механізму належного збереження персональних даних.

Надзвичайно важливим в сучасних умовах, на наш погляд, є *регламентація «права бути забутим»*. На думку Джефа Ауслуса, «право бути забутим» – це право фізичних осіб на те, щоб їхні дані більше не оброблялися та видалялися, коли вони більше не потрібні для законних цілей [17]. К. Джайшанкар стверджує, що «право бути забутим» надає можливість вимагати видалення застарілої або неточної інформації про себе з онлайн-платформ з метою захисту своєї особистої автономії та пом'якшення потенційної шкоди [18].

У п. 6 ч. 2 ст. 8 Закону України «Про захист персональних даних» вказано, що суб'єкт персональних даних має право пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними» [13]. Тобто існує положення, яке передбачає вимогу про видалення суто через незаконний спосіб обробки або недостовірність, натомість немає вимоги про доцільність, тобто використання для конкретних цілей.

Тож, ми пропонуємо доповнити п. 6 ч. 2 ст. 8 Закону України «Про захист персональних даних» таким положенням: «пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо немає більше потреби в цих даних для цілей, для яких їх збирали чи іншим чином обробляли, або ці дані обробляються незаконно чи є недостовірними».

Переконані, що конкретизація «права на забуття» не тільки сприятиме гармонізації українського законодавства із міжнародними стандартами щодо захисту особистих даних, зокрема, згідно з вимогами Європейського Союзу, а й дозволить громадянам мати більший контроль над своєю особистою інформацією та захистити їхні приватні дані.

Також не можемо оминут*и увагою* захист прав дітей у кіберпросторі. Адже сучасні діти, незалежно від свого віку, формують свій світогляд, не обмежуючись лише родинним оточенням або взаємодією з ровесниками. Значний вплив на психіку дитини мають онлайн-ресурси та кіберпростір загалом [4, с. 12]. Аналіз контенту в Інтернеті, зокрема у соціальних мережах, свідчить про те, що деякі з основних тем, що привертають увагу, мають стосунок до насильства та жорстокості. Часто ця інформація надмірно деталізована, зокрема щодо методів скоєння правопорушень, що відбивається на формуванні уявлень про ці події у молодіжної аудиторії.

Лисенко О. М. найбільш поширеними порушенням прав дитини у кіберпросторі вважає кібербулінг, порнографію, насильство, грумінг, пропаганду расової ненависті, формування психічної залежності від онлайн-ігор та онлайн-шахрайство [10, с. 28]. Як на міжнародному, так і на національному рівнях існують правові механізми щодо запобігання деяким з цього переліку порушенням. Проте більшості з них не надано належної уваги, як наприклад, кібербулінгу, грумінгу, пропаганді расової та етнічної ненависті та іншим.

Нацкомісією з питань моралі (*наразі ліквідована*) 26.10.2011 було ухвалено Рішення «Щодо врегулювання питання безпеки дітей в Інтернеті та встановлення правил безпечного користування мережею Інтернет дітьми» та надано Рекомендації власникам веб-ресурсів, цільовою аудиторією яких є діти [15]. Проте, враховуючи постійні зміни у системі інформаційних та цифрових технологій, а також актуальні зміни у кіберпросторі, вважаємо, що з метою підвищення обізнаності дітей про безпеку в Інтернеті та соціальних мережах, а також нормативному врегулюванні питань захисту прав дитини у кіберпросторі, необхідно на законодавчому рівні розробити та прийняти нормативно-правовий документ, який би регламентував права і обов'язки дітей у кіберпросторі та захистив їх від низки вище згаданих порушень, а саме є доцільною буде розробка Стратегії інформаційної безпеки дітей у кіберпросторі.

Також, вважаємо доцільним, проаналізувати проект «Безпека дітей у кіберпросторі», запущений Департаментом безпеки дітей, філією Вищої ради у справах сім'ї в Шарджі (ОАЕ), який підвищує обізнаність дітей, батьків, педагогів та експертів про безпеку в Інтернеті. Для підлітків 10-18 років ініціатива «Амбасадори кібербезпеки» організовує семінари «рівний рівному». Молодших дітей навчають за допомогою збірки оповідань про безпечне користування Інтернетом [19].

У ст. 28 Конституції України вказано, що кожна людина має право на повагу до своєї гідності [8]. У національному законодавстві відсутнє визначення поняття «гідність», оскільки воно є

морально-етичною концепцією та водночас особистим немайновим правом. Зазвичай гідність розуміється як визнання цінності кожної фізичної особи як унікальної біопсихосоціальної істоти [9, с. 64]. Тобто кожна особа – індивідуум, який заслуговує на повагу до своєї особистості.

Проте чи можливо захистити право на повагу до своєї гідності у кіберпросторі? Адже це питання, по суті, є неврегульованим в українському законодавстві. А інтернет «перенасичений» *мовою ворожнечі – кібербулінгом, пропагандою насильства, різного роду нетерпимістю*.

За даними Державної служби статистики України, у 2020 р. та 2021 р. від навмисного самоушкодження померли по 94 дитини, то за оперативними даними обласних військових адміністрацій, у 2022 році було здійснено 127 спроб самогубства серед дітей, а станом на 15 листопада 2023 року сталося 116 випадків дитячих суїцидів за неповний рік [22]. Серед основних причин суїцидів неповнолітніх часто називають кібербулінг. Кібер-булінг – залякування, яке відбувається з допомогою цифрових пристроїв, таких як мобільні телефони, комп'ютери та планшети [5]. Медіапростір все більше наповнюється історіями про цькування дітей та молоді через інтернет. І нерідко це призводить до страшних чи навіть фатальних наслідків. Разом з тим, проаналізувавши судову практику, можна побачити, що далі розголосу у ЗМІ чи Facebook справа, як правило, не заходить. Вважаємо, що у даному випадку, слід розглянути досвід правового регулювання цієї проблеми у англосаксонських державах.

Так, у Канаді за кібербулінг правопорушника можуть притягнути як до цивільної, так і до кримінальної відповідальності [21]. Цивільно-правова відповідальність застосується у випадку наклепу або цькування. Важливо зазначити, що правопорушник несе відповідальність за будь-які наслідки, про які він міг обґрунтовано здогадуватися. Кримінальна відповідальність застосовується у випадку онлайн-переслідування, наклепу, спрямованого проти особи, яка має владні повноваження, і який може завдати серйозної шкоди її репутації, а також публікації інтимних зображень без згоди. У США, як і в Канаді за кібербулінг застосовується і цивільна, і кримінальна відповідальність [20]. У 44 штатах США кібербулінг визнаний злочином. У штатах, де кібербулінг не визнаний кримінально-караним діянням, у законодавстві штату все одно можуть вимагати від установ, наприклад, шкіл, впровадження заходів, спрямованих на запобігання кібербулінгу, або ж захищати жертв іншими способами, такими як письмова шкільна політика проти кібербулінгу та захист поза кампусом. В іншому випадку, правопорушники виплачують грошову компенсацію жертвам.

Висновки. Отже, на основі проведеного дослідження можемо зробити висновок, що у кіберпросторі порушується низка людських прав, серед основних – право на приватність, право на інформацію, право на повагу до своєї гідності та інші. Саме тому, постає *необхідність у комплексному підході до вдосконалення захисту прав людини у кіберпросторі*.

Важливо впроваджувати дійсно ефективні механізми запобіганню порушень прав людини у кіберпросторі, як наприклад, *інститут майнової відповідальності за кібербулінг*. Однак, зазначимо, що для ефективного впровадження цього механізму, необхідно розробити дієві інструменти ідентифікації винних осіб, що часто є складним завданням через анонімність в інтернеті. На наше переконання, **варто вдосконалювати заходи для стримування та запобігання будь-яким проявам кіберзлочинності,** зокрема запобігання кібершахрайствам, кібертероризму тощо і загалом забезпечення належного рівня кібергігієни громадян у кіберпросторі. Обізнаність і освіта є ключовими в цьому аспекті. Ніхто не застрахований від загрози кібербулінгу, тому поінформованість породжує профілактику.

Також, вважаємо, що необхідно реалізовувати освітні ініціативи, спрямовані на підвищення рівня обізнаності користувачів про їхні права та способи захисту в інтернеті. Потрібно **розробити та активно реалізовувати і впроваджувати Стратегію цифрового громадянства**. Так, існують заходи безпеки, які повинні знати всі, хто використовує цифрові пристрої. Від скидання паролів до вимкнення обміну даними про місцезнаходження. Тобто кожна особа повинна розуміти необхідність збереження налаштувань свого облікового запису та захисту конфіденційності й особистої інформації, щоб запобігти можливим ризикам та загрозам в кіберпросторі.

Таким чином, вважаємо, що держава повинна бути зацікавлена у впровадженні ефективної інформаційної політики у сфері кіберзахисту прав людини. Переконані, що реалізація цих заходів сприятиме зниженню ризиків, пов'язаних із порушенням прав людини у кіберпросторі та створить умови для дійсно безпечного і захищеного використання ІКТ у повсякденному житті кожної людини.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Гнатюк Л.С. Особливості захисту персональних даних в сучасному кіберпросторі: нормативно-правовий досвід ЄС. Проблеми захисту прав людини в інформаційному суспільстві : матеріали наук.-практ. конф., м. Київ, 1 квіт. 2016 р. Київ, 2016. С. 88–96.
2. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного

характеру, вчинених через комп'ютерні системи (укр/рос) : Протокол Ради Європи від 28.01.2003 р.: станом на 21 лип. 2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_687#Text (дата звернення: 30.04.2024).
3. Загальний регламент про захист даних : Регламент Європ. Союзу від 27.04.2016 р. № 2016/679. URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (дата звернення: 29.04.2024).
4. Ігнатушко І.Ю. Вплив інтернет-мережі на моральне та фізичне здоров'я дітей. *Вплив інтернет-мережі на психіку дітей та молоді – виклик сьогодення* : Матеріали Всеукр. круглого столу, м. Одеса, 27 берез. 2017 р. Одеса, 2017. С. 12–13.
5. Кібербулінг – що це та як це зупинити?. *UNICEF*. URL: https://www.unicef.org/ ukraine/cyberbulling (дата звернення: 29.04.2024).
6. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : Конвенція Ради Європи від 28.01.1981 р.: станом на 6 лип. 2010 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення: 29.04.2024).
7. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001 р.: станом на 7 верес. 2005 р. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 29.04.2024).
8. Конституція України : від 28.06.1996 р. № 254к/96-ВР : станом на 1 січ. 2020 р. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text (дата звернення: 01.04.2024).
9. Конституція України. Науково-практичний коментар : станом на 20 трав. 2018 р. / Я.О. Берназюк та ін. Київ : Професіонал, 2018. 296 с.
10. Лисенко О.М. Міжнародно-правове регулювання прав дитини в кіберпросторі. *Соціологія права*. 2016. № 3 (18). С. 25–30.
11. Міжнародний пакт про громадянські і політичні права : Пакт Орг. Об'єдн. Націй від 16.12.1966 р. : станом на 19 жовт. 1973 р. URL: https://zakon.rada.gov.ua/laws/show/995_043#Text (дата звернення: 29.04.2024).
12. Пахомов В.В., Каріх І.В., Рєпін Д.А. Міжнародно-правове регулювання кіберпростору. *Молодий вчений*. 2021. № 4 (92). С. 269–272.
13. Про захист персональних даних : Закон України від 01.06.2010 р. № 2297-VI : станом на 27 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/ show/2297-17#Text (дата звернення: 30.04.2024).
14. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII: станом на 4 квіт. 2024 р. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text (дата звернення: 29.04.2024).
15. Рекомендації власникам веб-ресурсів, цільовою аудиторією яких є діти : Рішення від 26.10.2011 р. № 17. URL: https://zakon.rada.gov.ua/rada/show/vr017623-11#Text (дата звернення: 29.04.2024).
16. Худолєй Я.Г., Загребельна Н.А. Захист персональних даних у період дії в Україні правового режиму воєнного стану: загальнотеоретичні аспекти. *Legal Bulletin*. 2023. С. 75–82.
17. Ausloos J. The 'right to be forgotten'–worth remembering?. Computer law & security review. 2012. Vol. 28, no. 2. P. 143–152.
18. Jaishankar K. Human Rights in Cyberspace and Its Impact in the Physical Space. *Indian Social Institute, Bengaluru*, 1 December 2023. URL: https://www.linkedin.com/pulse/human-rights-cyberspace-its-impact-physical-space-prof-jaishankar-w3ihc (дата звернення: 30.04.2024).
19. Child Safety in Cyberspace. Sharjah, United Arab Emirates. UNICEF for every child. Sharjah Child Friendly Office. URL: https://www.childfriendlycities.org/child-safety-cyberspace (дата звернення: 26.05.2024).
20. Is Cyberbullying Illegal?. *The Law Dictionary*. URL: https://thelawdictionary.org /article/punishment-for-cyberbullying/ (дата звернення: 26.05.2024).
21. Legal Consequences of Cyberbullying. PREVNet. *Promoting Relationships & Eliminating Violence Network | PREVNet*. URL: https://www.prevnet.ca/cyberbullying/legal-consequences-cyberbullying (дата звернення: 29.05.2024).
22. Моніторинг випадків суїцидів серед дітей. *Уповноважений Верховної Ради України з прав людини - Головна*. URL: https://www.ombudsman.gov.ua/news_details/monitoring-vipadkiv-suyicidiv-sered-ditej. (дата звернення: 29.04.2024).