***Електронний журнал «Державне управління: удосконалення та розвиток» включено до переліку наукових фахових видань України з державного управління (Категорія «Б», Наказ Міністерства освіти і науки України № 1643 від 28.12.2019). Спеціальність – 281.***

***Державне управління: удосконалення та розвиток. 2025. № 9.***

**DOI: http://doi.org/10.32702/2307-2156.2025.9.7**

**УДК 351:343.6+004.91**

*Т. С. Яровой,*

*д. держ. упр., доцент,*

*професор кафедри публічного управління та адміністрування,*

*Заклад вищої освіти «Університет трансформації майбутнього», м. Чернігів*

*ORCID ID: https//orcid.org/0000-0002-7266-3829*

*І. О. Драган,*

*д. держ. упр., професор, завідуючий кафедрою права та правоохоронної діяльності, Державний університет «Житомирська політехніка», м.Житомир*

*ORCID ID: https//orcid.org/0000-0002-5716-1273*

*О. М. Долінченко,*

*к. держ. упр., доцент кафедри публічного управління,*

*ПрАТ «Вищий навчальний заклад*

*«Міжрегіональна академія управління персоналом», м. Київ*

*ORCID ID: https//orcid.org/0000-0002-2449-1049*

# ДЕРЖАВНА ПОЛІТИКА ЗАХИСТУ ДІТЕЙ У КІБЕРПРОСТОРІ ЯК ПРІОРИТЕТ ГУМАНІТАРНОЇ БЕЗПЕКИ: ЗАРУБІЖНИЙ ДОСВІД

*T. Yarovoi,*
*Doctor of Science in Public Administration, Associate Professor, Professor of the Department of Public Management and Administration, Higher Education Institution «University of Transformation of the Future», Chernihiv, Ukraine,*
*I. Dragan,*
*Doctor of Science in Public Administration, Professor, Head of the Department of Law and Law Enforcement Activities, Zhytomyr Polytechnic State University,*
*O. Dolinchenko,*
*PhD in in Public Administration, Associate Professor of of the Department of Public Administration, Private Higher Education Institution «Interregional Academy of Personnel Management», Kyiv, Ukraine*

# STATE POLICY OF CHILD PROTECTION IN CYBERSPACE AS A HUMAN SECURITY PRIORITY: INTERNATIONAL EXPERIENCE

*Стаття присвячена дослідженню державної політики захисту дітей у кіберпросторі, розглянутої як пріоритетного напряму гуманітарної безпеки. У ході аналізу було встановлено, що стрімка цифровізація суспільства, розширення мережевих технологій та глобальна інтеграція дітей у кіберпростір суттєво змінюють характер загроз, що постають перед молодим поколінням. Розкрито вплив транснаціональних цифрових платформ на формування ризиків у контексті безпеки неповнолітніх, зокрема в аспектах кібербулінгу, сексуальної експлуатації та використання особистих даних у злочинних цілях.*

*Розглянуто міжнародний досвід реалізації державної політики щодо захисту дітей від загроз у кіберпросторі, визначено спільні підходи та відмінності у стратегічних підходах різних країн. Виокремлено практики Сполучених Штатів Америки, Канади, Європейського Союзу та окремих країн Азії, що демонструють ефективні моделі правового регулювання, кримінального впровадження та запровадження превентивних заходів у сфері*

*кібербезпеки. Виявлено, що в розвинених країнах кіберзахист неповнолітніх є частиною загальної державної політики, що поєднує законодавчі ініціативи, просвітницькі кампанії, освітні програми та активну співпрацю з міжнародними організаціями та приватним сектором.*

*Проаналізовано ключові виклики у сфері державного управління кібербезпекою дітей, що пов'язані із динамічними технологічними змінами, низькою цифровою грамотністю населення та труднощами у міжнародній співпраці щодо боротьби з кіберзлочинами. Виокремлено основні бар'єри, які гальмують ефективне впровадження державної політики, серед яких недостатня адаптивність законодавства до новітніх кіберзагроз, відсутність єдиних механізмів моніторингу та обмеженість фінансових ресурсів для впровадження інноваційних технологій у сфері кіберзахисту.*

*Обґрунтовано необхідність імплементації найкращих зарубіжних практик у національну стратегію кібербезпеки, орієнтовану на захист інтересів дітей у цифровому середовищі. Аргументовано важливість посилення державного контролю за онлайн-платформами та введення додаткових механізмів регулювання для запобігання поширенню небезпечного контенту. Визначено, що одним із ключових елементів ефективної державної політики має стати розширення програм цифрової освіти серед дітей, батьків та освітян, що сприятиме підвищенню обізнаності про основні кіберзагрози.*

*The article is devoted to the study of the State policy of child protection in cyberspace, considered as a priority area of human security. The analysis shows that the rapid digitalization of society, the expansion of network technologies and the global integration of children into cyberspace significantly change the nature of the threats facing the younger generation. The author reveals the impact of transnational digital platforms on the formation of risks in the context of the safety of minors, in particular in terms of cyberbullying, sexual exploitation and the use of personal data for criminal purposes.*

*The author examines the international experience of implementing the State policy on protection of children from threats in cyberspace, identifies common approaches and differences in strategic approaches of different countries. The author highlights the practices of the United States of America, Canada, the European Union and certain Asian countries which demonstrate effective models of legal regulation, criminal enforcement and implementation of preventive measures in the field of cybersecurity. It is found that in developed countries, cyber protection of minors is part of the general public policy, which combines legislative initiatives, awareness campaigns, educational programs and active cooperation with international organizations and the private sector.*

*The author analyses the key challenges in the field of public administration of children's cybersecurity related to dynamic technological changes, low digital literacy of the population and difficulties in international cooperation in combating cybercrime. The main barriers that hinder the effective implementation of public policy are highlighted, including the lack of adaptability of legislation to the latest cyber threats, the lack of unified monitoring mechanisms and limited financial resources for the introduction of innovative technologies in the field of cyber protection.*

*The author substantiates the need to implement the best foreign practices into the national cybersecurity strategy aimed at protecting the interests of children in the digital environment. The importance of strengthening state control over online platforms and introducing additional regulatory mechanisms to prevent the spread of dangerous content is argued. It is determined that one of the key elements of an effective public policy should be the expansion of digital education programs among children, parents and educators, which will help to raise awareness of the main cyber threats.*

***Ключові слова:*** *державна політика, державне управління, гуманітарна безпека, гуманітарна політика, національна безпека, захист інтересів дітей, протидія домашньому насильству, кримінальне впровадження, кібербезпека, кіберпростір.*

***Keywords:*** *public policy, public administration, human security, humanitarian policy, national security, protection of children's interests, combating domestic violence, criminal enforcement, cybersecurity, cyberspace*

***Постановка проблеми у загальному вигляді та її зв'язок із важливими науковими чи практичними завданнями.*** Динамічний розвиток цифрового суспільства, активне поширення мережевих технологій та масштабне залучення дітей до інтернет-середовища суттєво змінюють характер ризиків і загроз для підростаючого покоління. З кожним роком зростає кількість випадків онлайн-насильства, сексуальної експлуатації, кібербулінгу та зловживання особистими даними дітей, що має як негайні, так і віддалені негативні наслідки. Усе це потребує від держав системних та оперативних заходів, спрямованих на формування безпечного інформаційного середовища й належне реагування на кіберзлочини.

Захист прав та інтересів дітей у кіберпросторі набуває пріоритетного значення у контексті гуманітарної безпеки, адже йдеться про збереження життя, здоров'я та психоемоційного добробуту молодого покоління. Недостатній рівень правової культури в суспільстві, розрив у цифрових навичках між дітьми й дорослими, а також повільне впровадження сучасних технологій моніторингу та протидії кіберзлочинам ускладнюють боротьбу з такими викликами. Водночас в умовах глобалізації й транскордонного характеру інтернет-загроз, держава має забезпечити міжвідомчу й міжнародну координацію, а також залучити громадські й приватні структури.

***Аналіз останніх досліджень і публікацій.*** Останні дослідження у сфері захисту дітей у кіберпросторі зосереджуються на розробці комплексних державних стратегій, що враховують сучасні цифрові виклики та тенденції.

Вчені та фахівці у галузі права, соціології та інформаційної безпеки (Саєнко М. І., Савела Є. А., Тополянський Ю. Ю., Беспалько І. Л., Вапнярчук В. В., Коваленко В. В., Осипчук Т. О., Флорескул С., Лосєва В., Жеребець О. М., Дубов Д. В., Бойко В. О., Гнатюк С. Л., Ісакова Т. О., Ожеван М. А., Покровська А. В.) акцентують увагу на необхідності удосконалення правових механізмів регулювання цифрового простору, що стосуються неповнолітніх.

***Формулювання цілей статті (постановка завдання).*** Мета дослідження полягає у здійсненні комплексного аналізу державної політики захисту дітей у кіберпросторі та узагальненні зарубіжного досвіду задля формування рекомендацій зі зміцнення гуманітарної безпеки.

***Виклад основного матеріалу дослідження.*** Міжнародна нормативна база, покликана гарантувати захист інтересів дітей у кіберпросторі, сформувалася під впливом багатьох інституцій, що намагаються виробляти універсальні підходи до забезпечення гуманітарної безпеки й попередження будь-яких форм насильницького впливу на неповнолітніх. Ключову роль у цьому процесі мають документи Організації Об'єднаних Націй, передусім Конвенція про права дитини, ухвалена в 1989 році [1], яка окреслює обов'язки держав щодо всебічної охорони та розвитку дитини. Чіткі настанови щодо захисту дітей від сексуальної експлуатації та насильства [2], що здійснюється за допомогою цифрових технологій, закріплено у низці резолюцій Генеральної Асамблеї ООН, які спрямовані на зміцнення національних і транснаціональних механізмів моніторингу протиправних дій у мережі, а також на посилення превентивної складової. Згаданий комплекс рекомендацій передбачає, серед іншого, ефективний державний нагляд, розвиток спеціалізованих правоохоронних структур, а також налагодження міжсекторальної координації, що охоплює державне управління, громадські організації та приватний бізнес, котрі зацікавлені у протидії домашньому насильству та поширенню віртуальних загроз.

Вагоме значення мають акти Ради Європи, серед яких вирізняється Конвенція про захист дітей від сексуальної експлуатації та сексуального

насильства (Ланцаротська конвенція), ухвалена 2007 року. Документ містить вимоги до національних урядів стосовно посилення кримінального впровадження проти осіб, що вчиняють злочини сексуального характеру проти дітей за допомогою інформаційних технологій, а також наголошує на необхідності проведення широких інформаційно-просвітницьких кампаній, здатних підвищити рівень правової культури дорослих і неповнолітніх [3]. Рекомендації Європейського Союзу зосереджені на директивах, що стосуються протидії торгівлі людьми, покарання за розповсюдження незаконного контенту та захисту персональних даних, адже економічна і національна безпека кожної з країн-учасниць тісно пов'язана зі станом цифрового середовища. Регламент (ЄС) 2016/679 (GDPR) [4] також упорядковує підходи до обробки чутливої інформації про дітей, що зобов'язує операторів онлайн-платформ посилювати технічні й організаційні заходи задля унеможливлення витоку даних або використання їх зі злочинною метою.

Міжнародна практика захисту дітей у кіберпросторі характеризується низкою спільних рис, серед яких помітне прагнення до гармонізації правових систем, що забезпечують ефективну кримінальну відповідальність за поширення дитячої порнографії чи залучення неповнолітніх до протиправних дій. Значна увага приділяється формуванню єдиних стандартів державної політики, які фокусуються на активній співпраці між профільними міністерствами, розбудові системи моніторингу забороненого вмісту та фінансуванні програм кібербезпеки, спрямованих на виявлення хакерських технологій, що можуть бути використані для грумінгу або булінгу. Водночас державне управління в межах різних юрисдикцій шукає баланс між захистом інтересів дітей і свободою слова, оскільки правове регулювання інтернету вимагає тонкої межі між запобіганням злочинам та невтручанням у приватні комунікації [5]. Деякі країни впроваджують суворі санкції та примусові інструменти блокування вебресурсів, інші надають пріоритет превентивним заходам і просвітницькій діяльності, покладаючись на етичні норми та саморегулювання IT-компаній.

Окремі розбіжності стають очевидними при порівнянні правозастосовних механізмів, оскільки у федеральних державах на кшталт США відбувається паралельне функціонування декількох рівнів влади, де кожен штат може встановлювати додаткові правові обмеження або зосереджуватися на специфіці локальних загроз [6]. У Європейському Союзі інституційна структура містить єдині директиви, що уніфікують правила реагування, проте доповнюються національними нормативними актами щодо протидії домашньому насильству, враховуючи культурні та соціальні особливості різних країн. Суттєву роль відіграє впровадження освітніх програм, де відмінності у підходах помітно позначаються на методиці викладання основ кібербезпеки. Спільним завданням залишається формування свідомого ставлення громадськості до небезпек мережі, оскільки розуміння складнощів інтернет-контенту та професійний супровід неповнолітніх допомагають уникнути багатьох ризиків.

Значна кількість держав розглядає освітні установи як головний майданчик для запровадження превентивних стратегій і програм, що покликані зміцнити гуманітарну безпеку й розвинути базові навички інформаційної гігієни серед учнів, особливо коли йдеться про ранній контакт із соціальними мережами та іншими онлайновими сервісами. Деякі ініціативи передбачають обов’язкове вивчення правил безпечної поведінки в інтернеті, зокрема опрацювання теми відповідального використання особистих даних і розпізнавання токсичного контенту. Подібні проєкти проводяться у співпраці з недержавними організаціями, які спеціалізуються на захисті молоді від зловживань та займаються просвітницькою діяльністю у межах національної безпеки. Часто залучаються також приватні компанії з галузі ІТ, що мають доступ до передових технологій сканування та блокування сумнівних ресурсів.

Важливим чинником успішного впровадження принципів кібербезпеки в навчальному середовищі вважається підготовка викладачів і психологів, здатних оперативно виявляти ознаки онлайн-насильства і сприяти своєчасній комунікації з правоохоронними органами. Педагоги проходять курси підвищення кваліфікації, де ознайомлюються з типами загроз у кіберпросторі,

протоколами реагування, а також методами взаємодії з батьками та самими учнями щодо профілактики повторних травматичних ситуацій [7]. Створюються шкільні команди з цифрової грамотності, які роз'яснюють учасникам освітнього процесу базові принципи безпечного інтернет-користування. Деякі держави акцентують увагу на розробці спеціальних додатків для смартфонів, котрі дають змогу учням сигналізувати про підозрілі контакти чи будь-які інші ознаки загрози. Усуваючи інформаційний вакуум, державна політика та державне управління здатні сприяти формуванню комплексного підходу, де поєднуються технологічні інновації, кримінальне впровадження, а також колективна відповідальність суспільства за добробут і безпеку молодого покоління.

Досвід кількох провідних держав демонструє широкий спектр підходів до формування та здійснення стратегій, спрямованих на гуманітарну безпеку й захист інтересів дітей у цифровому середовищі. Певні країни застосовують сувору регулятивну політику з акцентом на кримінальне впровадження та блокування заборонених ресурсів, тоді як інші покладаються на добровільну участь приватного сектору й посилену просвітницьку діяльність серед батьків, педагогів та неповнолітніх. Особливу роль мають міжвідомчі робочі групи, які аналізують загрози та розробляють методичні матеріали, що допомагають уніфікувати процедури реагування на випадки виявлення домашнього насильства чи сексуальної експлуатації у вебсередовищі. Інтенсивне зростання кіберзлочинності, пов'язаної з поширенням небезпечних контентів, зумовлює потребу в розвинених механізмах контролю й запобігання повторним правопорушенням.

Законодавчі ініціативи у Сполучених Штатах характеризуються чіткою сегментацією за віковими групами, що відображається в актах, спрямованих на захист персональних даних неповнолітніх та контроль за поширенням дитячого контенту еротичного характеру. Федеральні органи підтримують розвиток системи онлайн-сервісів, де працює державне управління у тісній співпраці з

громадськими організаціями для оперативного виявлення проблемних ресурсів і надання психологічної допомоги жертвам злочинних дій [8].

Канада приділяє значну увагу інтеграції превентивних освітніх програм у шкільні курси, залучаючи широкі кола експертів з дитячої психології й соціології, аби сформувати новий рівень цифрової грамотності серед учнів. Стратегія дає можливість просувати ідеї гуманітарної безпеки у багатонаціональному середовищі, де важливість культурних особливостей виховання відіграє помітну роль. Державні органи та недержавні інституції Європейського Союзу проводять скоординовану політику у сфері кібербезпеки, зосереджену на посиленні відповідальності великих онлайн-платформ, які повинні швидко реагувати на факти грумінгу або приниження гідності дітей у соцмережах. Періодичні кампанії з підвищення рівня цифрової обізнаності організовують у співпраці з провідними IT-корпораціями, що уможливлює використання сучасних технологій штучного інтелекту та машинного навчання для фільтрації шкідливих матеріалів. Азійські держави запроваджують доволі різнопланові заходи, зокрема, окремі регіони використовують обов’язкові системи ідентифікації користувачів, які обмежують доступ до соціальних платформ для осіб, що не досягли належного віку. Органи влади, освітні установи та громадські об’єднання створюють спеціалізовані тренінги, присвячені безпечній поведінці у кіберпросторі й протидії домашньому насильству, посилюючи рівень підготовки викладачів і психологів.

Реалізація державних політик спричиняє певні складнощі, зумовлені, зокрема, високою швидкістю розвитку інформаційних технологій і неможливістю завжди оперативно вносити відповідні зміни до законодавства. Певні країни намагаються вирішити проблему за допомогою гнучких нормативних актів, які передбачають загальні принципи реакції на нові загрози, однак така практика іноді вступає в суперечність із юридичною визначеністю та правовою безпекою. Високий рівень недовіри населення до органів влади у деяких регіонах спричиняє пасивність батьків, які не звертаються по кваліфіковану допомогу навіть у разі виявлення злочинних дій щодо власних

дітей, що ускладнює процес офіційного реагування. Досить гострою вважається проблема узгодження державного втручання з правом на приватність, оскільки певні механізми контролю в інтернеті можуть сприйматися як надмірне обмеження громадянських свобод [9]. Фінансова складова теж впливає на успішність політик, адже формування системи кібербезпеки з розгалуженою мережею експертів, інвестування у програмне забезпечення та розробку технічних рішень вимагають значних ресурсів, які не завжди доступні для країн, що перебувають у стані економічних труднощів.

Застосування світових напрацювань у сфері захисту неповнолітніх може надати суттєвий поштовх до вдосконалення українського законодавства та практики державного управління. Вітчизняний формат регулювання сфери кіберпростору, спрямований на припинення поширення небезпечного контенту та боротьбу з домашнім насильством, може запозичувати елементи комплексних програм, які давно реалізуються у північноамериканських і західноєвропейських державах. Розробка державних стратегій, побудованих на співпраці з органами місцевого самоврядування, приватним сектором та громадськими ініціативами, формуватиме фундамент для дієвого реагування на нові загрози, пов’язані з використанням анонімних інтернет-каналів, цифрових валют і платформ обміну контентом [10]. Особливий акцент слід робити на просвітницьких програмах, призначених для сімей, у яких батьки перебувають у соціально вразливому становищі й мають обмежені можливості супроводу дітей у мережевій комунікації. Україна може скористатися співпрацею з міжнародними експертами, які пропонують інноваційні підходи до виявлення та розслідування кримінальних правопорушень, включаючи використання спеціалізованих програм для аналізу трафіку і візуального розпізнавання заборонених матеріалів.

Форми домашнього насильства в кіберпросторі часто набувають нових ознак, оскільки насильники можуть застосовувати технологічні засоби контролю та маніпуляції над дітьми, блокуючи доступ до соціальних мереж або шантажуючи з використанням особистої інформації. Кібербулінг, викрадення

даних, створення фейкових профілів та поширення приватних світлин без згоди жертви належать до найбільш розповсюджених загроз, що підривають гуманітарну безпеку й негативно впливають на психоемоційний стан неповнолітніх. Державна політика, націлена на захист інтересів дітей у родинах, відображає основні принципи національної безпеки, які передбачають розвиток профілактичних заходів і системи швидкого реагування в умовах поширення цифрових загроз.

Кримінально-правові механізми, розроблені в зарубіжних юрисдикціях, демонструють прагнення забезпечити невідворотність покарання для осіб, що вчиняють злочини проти дітей у кіберпросторі. Судова практика багатьох західних держав включає випадки застосування підвищених санкцій за розповсюдження матеріалів, які містять сцени насильства або сексуальної експлуатації малолітніх, а також за грумінг і переслідування з використанням інформаційних технологій. Деякі рішення судів містять розширене тлумачення домашнього насильства, що охоплює примусове залучення неповнолітніх до небезпечних онлайн-активностей. Подібні правозастосовні прецеденти сприяють формуванню єдиних стандартів кримінального впровадження, де чітко визначені ознаки злочину та критерії кваліфікації протиправних дій.

Співпраця держави, правоохоронних органів і громадськості у виявленні та попередженні правопорушень потребує ефективних каналів комунікації, завдяки яким кожен випадок домашнього насильства в кіберпросторі не залишається поза увагою. Державне управління має координувати зусилля різних відомств, розвивати спеціальні платформи для повідомлень про злочини і підтримувати інформаційні кампанії, спрямовані на підвищення рівня обізнаності населення щодо інструментів захисту. Кібербезпека неповнолітніх значною мірою залежить від здатності суспільства вчасно ідентифікувати загрозу та надати якісну психологічну і правову допомогу тим, хто постраждав. Саме так державна політика забезпечує створення належної системи реагування, де поєднуються кримінальне впровадження, профілактичні програми та широка мережа соціальної підтримки, що захищає дітей у цифровому середовищі.

***Висновки та перспективи подальших розвідок у даному напрямі.*** Проведений комплексний аналіз засвідчив, що державна політика захисту дітей у кіберпросторі набуває особливої ваги в контексті сучасного інформаційного суспільства, оскільки вона визначає умови, за яких неповнолітні можуть розвиватися без загрози втягування у протиправні дії чи зазнання насильницького впливу з боку зловмисників. Формування дієвої системи державного управління, спрямованої на забезпечення гуманітарної та національної безпеки, має ґрунтуватися на багатовекторному підході, котрий поєднує правове регулювання, соціально-профілактичні програми, ефективне кримінальне впровадження та широку інформаційно-просвітницьку діяльність. Стратегії, побудовані на врахуванні кращих світових практик, запобігають ризикам, пов’язаним із домашнім насильством, сексуальною експлуатацією та іншими формами злочинної діяльності, реалізованої через цифрове середовище.

Перспективи подальших досліджень охоплюють кілька напрямів. Вважливо продовжувати порівняльний аналіз найновіших нормативно-правових рішень, що з’являються у державах із різними правовими системами, зокрема в аспектах удосконалення кримінальної відповідальності за кіберзлочини проти дітей. Актуальною стає розробка інструментів оцінювання ефективності існуючих програм, спрямованих на протидію домашньому насильству в онлайн-сфері, з урахуванням показників повторної віктимізації дітей і поширеності небажаного контенту. Дослідники можуть зосередитися на питаннях етичної взаємодії органів влади з приватним сектором, оскільки транснаціональні ІТ-компанії нерідко накопичують значний обсяг даних, що може стати предметом аналізу для державних інституцій. Крім того, перспективним є вивчення технологічних засобів (зокрема штучного інтелекту) для виявлення правопорушень у мережі та захисту інтересів дітей, що матиме значення не лише для національної, а й глобальної безпеки.

**Література**


1. Конвенція про права дитини. *ООН; Конвенція, Міжнародний документ від 20.11.1989.* URL: https://zakon.rada.gov.ua/go/995_021

2. Конвенція Ради Європи про захист дітей від сексуальної експлуатації та сексуального насильства. *Рада Європи; Конвенція, Міжнародний документ від 25.10.2007.* URL: https://zakon.rada.gov.ua/laws/show/994_927#Text

3. Роз'яснення до статті 23 Лансаротської конвенції – Домагання дитини для сексуальних цілей. (2020). *Офіс Ради Європи в Україні.* URL: https://www.coe.int/uk/web/kyiv/-/clarifications-to-article-23-of-the-convention-solicitation-of-children-for-sexual-purposes

4. Регламент Європейського Парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року 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). *Європарламент, Рада ЄС; Регламент, Міжнародний документ від 27.04.2016 № 2016/679.* URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

5. Саєнко М. І., Савела Є. А., Тополянський Ю. Ю. Міжнародний досвід протидії кіберзлочинності та кібершахрайству. *Науковий вісник Ужгородського національного університету. Серія: Право.* 2021. Вип. 64. С. 386-341. URL: http://visnyk-pravo.uzhnu.edu.ua/article/view/238897/237481

6. Беспалько І. Л., Вапнярчук В. В. Особливості процесу доказування в кримінальному процесі Сполучених Штатів Америки. *Науковий вісник Ужгородського Національного Університету. Серія: Право*. 2024. Вип. 81, ч. 3. С. 39-49.

7. Коваленко В. В., Осипчук Т. О. Теоретичні підходи щодо визначення проблеми розвитку цифрової компетентності з кібербезпеки вчителів закладів загальної середньої освіти. *Інноваційна педагогіка*. 2024. Вип. 67, т. 2. С. 264-269. URL:

https://lib.iitta.gov.ua/id/eprint/739871/1/Стаття%20Коваленко%20В.В.,%20Осипчук%20Т.О.pdf

8. Флорескул С. Лосєва В. Захист персональних даних у США. *Avitar.* 2024. URL: https://www.avitar.legal/post/zahist-personalnih-danih-u-ssha

9. Жеребець О. М. Реалізація державної політики у сфері протидії кіберзлочинності: законодавчий аспект. *Інформація і право.* 2021. № 4(39). С. 129-134. URL: http://il.ippi.org.ua/article/view/248834

10. Дубов Д. В., Бойко В. О., Гнатюк С. Л., Ісакова Т. О., Ожеван М. А., Покровська А. В. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. за заг. ред. Д. Дубова. К. : НІСД, 2018. 84 с. URL: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf

**References**

1. UN (1989), "Convention on the Rights of the Child", available at: https://zakon.rada.gov.ua/go/995_021 (Accessed 05 Sept 2025).

2. Council of Europe (2007), "Council of Europe Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse", available at: https://zakon.rada.gov.ua/laws/show/994_927#Text (Accessed 05 Sept 2025).

3. Council of Europe Office in Ukraine (2020), "Clarifications to Article 23 of the Convention - Solicitation of children for sexual purposes", available at: https://www.coe.int/uk/web/kyiv/-/clarifications-to-article-23-of-the-convention-solicitation-of-children-for-sexual-purposes (Accessed 05 Sept 2025).

4. Official Journal of the European Union (2016), "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)", available at: https://zakon.rada.gov.ua/laws/show/984_008-16#Text (Accessed 05 Sept 2025).

5. Saienko, M. I., Savela, Ye. A. and Topolians'kyj, Yu. Yu. (2021), “ International experience in combating cybercrime and cyberfraud ”, Naukovyj visnyk Uzhhorods'koho natsional'noho universytetu. Seriia: Pravo, vol. 64, pp. 386-341, available at: http://visnyk-pravo.uzhnu.edu.ua/article/view/238897/237481 (Accessed 05 Sept 2025).

6. Bespal'ko, I. L. and Vapniarchuk, V. V. (2024), “Peculiarities of the evidentiary process in the criminal process of the United States of America”, Naukovyj visnyk Uzhhorods'koho Natsional'noho Universytetu. Seriia: Pravo, vol. 81, no. 3, pp. 39-49.

7. Kovalenko, V. V. and Osypchuk, T. O. (2024), “Theoretical approaches to defining the problem of developing digital competence in cybersecurity for teachers of secondary education institutions”, Innovatsijna pedahohika, vol. 67, no. 2, pp. 264-269, available at: https://lib.iitta.gov.ua/id/eprint/739871/1/Stattia%20Kovalenko%20V.V.,%20Osypchuk%20T.O.pdf (Accessed 05 Sept 2025).

8. Floreskul, C. and Losieva, V. (2024), “Personal data protection in the USA”, available at: https://www.avitar.legal/post/zahist-personalnih-danih-u-ssha (Accessed 05 Sept 2025).

9. Zherebets', O. M. (2021), “Implementation of state policy in the field of combating cybercrime: legislative aspect”, Informatsiia i pravo, vol. 4(39), pp. 129-134, available at: http://il.ippi.org.ua/article/view/248834 (Accessed 05 Sept 2025).

10. Dubov, D. V., Bojko, V. O., Hnatiuk, S. L., Isakova, T. O., Ozhevan, M. A. and Pokrovs'ka, A. V. (2018), Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyj dosvid ta mozhlyvosti dlia Ukrainy [Public-private partnership in the field of cybersecurity: international experience and opportunities for Ukraine], NISD, Kyiv, Ukraine, available at: https://niss.gov.ua/sites/default/files/2018-06/AD_Dubov_206x301_pp1-84_press-b44d7.pdf (Accessed 05 Sept 2025).

*Стаття надійшла до редакції 08.09.2025 р.*