УДК 343.9:094 (477)
DOI https://doi.org/10.24144/2788-6018.2025.06.3.12

КІБЕРСТІЙКІСТЬ ТА ПРАВА ЛЮДИНИ: ІМПЛЕМЕНТАЦІЯ МІЖНАРОДНИХ ПРЕВЕНТИВНИХ МОДЕЛЕЙ У ЦИФРОВИЙ ПРОСТІР В УКРАЇНІ[1]

Олійник А.А.,
аспірант кафедри адміністративного і кримінального права
юридичного факультету
Дніпровського національного університету
імені Олеся Гончара
ORCID: 0009-0001-4849-0120

Олійник А.А. Кіберстійкість та права людини: імплементація міжнародних превентивних моделей у цифровий простір в Україні.

Актуальність дослідження зумовлена тотальною цифровізацією та безпрецедентним зростанням кіберзлочинності, що загрожує правам і свободам людини. У контексті гібридної війни та постійних інформаційних атак, розуміння превентивної ролі інформаційної безпеки та кримінально-правової політики набуває стратегічного значення. Стрімка трансформація технологій зумовлює зміну традиційного розуміння конституційних прав (приватність, свобода слова, власність), які набувають нового виміру в умовах цифрової реальності. Кіберпростір створює нові системні загрози для цих прав, включаючи несанкціонований доступ, цифрову ідентифікацію та шахрайство. Метою статті є комплексне наукове обґрунтування та розробка методологічних засад і практичних рекомендацій щодо вдосконалення кримінально-правової політики превенції кіберзлочинності в Україні шляхом імплементації міжнародних превентивних моделей для забезпечення кіберстійкості та гарантування конституційних прав громадян у цифровому просторі. Ключовим результатом є наукове обґрунтування того, що ефективна кримінально-правова політика превенції має ґрунтуватися на багаторівневій імплементації міжнародних превентивних моделей, яка створює синергію між кіберстійкістю держави та особи. Кіберстійкість держави (макрорівень) забезпечує нормативну, інституційну та технічну базу для захисту критичної інфраструктури, тоді як кіберстійкість індивіда (мікрорівень) безпосередньо знижує ризики віктимності. Стійкість держави неможлива без стійкості її громадян, оскільки людський фактор виступає найслабшою ланкою у системі захисту. Особлива увага приділена когнітивній безпеці, а саме, здатності людини критично сприймати інформацію та захищати свідомість від маніпуляцій, дезінформації та психологічного впливу. Обґрунтовано, що когнітивна безпека є елементом кримінологічної превенції кіберзлочинів, що порушують права особи, оскільки маніпуляції свідомістю є першим кроком до шахрайства або вербування, порушуючи право людини на об'єктивну інформацію та вільний вибір. Вдосконалення кримінально-правової політики залежить від імплементації трьох моделей: конвенційно-правової (гармонізація з NIS2, GDPR та Будапештською конвенцією), інституційно-технічної (захист системи) та когнітивно-освітньої (пріоритетність програм з кібергігієни). Комплексний підхід передбачає синергію правових, технічних та освітніх механізмів, що дозволяє не лише реагувати, а й запобігати кіберзлочинам.

Практичні рекомендації вдосконалення превентивної політики включають законодавчу гармонізацію (впровадження стандартів NIS2 та вимог ЄСПЛ) та інституційну спеціалізацію правоохоронних органів для протидії високотехнологічним злочинам у цифровому середовищі. Важливо посилити когнітивний імунітет через створення єдиної національної платформи кіберосвіти та інтеграцію когнітивної безпеки в освітню стратегію, що знизить віктимність громадян і зміцнить національну кіберстійкість.

Ключові слова: кіберзлочинність, міжнародне співробітництво, кримінальна відповідальність, права людини, цифрове середовище, кіберстійкість, запобігання злочинності, національна безпека.

Oliinyk A.A. Cyber resilience and human rights: implementation of international preventive models in the digital space in Ukraine.

The relevance of the study is determined by total digitalization and unprecedented growth of cybercrime, which threatens human rights and freedoms. In the context of hybrid warfare and constant

[1] Дослідження було частково профінансовано Міністерством закордонних справ Чеської Республіки в межах проєкту 25-PKVV-UM-004 «Development of Education, Research, and International Cooperation at Oles Honchar Dnipro National University (DNU)» , реалізованого Карловим університетом і Дніпровським національним університетом імені Олеся Гончара.

information attacks, understanding the preventive role of information security and criminal law policy is of strategic importance. The rapid transformation of technology is changing the traditional understanding of constitutional rights (privacy, freedom of speech, property), which are taking on a new dimension in the digital reality. Cyberspace creates new systemic threats to these rights, including unauthorized access, digital identification, and fraud. The purpose of this article is to provide a comprehensive scientific rationale and develop methodological principles and practical recommendations for improving criminal law policy on cybercrime prevention in Ukraine through the implementation of international preventive models to ensure cyber resilience and guarantee the constitutional rights of citizens in the digital space. The key result is a scientific justification that effective criminal law prevention policy should be based on the multi-level implementation of international preventive models, which creates synergy between the cyber resilience of the state and the individual.

The cyber resilience of the state (macro level) provides the regulatory, institutional, and technical framework for protecting critical infrastructure, while the cyber resilience of individuals (micro level) directly reduces the risks of victimization. The resilience of the state is impossible without the resilience of its citizens, as the human factor is the weakest link in the protection system. Particular attention is paid to cognitive security, namely, the ability of a person to critically perceive information and protect their consciousness from manipulation, disinformation, and psychological influence. It is justified that cognitive security is an element of criminological prevention of cybercrimes that violate human rights, since manipulation of consciousness is the first step towards fraud or recruitment, violating the human right to objective information and free choice. The improvement of criminal law policy depends on the implementation of three models: conventional legal (harmonization with NIS2, GDPR, and the Budapest Convention), institutional-technical (system protection), and cognitive-educational (priority of cyber hygiene programs). A comprehensive approach involves the synergy of legal, technical, and educational mechanisms, which allows not only to respond to but also to prevent cybercrime. Practical recommendations for improving preventive policies include legislative harmonization (implementation of NIS2 standards and ECHR requirements) and institutional specialization of law enforcement agencies to combat high-tech crimes in the digital environment. It is important to strengthen cognitive immunity by creating a unified national cyber education platform and integrating cognitive security into the education strategy, which will reduce citizen victimization and strengthen national cyber resilience.

Key words: cybercrime, international cooperation, criminal liability, human rights, digital environment, cyber resilience, crime prevention, national security.

Постановка проблеми. Цифрова трансформація суспільства створює для держави, спільноти та окремих громадян нові можливості, але водночас продукує глобальні і локальні ризики порушення прав людини у цифровому середовищі. Кіберстійкість в умовах сьогодення стає ключовим елементом національної безпеки та створення прийнятних умов для реалізації і захисту прав людини. Її особливості проявляються на двох взаємопов'язаних рівнях – державному та індивідуальному, що формує комплексну основу для наукового обґрунтування кримінально-правової політики превенції кіберзлочинності. Кіберстійкість можна охарактеризувати як здатність держави (на рівні різних інституцій) та людини протидіяти, адаптуватися та відновлюватися після кіберінцидентів. Її значення різниться на рівні держави (захист критичної інфраструктури, державних сервісів) та особи (захист персональних даних, цифрової ідентичності).

Сучасні кримінальні правопорушення у цифровій сфері за своєю природою мають транскордонний характер, оскільки вони не обмежуються лише територією однієї країни чи віртуальним простором. Ці злочинні діяння, що набувають глобального, міждержавного та міжнародного характеру, створюють виклики для національного суверенітету та правоохоронної системи. Злочинність у цифровій сфері набула глобального масштабу, що унеможливлює ефективну превенцію виключно на національному рівні. Це вимагає міжнародної координації для захисту національного суверенітету та безпеки громадян. Тому, у цьому контексті, представляє науково-практичний інтерес комплексний аналіз міжнародних превентивних моделей та можливості їх системної та ефективної імплементації у національний простір.

Мета статті полягає у дослідженні особливостей кіберстійкості держави та особи як основи для комплексного обґрунтування практичних рекомендацій щодо вдосконалення кримінально-правової політики превенції кіберзлочинності в Україні шляхом імплементації міжнародних превентивних моделей для забезпечення конституційних прав громадян у цифровому просторі.

Стан опрацювання проблематики. Питанням вдосконалення законодавства та кримінально-правової охорони різних об'єктів у цифровому просторі, а також проблемам кібербезпеки та інформаційного захисту, приділяли увагу такі вчені, як: А. Бабенко, Г. Дідківська, Н. Бааджи, І. Березовська, Н. Бендовський, Д. Бірюков, О. Бодунов, В. Бочковой, Н. Верлос, В. Воронкова,

О. Гиляка, М. Карчевський, О. Колб, Т. Коломоєць, Т. Корнякова, В. Ліпкан, С. Лихова, Л. Мудрієвська, В.Нікітенко, Є. Пилипенко, О. Петришин, Ю. Размєтаєва, Д. Ричка, Л. Тарасенко, К. Тверезовська, В. Топчий Н. Юзікова, A. Calderaro, P. Chiara, C. Djeffal, Dunstan Allison-Hope, G. Hulkó, D. Kardefelt-Winther, M. Kettemann, G. Lansdown, S. Livingstone, K. Macdonald, M. Stoilova, A. Third, B. Wagner та ін.

Українські автори зосереджують увагу на імплементації міжнародних норм у національне законодавство, адаптації до умов воєнного часу та захисті критичної інфраструктури, а також проблемах цифрових прав людини в умовах глобальних ризиків та розвитку ШІ [1-9]. Дослідження вчених акцентують увагу на кримінально-правовій охороні об'єктів у цифровому просторі, проблемах гармонізації з Будапештською конвенцією та необхідності розвитку цифрової освіти. Водночас українська наукова думка меншою мірою розкриває питання інтеграції прав людини у технічні стандарти, захисту прав дитини в цифровому середовищі та механізмів превентивного реагування на кіберзагрози. Українська правова доктрина розглядає кримінально-правову політику превенції кіберзлочинності та гарантування прав громадян у цифровому просторі як прямий результат реалізації принципу верховенства права та необхідності приведення національного законодавства у відповідність до міжнародних стандартів, зокрема положень Конвенції Ради Європи про кіберзлочинність та стратегій ЄС/НАТО щодо кіберстійкості.

Зарубіжні дослідники розглядають кіберстійкість у контексті захисту прав людини та цифрового суверенітету, акцентуючи на превентивних моделях, таких як GDPR, Directive (Network and Information Security 2), Cyber Resilience Act 2022/0356, а також стандартах NIST та ISO/IEC 27001. Їхні роботи підкреслюють важливість інтеграції технічних і правових механізмів, прозорості алгоритмів, захисту персональних даних та прав дитини в цифровому середовищі [10-16]. Науковий інтерес, у межах зарубіжного підходу, представляє розробка та запровадження концепцій «Human Rights by Design» та «Children's Rights in Digital Governance», орієнтованої на глобальні стандарти [17–22].

Таким чином, міжнародно-правове значення кіберстійкості полягає у забезпеченні балансу між безпекою та правами людини, а імплементація превентивних моделей має бути комплексною: від технічних стандартів до правових гарантій. Подальший розвиток законодавства України повинен враховувати глобальні тенденції, забезпечувати ефективну кримінально-правову охорону та інтеграцію у міжнародні системи кіберзахисту.

Виклад основного матеріалу. В умовах тотальної цифровізації та гібридної війни в Україні виникла невідповідність між швидкістю розвитку технологічних загроз глобального і локального характеру та ефективністю національних правових механізмів протидіяти їм та попереджати. Стрімке зростання кіберзлочинності та цілеспрямовані інформаційні атаки призводять до трансформації традиційних конституційних прав, починаючи з права на приватність, власність і до когнітивної безпеки, вимагаючи проактивного захисту. Система кіберзахисту, яка існує сьогодні, має базове законодавче підґрунтя [23, 24, 25]. Поряд з цим, вона залишається переважно реактивною, концентруючись на покаранні, а не на комплексному запобіганні. Недостатня імплементація міжнародних превентивних моделей (правових, технічних та освітніх), сформованих Радою Європи, ЄС та НАТО, створює загрозу для кіберстійкості та підриває довіру громадян до цифрового середовища. Це актуалізує необхідність наукового обґрунтування та розробки шляхів адаптації міжнародного досвіду для формування системної та багаторівневої превентивної політики, що гарантуватиме дієвий захист прав людини у віртуальному просторі.

Реалізація визначеної у статті мети дослідження вимагає, перш за все, аналізу міжнародно-правового підґрунтя, яке формує позитивний обов'язок держави щодо захисту прав людини у цифровому просторі.

З огляду на це, міжнародно-правова модель превенції кіберзлочинності ґрунтується на двох ключових стовпах: Конвенційних гарантіях прав людини та Стратегічних зобов'язаннях щодо кіберстійкості.

Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) є наріжним каменем кримінально-правової превенції, встановлюючи універсальні визначення кіберзлочинів, а також механізми міжнародного співробітництва. Водночас, фундаментальні конституційні права людини (зокрема, право на приватність, гарантоване ст. 8 Європейської Конвенції **з** прав людини), формують межі допустимого державного втручання та підкреслюють необхідність пропорційності будь-яких превентивних заходів [26].

Таким чином, превентивна політика України у цифровому просторі має бути двовекторною: а) спрямованою на гармонізацію кримінально-правових норм відповідно до міжнародних вимог; б) одночасно спрямованою на захист особистих прав від надмірного втручання держави.

Для забезпечення цільового захисту прав людини у цифровому просторі, необхідно розрізняти два взаємозалежні рівні цільової стійкості: кіберстійкість держави (макрорівень) та кіберстійкість

людини (мікрорівень). Саме такий підхід може бути основою вибору та адаптації міжнародних превентивних моделей.

Кіберстійкість держави можна визначити як здатність національної системи інституцій (уряду, критичної інфраструктури, військових та фінансових мереж) передбачати, протистояти, відновлюватися та адаптуватися до кібератак, зберігаючи при цьому свої основні функції та дотримуючись національних інтересів країни. Цей рівень потребує правової та інституційної превенції (наприклад, гармонізації законодавства, створення спеціалізованих підрозділів за моделлю НАТО) та технічної превенції (стандартизації захисту за Директивами ЄС). Для держави кіберстійкість означає захист критичної інфраструктури, державних сервісів та економічної стабільності. Вона реалізується через національні стратегії, законодавчі акти та спеціалізовані інституції (CERT, SOC). Міжнародні моделі, такі як NIS2 Directive (ЄС), Cyber Resilience Act, а також US National Cybersecurity Strategy, передбачають комплексні механізми управління ризиками, обов'язкові стандарти безпеки та координацію реагування на інциденти.

Для особи кіберстійкість зводиться до захисту персональних даних, цифрової ідентичності та фінансової безпеки. Основні інструменти-багатофакторна автентифікація, резервне копіювання, кібергігієна та навчання. Міжнародні рекомендації, зокрема NIST Cybersecurity Framework та ISO/IEC 27001, акцентують на персональній відповідальності за безпеку цифрового середовища. Кіберстійкість людини складається зі здатності індивіда (громадянина) уникати, розпізнавати та мінімізувати негативний (шкідливий) вплив кіберзагроз, спрямованих на його особисті права, фінанси та свідомість. Цей рівень є основою для когнітивної превенції. Когнітивна безпека становить здатність людини критично сприймати та опрацьовувати інформацію, захищаючи власну свідомість від маніпуляцій, дезінформації та цілеспрямованого психологічного впливу. Це безпосередньо стосується превенції злочинності проти особи, оскільки маніпуляції свідомістю часто є першим кроком до вчинення шахрайства або вербування. Особлива роль відводиться захисту свідомості людини від маніпуляцій, що забезпечує право людини на об'єктивну інформацію та вільний вибір.

Кримінально-правова політика повинна включати просвітницькі кампанії з медіаграмотності, що є ключовим інструментом запобігання злочинам, які починаються з обману та психологічного тиску.

Професор Г.Г. Почепцов вказує на важливість когнітивної безпеки, особливо в умовах сучасного інформаційного суспільства. Когнітивна безпека охоплює заходи, спрямовані на захист розумових процесів та розвиток навичок критичного мислення в суспільстві. Пропаганда та маніпуляція інформацією можуть серйозно впливати на сприйняття реальності та призводити до негативних наслідків [27, с. 86-87]. Зміна сприйняття та ментальних операцій може мати серйозні наслідки для індивіда та суспільства в цілому.

Злочинність проти людини в цифровому просторі тепер включає також психологічний тиск, кібербулінг, створення фейкових новин для дезорієнтації та інші форми впливу на її когнітивні процеси. При цьому, стійке цифрове суспільство не може бути таким без когнітивно стійких громадян. Суспільство, яке легко піддається маніпуляціям, є вразливим до дезінформації, що може призвести до соціальної дестабілізації, паніки та навіть прямого вчинення злочинів під впливом неправдивої інформації. Тому формування критичного мислення та медіаграмотності є невід'ємною частиною цифрової стійкості [28, с. 178].

Різниця між кіберстійкістю держави і індивіда полягає в масштабі та рівні регулювання: а) держава діє системно, забезпечуючи безпеку національних ресурсів, б) особа покладається на індивідуальні практики та добровільні стандарти. Водночас обидва рівні взаємопов'язані коли низька кіберстійкість громадян підвищує ризики для держави, а слабка державна політика створює загрози для кожного громадянина, користувача у цифровому просторі.

Вирішальне значення для імплементації міжнародних превентивних моделей має встановлення чіткого балансу між кіберстійкістю держави та конституційними правами громадян, що знаходиться під суворим контролем Європейського суду з прав людини (ЄСПЛ). Будь-які кримінально-правові чи адміністративні заходи превенції кіберзлочинності, що обмежують права, мають відповідати алгоритму ЄСПЛ: а) бути встановленими законом; б) переслідувати легітимну мету, в) бути необхідними у демократичному суспільстві (пропорційними).

Позиція ЄСПЛ у справі Dmitriyevskiy v. Russia, 29.01.2018 має значення для визначення меж державного втручання в умовах гібридної війни та зростання кіберзагроз [30]. Суд підтвердив, що цілі національної безпеки, територіальної цілісності та громадської безпеки, якими держава виправдовує втручання, повинні тлумачитися обмежувально. Це означає, що кримінально-правові заходи превенції кіберзлочинності (наприклад, моніторинг комунікацій чи блокування контенту) можуть бути застосовані лише тоді, коли держава переконливо доведе наявність нагальної соціальної потреби. ЄСПЛ вимагає, щоб втручання було пропорційним переслідуваним законним

цілям і відповідало поняттю «необхідності в демократичному суспільстві». Надмірні повноваження правоохоронних органів без належного судового контролю, навіть під приводом боротьби з кіберзлочинністю, можуть бути визнані порушенням ст. 10 (свобода вираження поглядів) або ст. 8 (право на приватність) Європейської Конвенції **з** прав людини [26]. Справа встановлює критерії оцінки контенту, який, хоча й не містить прямого заклику до насильства, може бути спрямований на розпалювання ворожнечі, ненависті чи нетерпимості. Це положення має пряме відношення до когнітивної безпеки та криміналізації дезінформації в Україні, оскільки дозволяє правоохоронним органам вживати превентивних заходів проти висловлювань, що можуть призвести до шкідливих наслідків або злочинів на ґрунті ненависті (*hate crimes*) у цифровому просторі. Таким чином, імплементація міжнародних превентивних моделей в Україні повинна суворо відповідати цим стандартам ЄСПЛ, забезпечуючи баланс між ефективною протидією кіберзагрозам та захистом фундаментальних прав людини. Забезпечення цього балансу вимагає не лише реактивного застосування кримінально-правових норм, а й проактивного впровадження комплексних превентивних стратегій, які охоплюють правові, технічні та когнітивні аспекти. Саме тому, подальший аналіз фокусується на структуруванні та адаптації ключових міжнародних превентивних моделей у цифровий простір.

Забезпечення національної кіберстійкості та гарантування конституційних прав громадян в умовах гібридних загроз вимагає проактивного впровадження комплексних превентивних моделей, що охоплюють правові, інституційні, технічні та когнітивні аспекти. Застосування цих міжнародних стандартів має відповідати критеріям ЄСПЛ, забезпечуючи необхідний баланс між ефективною протидією кіберзагрозам та захистом фундаментальних прав людини.

Для формування в Україні кіберстійкості держави та людини як синтезу загального поняття національної кіберстійкості найбільш релевантними є три ключові моделі превенції, кожна з яких впливає на стійкість на різних рівнях.

Право-регуляторна модель (конвенційна основа) знаходить своє концептуальне втілення у превентивній моделі ОБСЄ та Ради Європи. Саме вона фокусується на гармонізації законодавства та діалектиці прав і безпеки, використовуючи Будапештську конвенцію як інструмент уніфікації кримінально-правових норм, встановлюючи універсальні визначення кіберзлочинів та механізми міжнародного співробітництва, що забезпечує законність будь-якого втручання., а практику ЄСПЛ – як гаранта пропорційності державного втручання. Водночас, забезпечення безпеки вимагає певних обмежень приватності (моніторинг комунікацій чи доступ до електронних доказів), що створює «діалектику» у формі постійної напругу між захистом індивідуальної недоторканності та необхідністю ефективної протидії злочинності. Будь-які втручання мають бути суворо пропорційними до легітимної мети, чітко регламентованими законом і підлягати належному судовому контролю. Для результативного реагування необхідне функціонування ефективної правової основи, яка б забезпечувала оперативний доступ до електронних доказів та співпрацю з постачальниками інтернет-послуг.

Для національної практики правозастосування важливо забезпечити пропорційність превентивних заходів, узгодивши процедури доступу до електронних доказів із практикою ЄСПЛ, та завершити гармонізацію кримінального законодавства з міжнародними конвенційними вимогами.

Наступна модель технічного та інституційного характеру (стійкість системи) (відділ CCIPS та NCIJTF США) демонструє, що превентивна здатність прямо залежить від створення спеціалізованих підрозділів у правоохоронній системі. Ці структури, а особливо кадровий склад, мають володіти необхідними технічними знаннями та навичками кіберрозслідувань, функціонуючи не лише реактивно, а й проактивно у моніторингу та запобіганні загрозам. Впровадження сучасних систем інформаційної безпеки (шифрування, аутентифікація, антивірусний захист) створює технічні бар'єри, що є першим рівнем захисту конституційних прав на приватність, власність у цифровій сфері.

В Україні доцільно впровадити стандарти NIS2 для всіх суб'єктів критичної інфраструктури та посилити інституційну спеціалізацію правоохоронних органів для забезпечення високої якості кіберрозслідувань та протидії високотехнологічним злочинам.

Модель когнитивної превенції та освітньої стійкості, спрямованої на захист індивіда, виступає найбільш важливою для превентивного захисту прав людини від маніпуляцій, що часто є початковою фазою кіберзлочину. Когнітивна безпека становить здатність людини критично сприймати та опрацьовувати інформацію, захищаючи власну свідомість від маніпуляцій, дезінформації та цілеспрямованого психологічного впливу. У цьому напрямі, просвітницькі кампанії з медіаграмотності виступають основним інструментом, що підвищує когнітивну стійкість громади проти злочинного вербування та шахрайства. Це безпосередньо стосується превенції злочинності проти особи, оскільки маніпуляції свідомістю часто є першим кроком до вчинення шахрайства. Гарантування права людини на вільний вибір та об'єктивну інформацію становить невід'ємну частину сучасної кримінально-правової політики.

У контексті запровадження цієї моделі в Україні, важливо інтегрувати когнітивну безпеку та медіаграмотність у національну освітню стратегію як пріоритетний інструмент кримінологічної превенції на рівні особи, знижуючи її віктимність та мінімізуючи негативні наслідки впливу загроз локального і глобального характеру.

Висновки. Ключовим результатом дослідження стало наукове обґрунтування того, що ефективна кримінально-правова політика превенції кіберзлочинності в Україні має ґрунтуватися на багаторівневій імплементації міжнародних превентивних моделей, яка створює синергію між кіберстійкістю держави та особи. Системний аналіз засвідчив, що забезпечення конституційних прав громадян у цифровому просторі можливе лише за умов усвідомлення та практичної реалізації взаємозалежності кіберстійкості держави та особи. Дослідження підтвердило, що кіберстійкість держави та особи є взаємопов'язаною основою для формування ефективної превенції: державний рівень (Макрорівень) забезпечує нормативну, інституційну та технічну базу для захисту критичної інфраструктури, що є необхідною умовою для гарантування конституційних прав громадян; тоді як індивідуальний рівень (Мікрорівень) безпосередньо знижує ризики віктимності. Без належного рівня цифрової грамотності громадян навіть найсучасніші державні механізми залишаються недостатньо ефективними.

Вдосконалення кримінально-правової політики превенції кіберзлочинності прямо залежить від імплементації міжнародних превентивних моделей. Це передбачає: гармонізацію законодавства з директивами ЄС (NIS2, GDPR) та положеннями Будапештської конвенції (конвенційно-правова модель); забезпечення інституційної бази та технічної готовності критичної інфраструктури (інституційно-технічна модель); а також пріоритетність освітніх програм з кібергігієни та психологічної стійкості до маніпуляцій (когнітивно-освітня модель).

З огляду на це, комплексний підхід до кіберстійкості передбачає синергію правових, технічних та освітніх механізмів, що дозволяє не лише реагувати на кіберзлочини, а й запобігати їм. Для подальшого вдосконалення кримінально-правової політики превенції в Україні актуальною є необхідність розробки уніфікованих індикаторів кіберстійкості, створення єдиної національної платформи кіберосвіти з фокусом на когнітивній безпеці та внесення системних змін до кримінального законодавства для врахування нових форм кіберзлочинності.

Об'єктом подальших наукових розвідок, на національному рівні, можуть бути питання, пов'язані із імплементацією міжнародних превентивних моделей у кримінально-правову політику України; вдосконалення законодавства щодо охорони об'єктів у цифровому просторі та розробки механізмів превенції кіберзлочинності, що враховують синергію державної та індивідуальної кіберстійкості. Сьогодні особливого значення набувають проблеми забезпечення інформаційної безпеки та захисту персональних даних у контексті глобальних стандартів (GDPR, NIS2), а також інтеграція освітніх і соціальних програм для формування культури безпечної поведінки громадян у кіберпросторі.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Yuzikova N.S., Korniakova T.V., Chumak A. Enforcement of the functions of the judiciary with artificial intelligence A.S. *Visegrad Journal on Human Rights*. № 1, 2022. S. 177–182. URL: https://journal-vjhr.sk/wp-content/uploads/2022/04/ VJHR_ 1_2022.pdf.
2. Юзікова Н.С. Інформаційна безпека у системі заходів запобігання кримінальним правопорушенням у сфері інформаційних технологій: досвід країн ЄС та США. *Аналітично-порівняльне правознавство* 2023. № 5. С. 506–512. DOI: https://doi.org/10.24144/2788-6018.2023.05.91. URL: https://app-journal.in.ua/wp-content/uploads/2023/10/APP_05_2023.pdf.
3. Бочковой В.А., Бааджи Н.А. Обмеження цифрових прав людини в умовах сучасних правових викликів. *Науоквий вісник УжНУ. Серія: Право.* 2024. URL: https://doi.org/10.24144/2307-3322.2024.84.4.31.
4. Тверезовська К.С. (2024). Поняття, види та значення цифрових прав людини. *Юридичний науковий електронний журнал*. № 6. 2024. URL: https://doi.org/10.32782/2524-0374/2024-6/119.
5. Петришин О.В., Гиляка О.С. Права людини в цифрову епоху: виклики, загрози та перспективи. *Journal of the National Academy of Legal Sciences of Ukraine*. 2021. https://doi.org/10.37635/jnalsu.28(1).2021.15-23.
6. Коломоєць Т., Верлос Н., Нікітенко В., Воронкова В. Цифрові права людини в умовах розвитку штучного інтелекту та глобалізації. *Human Studies*. 2024. URL: https://doi.org/10.32782/hst-2024-20-97-24.
7. Размєтаєва Ю.С. Цифрові права людини та проблеми екстериторіальності в їх захисті. Право та державне управління. 2020. № 4. С. 18–23. DOI: https://doi.org/10.32840/pdu.2020.4.2. URL: http://pdu-journal.kpu.zp.ua/archive/4_2020/4.pdf.

8. Тарасенко Л. Право на доступ до інтернету. Вісник Львівського університету. Серія юридична. 2020. Випуск 71. № 6.2024. С. 53–61. URL: https://publications.lnu.edu.ua/bulletins/index.php/law/article/view/11022.
9. Chiara, P.G. (2025). Understanding the regulatory approach of the Cyber Resilience Act: Protection of fundamental rights in disguise? *European Journal of Risk Regulation*. https://doi.org/10.1017/err.2025.9.
10. Calderaro, A. (2025). Human rights and cybersecurity: Contentious communities in cyber diplomacy practice. In *Cybersecurity and human rights*. Springer. https://doi.org/10.1007/978-3-031-93385-1_10.
11. Hulkó, G., & Kálmán, J. (2025). The politics of digital sovereignty and the European Union's legislation: Navigating crises. *Frontiers in Political Science*. https://doi.org/10.3389/fpos.2025.1548562.
12. Livingstone, S., Stoilova, M., & Kardefelt-Winther, D. (2016). Global kids online: Researching children's rights globally in the digital age. *Journal of Children and Media*. https://doi.org/10.1177/2043610616676035.
13. Third, A., Livingstone, S., & Lansdown, G. (2024). Recognizing children's rights in relation to the digital environment: Challenges of voice and evidence. In *Research handbook on human rights and digital technology*. Edward Elgar Publishing. https://doi.org/10.4337/9781035308514.00026.
14. Djeffal, C. (2022). Children's rights by design and internet governance. *Laws, 11*(6), 84. https://doi.org/10.3390/laws11060084.
15. Wagner, B., & Kettemann, M. (Eds.). (2024). *Research handbook on human rights and digital technology*. Edward Elgar Publishing. https://doi.org/10.4337/9781035308514.
16. Macdonald, K. (2023). *Cybercrime: Awareness, prevention, and response*. Emond Publishing. https://emond.ca/Store/Books/Cybercrime-Awareness-Prevention-and-Response.
17. Human Rights by Design. Council of Europe (2019). URL: https://rm.coe.int/-human-rights-by-design-future-proofing-human-rights-protection-in-the/1680ab2279.
18. Committee on the Rights of the Child UN. General Comment No. 25 (2021). URL: https://www.ohchr.org/en/documents/general-comments-and-recommendations/general-comment-no-25-2021-childrens-rights-relation.
19. Amanda Third, Philippa Collin, Catharine Fleming, Benjamin Hanckel, Lilly Moody, Teresa Swist & Georgina Theakstone. Governance, children's rights and digital health. URL: https://www.governinghealthfutures2030.org/wp-content/uploads/ 2021 /10/Governance-childrens-rights-and-digital-health.pdf.
20. Dunstan Allison-Hope. Human Rights by Design. Februa 17, 2017. URL: https://www.bsr.org/en/blog/human-rights-by-design.
21. Christian Djeffal. Children's rights by design and internet governance: revisiting general comment no. 25 (2021) on children's rights in relation to the digital environment. TUM School of Social Sciences and Technology. Technical University of Munich. Munich. Germany. URL: https://www.mdpi.com/2075-471X/11/6/84.
22. Про рішення ради національної безпеки і оборони України від 15.10.2021 р. «Про стратегію інформаційної безпеки»: Указ Президента України від 28.12. 2021 р. № 685/2021. URL: https://zakon.rada.gov.ua/laws/show/ 685/ 2021#n33.
23. Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації: Рішення РНБО від 29 грудня 2016 року. URL: https://zakon.rada.gov.ua/laws/show/n0015525-16#Text.
24. Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про Доктрину інформаційної безпеки України». Указ Президента України від 25 лютого 2017 р. № 47/2017. URL: https://zakon.rada.gov.ua/laws/show/47/2017#Text.
25. Конвенція про захист прав людини і основоположних свободи. URL: http://zakon4.rada.gov.ua/laws/show/-995004#Text.
26. Почепцов Г.Г. Теория комунікації К.: Ваклер, 2001. 656 с.
27. Олійник А.А. Формування стійкого цифрового суспільства: превентивна роль інформаційної безпеки та кримінально-правової політики у запобіганні злочинності. *Актуальні проблеми вітчизняної юриспруденції* № 2. 2025. С. 177–182. DOI: https://doi.org/10.32782/2408-9257-2025-2-27. URL: http://apnl.dnu.in.ua/2_2025/29.pdf.
28. Dmitriyevskiy v. Russia від 29.01.2018. URL: https://hudoc.echr.coe.int/eng?i=001-177214.