ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 4 (14), 2024

УДК 342.7: 316.4: 004.056
DOI 10.31732/2708-339X-2024-14-A13

КІБЕРБЕЗПЕКА: ВИКЛИКИ ЦИФРОВОЇ ЕРИ ЧЕРЕЗ ПРИЗМУ КОНГРЕСУ ООН У КІОТО

Горєлова В.Ю.,
кандидат юридичних наук
доцент кафедри державно-правових дисциплін
Університету економіки та права «КРОК»
Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: HorelovaVY@krok.edu.ua
ORSID: https://orcid.org/0000-0001-6536-2422

CYBERSECURITY: CHALLENGES OF THE DIGITAL AGE THROUGH THE PRISM OF THE UN CONGRESS IN KYOTO

Horielova V.Yu.,
candidate of legal sciences
associate professor of department of state legal sciences of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: HorelovaVY@krok.edu.ua
ORSID: https://orcid.org/0000-0001-6536-2422

Анотація. *У статті розглядаються ключові проблеми кіберзлочинності, які були предметом обговорення на 14-му Конгресі ООН [1] із запобігання злочинності, що проходив у Кіото. Особливий акцент зроблено на етичних аспектах і правах людини в контексті забезпечення кібербезпеки. Аналізуються сучасні виклики, з якими стикається міжнародна спільнота у боротьбі з кіберзлочинністю, а також можливості застосування передових технологій, таких як штучний інтелект (ШІ) та великі дані, для протидії цій загрозі. Виявлено, що використання технологій стеження, зокрема систем моніторингу онлайн-активності, аналізу користувацьких даних чи впровадження масового спостереження, хоча й має значний потенціал у боротьбі з кіберзлочинністю, водночас створює серйозні етичні та правові проблеми. Зокрема, такі методи можуть порушувати основоположні права і свободи людини, серед яких право на приватність, свободу вираження поглядів та свободу пересування у цифровому середовищі. У статті наголошується на необхідності обмеження використання таких технологій і забезпечення їх відповідності міжнародним етичним стандартам. Підкреслюється, що для ефективної протидії кіберзлочинності в сучасних умовах необхідно вдосконалювати національні законодавства, які мають адаптуватися до стрімкого розвитку новітніх технологій та глобальних викликів. Вказується на те, що існуючі закони повинні не лише забезпечувати належну правову відповідальність за кіберзлочини, але й створювати нормативну базу для регулювання технологій, що використовуються у сфері кібербезпеки. Зроблено зауваження що до того, що законодавчі норми враховували потребу у захисті людської гідності, приватності та свободи в умовах цифровізації. Окремо виділяється необхідність включення етичних стандартів до законодавства, що регулює використання інноваційних технологій. Наголошено що етичні принципи повинні слугувати основою для забезпечення справедливості, прозорості й підзвітності у процесах, пов'язаних із кібербезпекою. Зокрема, це стосується використання ШІ для аналізу даних та прийняття рішень. Міжнародна співпраця в цій сфері визнається критично важливою, оскільки кіберзлочини не мають державних кордонів. Інтеграція етичних стандартів у національні законодавства, зокрема в Україні, сприятиме створенню більш безпечного цифрового простору. У статті наголошується на важливості обміну досвідом між країнами, співпраці у створенні єдиних нормативних підходів та формуванні глобальної культури відповідальності у сфері кібербезпеки.*

Ключові слова: *кіберзлочинність, кібербезпека, етика, права людини, міжнародна співпраця.*
Формул*: 0, рис.: 0, табл.: 0, бібл.: 14.*

Abstract. *The article examines key issues of cybercrime discussed at the 14th UN Congress on Crime Prevention held in Kyoto. Particular emphasis is placed on ethical aspects and human rights in the context of ensuring cybersecurity. The article analyzes the current challenges facing the international community in combating cybercrime, as well as the potential use of advanced technologies such as artificial intelligence (AI) and big data to counter this threat. It is revealed that while surveillance technologies, including online activity monitoring systems, user data analysis, and mass surveillance implementation, hold significant potential in the fight against cybercrime, they simultaneously raise serious ethical and legal concerns. In particular, these methods may violate fundamental human rights and freedoms, including the right to privacy, freedom of expression, and freedom of movement in the digital environment. The article emphasizes*

the need to limit the use of such technologies and ensure their compliance with international ethical standards. The authors stress that for effective counteraction to cybercrime in today's conditions, national legislation must be improved and adapted to the rapid development of new technologies and global challenges. Existing laws should not only ensure proper legal accountability for cybercrimes but also create a regulatory framework for technologies used in the cybersecurity sector. It is crucial that legislative norms consider the need to protect human dignity, privacy, and freedom in the context of digitalization. The article highlights the necessity of integrating ethical standards into the legislation regulating the use of innovative technologies. Ethical principles should serve as the foundation for ensuring fairness, transparency, and accountability in processes related to cybersecurity, particularly in the use of AI for data analysis and decision-making. International cooperation in this area is recognized as critically important, as cybercrimes transcend national borders. The integration of ethical standards into national legislation, particularly in Ukraine, will contribute to creating a safer digital space. The article underscores the importance of experience exchange between countries, cooperation in developing unified regulatory approaches, and fostering a global culture of responsibility in the cybersecurity sphere.
***Keywords**: cybercrime, cybersecurity, ethics, human rights, international cooperation.*
***Formulas**: 0, fig.: 0, tabl.: 0 bibl.: 14.*

Постановка проблеми. На сьогодні кіберзлочинність перетворилася на глобальний виклик, що вражає не лише окремі компанії чи установи, а й цілі суспільства, загрожуючи їх безпеці, економічній стабільності та правам людини. Постійне зростання кількості кібератак і складність сучасних цифрових загроз вимагають не лише технічних, але й правових та етичних рішень. Особливо гостро постає питання захисту персональних даних і дотримання прав людини в умовах стрімкого розвитку технологій. Відсутність єдиних стандартів реагування та недостатня міжнародна співпраця ускладнюють ефективну боротьбу з кіберзлочинністю на глобальному рівні.

Актуальність теми дослідження. Зростання кіберзлочинності та її вплив на різні сфери суспільного життя роблять питання кібербезпеки одним із найактуальніших у сучасному світі. Кібератаки на медичні установи, банківські системи та державні органи загрожують не лише економічній стабільності, а й безпеці громадян. У сучасних умовах цифрової трансформації особливого значення набуває забезпечення захисту персональних даних, конфіденційності та основоположних прав людини. Водночас використання технологій, таких як штучний інтелект та великі дані, вимагає етичного переосмислення та встановлення чітких правових рамок для їх застосування. Таким чином, дослідження цієї тематики є надзвичайно важливим для розробки ефективних механізмів кіберзахисту та інтеграції етичних стандартів у національне законодавство, що сприятиме безпечному розвитку цифрового суспільства [2].

Метою статті є дослідження сучасних викликів кіберзлочинності з акцентом на етичні та правові аспекти її подолання, а також розробка рекомендацій щодо впровадження міжнародних стандартів кібербезпеки та етичних принципів у законодавство України для забезпечення захисту прав людини в цифровому середовищі.

Аналіз останніх досліджень і публікацій. Праці закордонних науковців, таких як М. Бреннер, С. Гудман, Л. Шеллі, досліджують етичні аспекти кібербезпеки. Українські науковці Р.В. Лук'янчук, Ю. Бельський та О. Радутний аналізують національні механізми захисту від кіберзагроз, акцентуючи на правових та етичних аспектах.

Викладення основного матеріалу. 14-й Конгрес ООН із запобігання злочинності відбувся в 2020 році в місті Кіото, Японія, ставши важливою платформою для глобальних дискусій про сучасні загрози в сфері безпеки та стратегії їх подолання. Конгрес зібрав провідних експертів, політиків та представників державних і приватних організацій для обговорення новітніх тенденцій у сфері кримінального правосуддя, кібербезпеки та прав людини. Конгрес відкрила виконавча директорка Управління ООН з наркотиків і злочинності (UNODC) Гада Валлі [3], а президентом Конгресу [1] була міністерка юстиції Японії Йоко Камікава [4], яка акцентувала на важливості Кіотської декларації та необхідності міжнародної співпраці для досягнення Цілей сталого розвитку (SDG) через посилення правосуддя та безпеки. Основними темами, що обговорювались на Конгресі, стали глобальні виклики кіберзлочинності, зростання кібератак та важливість міжнародного співробітництва у боротьбі з цифровими загрозами. Конгрес зосередився на численних питаннях кібербезпеки, таких як захист персональних даних, боротьба з кібертероризмом і розвиток нових правових механізмів, здатних забезпечити ефективну реакцію на

нові типи кіберзлочинів. Особлива увага була приділена питанням етики в контексті кібербезпеки. Учасники наголошували на важливості балансування між необхідністю захисту інформації та дотриманням прав людини, зокрема конфіденційності особистих даних та захисту свободи слова. Місто Кіото стало важливою платформою для підвищення рівня обізнаності про виклики, з якими стикаються держави в умовах цифровізації. Японія, яка є одним із лідерів у сфері технологій, стала ідеальним місцем для проведення такого заходу. Конгрес у Кіото [1] сприяв розвитку міжнародних зв'язків та створенню єдиної стратегії для боротьби з кіберзлочинністю на глобальному рівні. Учасники Конгресу домовились про необхідність встановлення універсальних стандартів кібербезпеки, що мають сприяти ефективному реагуванню на кібератаки та захисту національних і глобальних інфраструктур. На Конгресі було порушено ряд важливих тем, серед яких: 1) зростання кіберзлочинності (учасники відзначили небезпечну тенденцію до збільшення кількості кібератак, які мають серйозні наслідки для економіки, державних інститутів та приватних осіб); 2) міжнародна співпраця (одним із основних напрямків дискусій стало питання про необхідність створення механізмів для обміну інформацією між державами та організаціями, що займаються кібербезпекою); 3) етичні питання (обговорювались аспекти захисту прав людини в умовах цифрових загроз, зокрема захист конфіденційності особистих даних та боротьба зі злочинним контентом в Інтернеті, не порушуючи основоположні свободи); 4) штучний інтелект та великі дані (обговорення зосередились на використанні сучасних технологій для боротьби з кіберзлочинністю, а також на потенційних етичних ризиках від їхнього використання в контексті стеження та збору персональної інформації). Завдяки цим дискусіям, 14-й Конгрес ООН [1] в Кіото став важливим етапом у формуванні міжнародної стратегії щодо кібербезпеки та етики в цифровому середовищі, визначивши ключові напрямки для подальшої роботи на глобальному та національному рівнях [5].

Кіберзлочинність охоплює широкий спектр злочинних дій, що здійснюються за допомогою інформаційно-комунікаційних технологій. Одним з найпоширеніших типів кіберзлочинів є атаки на фінансові установи, такі як банківські системи, що включають крадіжку особистих даних, шахрайство з кредитними картками та здійснення кібератак на платіжні системи. Зловмисники часто використовують фішинг, зловмисне програмне забезпечення (віртуальні віруси), а також методи відмови в обслуговуванні (DDoS-атаки) для крадіжки грошей або здійснення фінансових махінацій [6].

Іншим важливим напрямком кіберзлочинності є атаки на медичні установи. Зокрема, хакери часто цілеспрямовано атакують медичні бази даних для крадіжки особистої інформації пацієнтів, що може призвести до серйозних наслідків, таких як крадіжка ідентичності або продаж медичних записів на чорному ринку [7]. Крім того, зловмисники можуть здійснювати кібератаки на медичні пристрої або системи управління, що ставить під загрозу життя людей. Інші важливі типи кіберзлочинів включають атакування інфраструктури критичного значення, такої як енергетичні системи, транспортні мережі та водопостачання. Такі атаки можуть мати катастрофічні наслідки для громадської безпеки і здатні паралізувати цілі регіони або країни [8].

Кіберзлочинність є глобальним явищем, яке не знає кордонів. Хакери можуть здійснювати свої злочини з будь-якої точки світу, що ускладнює їх розслідування та покарання. Кіберзлочинці часто приховують свою діяльність, використовуючи методи анонімізації через мережі, такі як веб-пошукач «Tor»[9], або через заражені комп'ютери, що використовуються як «зомбі-мережі». Це створює додаткові труднощі для правопорядку, оскільки відсутність фізичних кордонів у кіберпросторі дозволяє злочинцям діяти з будь-якої країни, що знижує ефективність національних правових систем. Цей транснаціональний аспект кіберзлочинності вимагає міжнародного співробітництва для обміну даними про кіберзлочини, вироблення спільних стандартів безпеки та створення глобальних механізмів боротьби з кіберзлочинцями. Важливими інструментами для подолання кіберзлочинів є міжнародні угоди та організації, такі як Конвенція Ради Європи про кіберзлочинність (Будапештська конвенція) [10] та «Інститут Інтерполу», які працюють над забезпеченням міжнародного правопорядку в кіберпросторі [11]. Слід зазначити, що кіберзлочинність має

серйозні наслідки як для глобальної безпеки, так і для світової економіки. На глобальному рівні, кібератаки можуть спричиняти порушення функціонування державних інститутів, економічну дестабілізацію та загрози національній безпеці. Наприклад, кібератаки на електричні мережі, урядові структури або транспортні системи можуть паралізувати критичні елементи державної інфраструктури та створити хаос у суспільстві а економічні наслідки кіберзлочинності є надзвичайно великими. Так, згідно з оцінками, глобальні втрати від кіберзлочинності досягли трильйонів доларів, що включає не лише прямі фінансові збитки, але й витрати на відновлення після атак, компенсацію постраждалим та заходи для забезпечення безпеки в майбутньому. Багато компаній витрачають значні ресурси на забезпечення кібербезпеки та відновлення своїх систем після атак, що знижує ефективність їхньої роботи та може призводити до втрати довіри споживачів. Відтак, кіберзлочинність є серйозним викликом для глобальної безпеки та економіки, і боротьба з цими загрозами вимагає ефективної міжнародної співпраці, зміцнення правових норм та розвитку нових технологій для протидії злочинності в цифровому середовищі.

Одним з основних викликів, з якими стикається сучасне суспільство в умовах цифрових загроз, є забезпечення захисту прав людини в кіберпросторі. Кібербезпека, з одного боку, є необхідною для захисту від злочинних дій, таких як крадіжка особистих даних, шахрайство, кібератаки на критичні інфраструктури, а з іншого – вимагає дотримання фундаментальних прав і свобод, таких як право на приватність, свободу слова та право на доступ до інформації. У контексті цифрових загроз важливо підтримувати баланс між забезпеченням безпеки та захистом прав людини. Наприклад, застосування засобів кібербезпеки, таких як моніторинг інтернет-активності громадян для виявлення потенційних кіберзлочинців, не повинно порушувати права на конфіденційність та особисту недоторканність. Використання новітніх технологій для виявлення кіберзлочинів повинно здійснюватися з дотриманням етичних принципів, що враховують потребу в захисті базових прав людини в цифровому середовищі.

Однією з найскладніших етичних дилем у сфері кібербезпеки є питання балансу між конфіденційністю особистих даних і необхідністю боротьби з кіберзлочинами. Боротьба з кіберзлочинністю вимагає використання потужних технологій для моніторингу та аналізу великих обсягів інформації, однак це може призводити до порушень права на приватність. З одного боку, ефективне виявлення та попередження кіберзлочинів, таких як фінансові шахрайства чи кібертероризм, потребує доступу до великої кількості особистих даних. З іншого боку, ці дії можуть призвести до ненавмисного вторгнення в особисте життя громадян і порушення їхніх прав на конфіденційність. Тому важливо розробляти правові норми, які дозволяють забезпечити ефективний захист від кіберзлочинців, не порушуючи при цьому прав громадян на приватність.

Використання технологій стеження для боротьби з кіберзлочинністю, таких як системи моніторингу онлайн-активності, аналізування даних користувачів чи впровадження систем масового стеження, може призвести до значних етичних і правових проблем. Хоча ці технології можуть допомогти у виявленні та запобіганні кіберзлочинам, вони також створюють ризик виникнення явища, яке часто називають «великою братом» – постійного нагляду за громадянами державою чи іншими суб'єктами. Ці технології можуть бути використані для моніторингу особистої діяльності громадян у мережі, що викликає побоювання щодо зловживань та порушень основоположних прав людини. Постійне стеження може спричинити втрату приватності, обмеження свободи вираження думок і навіть використовуватись для політичних чи соціальних репресій [112]. Етичні аспекти такого стеження полягають у питаннях, наскільки далеко можна йти в обмеженні прав людини заради забезпечення національної безпеки чи боротьби з кіберзлочинністю. Тому важливо, щоб використання технологій стеження мало чіткі обмеження, контролювалося відповідними інститутами та не призводило до серйозних порушень основних прав і свобод людини. Таким чином, етичні та правові аспекти кібербезпеки полягають у необхідності забезпечення захисту від кіберзлочинності без шкоди для прав людини, що потребує створення чіткої правової бази, яка балансуватиме між безпекою та особистими свободами. Таким чином, одним із ключових аспектів міжнародної співпраці у боротьбі з кіберзлочинністю

є необхідність створення єдиних стандартів реагування на кібератаки. Кіберзлочинність не має національних кордонів, що ускладнює боротьбу з нею на рівні окремих країн. Тому саме міжнародне співробітництво є надзвичайно важливим для ефективного вирішення проблеми.

На Конгресі ООН [1] з запобігання злочинності в Кіото було підкреслено важливість формулювання спільних міжнародних стандартів для реагування на кібератаки, які б дозволяли країнам обмінюватися інформацією, координувати свої дії і запобігати поширенню кіберзлочинів. Такі стандарти повинні охоплювати визначення кіберзлочинності, стратегії протидії кіберзагрозам, а також механізми юридичного співробітництва для оперативного розслідування та покарання винних.

Крім того, вважається необхідним створювати міжнародні платформи для обміну досвідом, найкращими практиками та технологіями, що дозволяють ефективно реагувати на нові загрози у кіберпросторі. Ці ініціативи можуть сприяти швидкому реагуванню на атаки та мінімізації їхніх негативних наслідків для глобальної безпеки. Обмін інформацією між країнами є основою ефективної боротьби з кіберзлочинністю, адже у глобалізованому світі кіберзагрози можуть виникати в будь-якій точці планети і швидко поширюватися через цифрові канали. Тому без швидкого і ефективного обміну інформацією між урядами, правоохоронними органами, міжнародними організаціями та приватним сектором не можна забезпечити достатній рівень кібербезпеки.

Важливими елементами цього процесу є створення міжнародних баз даних для обміну інформацією про кіберзлочини, розробка стандартів щодо збору і обміну доказами кіберзлочинів, а також сприяння співпраці між державами в розслідуванні кібератак. Оскільки кіберзлочинці часто діють анонімно і використовують території кількох країн, координація між країнами є необхідною для запобігання, виявлення та покарання таких злочинів. Приналежно, в рамках міжнародних організацій, таких як Інтерпол та Європол, були створені спеціалізовані підрозділи для боротьби з кіберзлочинністю, що дозволяють здійснювати обмін даними про кіберзлочини та координувати дії різних країн у відповідь на спільні загрози [13].

Приватний сектор відіграє критичну роль у забезпеченні кібербезпеки, оскільки більшість глобальних цифрових інфраструктур належать компаніям, а не державам. Інтернет-платформи, банки, медичні установи та інші організації регулярно стикаються з кіберзагрозами, тому їх залучення до боротьби з кіберзлочинністю вбачається обов'язковим.

Так, на Конгресі в Кіото [1] було зазначено важливість партнерства між державами і приватним сектором у забезпеченні кібербезпеки. Приватні компанії повинні не лише дотримуватися національних стандартів безпеки, але й активно співпрацювати з урядами для розробки та впровадження заходів з кіберзахисту. До таких заходів відносяться спільні дослідження та інновації в галузі кібербезпеки, а також активний обмін інформацією про нові загрози та вразливості. Приватний сектор також може допомогти у боротьбі з кіберзлочинністю через використання новітніх технологій, таких як штучний інтелект, аналіз великих даних та блокчейн. Ці технології можуть бути застосовані для виявлення та запобігання кіберзлочинам ще на етапі їх планування або підготовки.

Таким чином, міжнародна співпраця у боротьбі з кіберзлочинністю повинна включати ефективний обмін інформацією, створення єдиних стандартів реагування на кібератаки та залучення приватного сектору до захисту глобальної кіберінфраструктури. Тільки за умови комплексного підходу, що включає взаємодію держав, міжнародних організацій і приватних компаній, можна забезпечити ефективну протидію кіберзлочинності в умовах глобалізації цифрового середовища.

У сучасному світі боротьба з кіберзлочинністю стає дедалі більш складною через швидкий розвиток технологій, які використовуються не лише для забезпечення безпеки, а й для здійснення злочинних дій. Важливою складовою цієї боротьби є застосування новітніх технологій, таких як штучний інтелект (ШІ) та аналітика великих даних, що мають значний потенціал у сфері кіберзахисту. З одного боку, ці технології можуть забезпечити своєчасне виявлення та нейтралізацію кіберзагроз, а з іншого — породжують низку етичних, правових і технічних проблем, які потребують ретельного аналізу та регулювання. Так, штучний інтелект і великі дані використовуються для аналізу величезних обсягів

інформації, що надходить із різних джерел, зокрема з кіберпростору, в реальному часі. Це дозволяє виявляти аномалії, які можуть свідчити про спроби здійснення кіберзлочинів, таких як фішинг, зломи чи шкідливі програми. ШІ може допомогти в автоматизації процесів виявлення та реагування на кіберзагрози, що істотно знижує час на реакцію та зменшує ризик успіху атаки. Великі дані, в свою чергу, забезпечують можливість здійснювати комплексний аналіз та прогнозувати потенційні загрози, що дозволяє будувати більш ефективні стратегії кіберзахисту.

Проте використання цих технологій несе з собою не тільки переваги, але й суттєві ризики. Одним із головних ризиків є проблема захисту приватності особистих даних. ШІ і великі дані здатні збирати та обробляти великі обсяги персональної інформації, що ставить під загрозу конфіденційність. За допомогою таких технологій можна не лише захистити дані, а й порушити основні права людини, зокрема право на приватність та свободу особистої інформації. З цієї точки зору, етичні питання стають надзвичайно важливими, оскільки застосування штучного інтелекту в контексті кібербезпеки повинно забезпечувати баланс між захистом інтересів держави та правами людини [14].

В Україні, як і в багатьох інших країнах, проблема кіберзлочинності є однією з найважливіших у контексті національної безпеки. Проте для ефективної боротьби з кіберзлочинами необхідно вдосконалювати національне законодавство, яке наразі потребує адаптації до новітніх технологій і глобальних викликів [15]. Закони повинні не лише забезпечувати правову відповідальність за кіберзлочини, а й включати етичні стандарти, що регулюють використання новітніх технологій у сфері кібербезпеки [16]. Важливим елементом цього процесу є створення законодавчих норм, які забезпечують прозорість і підзвітність при використанні технологій штучного інтелекту та аналізу великих даних у боротьбі з кіберзлочинами [17].

У цьому контексті рекомендації для України, засновані на результатах Конгресу ООН [1] у Кіото, передбачають необхідність розвитку національної політики в сфері кібербезпеки на основі етичних принципів, таких як прозорість, справедливість та відповідальність. Важливо інтегрувати міжнародні стандарти у національне законодавство, зокрема щодо обміну інформацією між країнами і координації дій на глобальному рівні. Крім того, необхідно залучати приватний сектор до захисту кіберінфраструктури, оскільки саме він є основним оператором сучасних цифрових технологій.

Одним із важливих аспектів є розвиток міжнародної співпраці, зокрема щодо обміну інформацією про кіберзагрози, що дозволяє державам швидше реагувати на кібернапади та запобігати їх поширенню. Враховуючи глобальний характер кіберзлочинності, країни повинні співпрацювати не лише в сфері правового регулювання, а й у розробці технологічних рішень для захисту від нових видів кіберзлочинів.

Отже, варто підкреслити, що результати Конгресу ООН [1], що відбувся в Кіото, створили потужну основу для глобальної боротьби з кіберзлочинністю, акцентуючи увагу на необхідності інтеграції етичних принципів у політику кібербезпеки. Дане питання є важливим для гармонійного розвитку цифрового суспільства, яке повинне не лише реагувати на кіберзагрози, але й забезпечувати права людини в умовах технологічних змін. Перспективи розвитку кібербезпеки у майбутньому полягають у постійному вдосконаленні міжнародного співробітництва, розвитку новітніх технологій та створенні правових і етичних стандартів, що гарантуватимуть захист прав громадян у цифровому світі.

Література:

1. United Nations. URL: https://www.unodc.org/unodc/en/justice-and-prison-reform/cpcj-kyoto-crime-congress-2021.html. (дата звернення: 13.11.2024)

2. Європейське агентство з кібербезпеки (ENISA). Кібербезпека та кіберзлочинність в ЄС. ENISA Publications, 2022. URL: https://www.enisa.europa.eu/publications. (дата звернення: 13.11.2024)

3. United Nations. URL: https://www.un.org/sg/ru/content/profiles/ghada-waly. (дата звернення: 13.11.2024)

4. Yoko Kamikawa Office. URL: https://www.kamikawayoko.net(дата звернення: 13.11.2024)

5. Організація Об'єднаних Націй. 14-й Конгрес ООН з попередження злочинності та кримінальної юстиції. UNODC, 2018. URL: https://www.unodc.org/unodc/en/commissions/CCPCJ/14th-ccpcj.html. (дата звернення: 13.11.2024)

6. APWG. URL: https://apwg.org/trendsreports/.(дата звернення: 13.11.2024)
7. Frontiers in Computer Science. URL: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full. (дата звернення: 13.11.2024)
8. United States Agency for International Development. URL:. https://www.usaid.gov/ukraine/fact-sheets/aug-05-2022-cybersecurity
9. Tor Browser. URL: https://www.torproject.org/.(дата звернення: 13.11.2024)
10. Рада Європи. Конвенція про кіберзлочинність. Угода № 185, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. (дата звернення: 13.11.2024)
11. World Economic Forum. URL: https://www.weforum.org/stories/2021/11/cyber-security-evolving-cyber-crime-attacks/.(дата звернення: 13.11.2024)
12. The impacts on society and people. URL: https://digitalsociology.org.uk/ethics-digital-surveillance/.(дата звернення: 13.11.2024)
13. Christen, M., Gordijn, B., Loi, M. The Ethics of Cybersecurity. Springer, 2021.
14. Kranenbarg, M. W., Leukfeldt, R. Artificial Intelligence and Cybersecurity: The Impact on Legal and Ethical Issues. Springer, 2021.

References:

1. United Nations. URL: https://www.unodc.org/unodc/en/justice-and-prison-reform/cpcj-kyoto-crime-congress-2021.html(Accessed November 13, 2024)
2. European Cyber Security Agency (ENISA). Cybersecurity and cybercrime in the EU. ENISA Publications, 2022. URL: https://www.enisa.europa.eu/publications. (Accessed November 13, 2024)
3. United Nations. URL:https://www.un.org/sg/en/content/profiles/ghada-waly (Accessed November 13, 2024)
4. Yoko Kamikawa Office. URL: https://www.kamikawayoko.net(Accessed November 13, 2024)
5. United Nations. 14th United Nations Congress on Crime Prevention and Criminal Justice. UNODC, 2018. URL:https://www.unodc.org/unodc/en/commissions/CCPCJ/14th-ccpcj.html. (Accessed November 13, 2024)
6. APWG.2023. URL: https://apwg.org/trendsreports (Accessed November 13, 2024)
7. Frontiers in Computer Science.2022. URL: https://www.frontiersin.org/journals/computer-science/articles/10.3389/fcomp.2021.563060/full /. (Accessed November 13, 2024)
8. United States Agency for International Development. URL: https://www.usaid.gov/ukraine/fact-sheets/aug-05-2022-cybersecurity. (Accessed November 13, 2024)
9. Tor Browser. URL: https://www.torproject.org/. (Accessed November 13, 2024)
10. Council of Europe. Convention on Cybercrime. Agreement No. 185, 2001. URL: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185. (Accessed November 13, 2024)
11. World Economic Forum. URL: https: //www.weforum.org/stories/2021/11/cyber-security-evolving-cyber-crime-attacks/. (Accessed November 13, 2024)
12. The impacts on society and people. URL: https: //digitalsociology.org.uk/ethics-digital-surveillance. (Accessed November 13, 2024)
13. Christen, M., Gordijn, B., Loi, M. (2021). The Ethics of Cybersecurity. Springer
14. Kranenbarg, M. W., Leukfeldt, R.(2021). Artificial Intelligence and Cybersecurity: The Impact on Legal and Ethical Issues. Springer

Стаття надійшла до друку 15 листопада 2024 року