ISSN (Print) 2708-339X ISSN (Online) 2786-7498
Legal Bulletin № 3 (13), 2024

УДК 351
DOI 10.31732/2708-339X-2024-13-A11

ПРАВОВЕ ЗАБЕЗПЕЧЕННЯ ТА ПЕРСПЕКТИВИ РОЗВИТКУ ДЕРЖАВНОЇ ПОЛІТИКИ У СФЕРІ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

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

Вихрист С.М.,
кандидат юридичних наук
доцент кафедри державно-правових дисциплін
Університету економіки та права «КРОК»
м. Київ, вул. Табірна, 30-32, Україна, 03113
e-mail: smvykhryst@krok.edu.ua
ORSID: https://orcid.org/0000-0002-3844-1165

LEGAL SUPPORT AND PROSPECTS FOR THE DEVELOPMENT OF STATE POLICY IN THE FIELD OF INFORMATION SECURITY

Horielova V.Y.,
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

Vikhryst S.M.,
candidate of legal sciences
associate professor of department of state legal sciences of «KROK» University
Kyiv, Tabirna St., 30-32, Ukraine, 03113
e-mail: smvykhryst@krok.edu.ua
ORSID: https://orcid.org/0000-0002-3844-1165

Анотація*. Стаття присвячена дослідженню сучасного стану правового забезпечення державної політики у сфері інформаційної безпеки та визначенню концептуальних напрямків розвитку даної політики. В статті узагальнено правове надбання українського народу, що висвітлено в положеннях Основного закону України. Досліджено підґрунтя правового забезпечення у сфері інформаційної безпеки, що міститься в положеннях міжнародних договорів, ратифікованих нашою державою та згода на обов'язковість яких надана Верховною Радою України. Окрім того, окреслені перспективні напрямки розвитку державної політики у сфері інформаційної безпеки, що знаходяться на етапі розробки у міжнародних організаціях у сфері інформаційних технологій та спрямовані на створення новітніх стандартів щодо боротьби з кіберзлочинністю та забезпечення інформаційної безпеки на міжнародному рівні. Стверджується, що перспективними кроками до розвитку державної політики України у сфері інформаційної безпеки має бути комплексний підхід, який враховуватиме сучасні виклики в цифровому просторі з метою створення умов для безпечного функціонування кіберпростору та його використання в інтересах особи, суспільства і держави. Встановлено, що персективним підґрунтям для формування державної політики може слугувати міжнародні форуми та центри глобальної співпраці з кібербезпеки, які засновані і діють в якості глобальної ініціативи для обміну знаннями з метою зміцнення спроможностей у сфері кібербезпеки шляхом співпраці між урядами, міжнародними організаціями та приватним сектором а також з метою спрямування на об'єднання зусиль різних держав і організацій для покращення міжнародного співробітництва в питаннях кібербезпеки, обміну інформацією та розробки спільних стандартів. У статті підсумовується коло ключових напрямків розвитку державної політики у сфері інформаційної безпеки.*

Ключові слова: *інформаційна безпека, право, державна політика, інформація.*

***Формул**: 0, рис.: 0, табл.: 0, бібл.: 12.*

***Abstract**. The article is devoted to the study of the current state of legal support for the state policy in the field of information security and the determination of conceptual directions for the development of this policy. The article summarizes the legal heritage of the Ukrainian people as reflected in the provisions of the Basic Law of Ukraine. The article examines the basis of legal support in the field of information security contained in the provisions of international treaties ratified by our state and ratified by the Verkhovna Rada of Ukraine. In addition, the article outlines promising areas for the development of the state policy in the field of information security, which are currently being developed by international organisations in the field of information technology and are aimed at creating the latest standards for combating cybercrime and ensuring information security at the international level. It is argued that promising steps towards the development of Ukraine's state policy in the field of information security should be an integrated approach that takes into account current challenges in the digital space to create conditions for the safe functioning of cyberspace and its use in the interests of the individual, society, and the State. It is established that international forums and centres for global cooperation on cybersecurity, which are established and operate as a global initiative for knowledge exchange to strengthen cybersecurity capabilities through cooperation between governments, international organisations, and the private sector, as well as aiming to unite the efforts of various states and organisations to improve international cooperation in cybersecurity, exchange of information, and the development of common standards, can serve as a prospective basis for public policy formation. The article summarizes the range of key areas for the development of the state policy in the field of information security.*

***Keywords**: information security, law, state policy, information.*
***Formulas**: 0, fig.: 0, tabl.: 0, bibl.: 12.*

Постановка проблеми. Питання забезпечення інформаційної безпеки в сучасному всесвіті проблематичне з огляду на багатогранність її структурних компонентів, які складаються не лише з правових, але й організаційно-розпорядчих та технічних елементів. Приналежно, правове забезпечення та регулювання інформаційної безпеки займає ключове місце, адже від правової визначеності впорядкування та контрою всіх розпорядчих дій і векторів державної політики залежить формування безпекоорієнтованого інформаційного середовища в Україні, тобто стрімкий розвиток цифровізації не повинен спричиняти шкоди людині та створювати потенційні загрози. Необхідним кроком забезпечення інформаційної безпеки є її ефективне правове забезпечення. Таким чином, вбачається за необхідне дослідити сучасний стан правового забезпечення інформаційної безпеки та виявити концептуальні засади щодо напрямків державної політики у даній сфері.

Актуальність теми дослідження. Посилення процесів цифровізації у сучасному світі, де інформаційні технології і цифрові комунікації займають центральне місце у життєдіяльності людини, питання інформаційної безпеки набирає надзвичайної актуальності. Правове забезпечення інформаціцної безпеки, таким чином, повинно охоплювати всі аспекти (від захисту особистих даних до забезпечення глобальної стабільності країни).

Метою статті є дослідження правового підґрунтя щодо забезпечення державної політики у сфері інформаційної безпеки; характеристика перспектив розвитку та засад щодо основних напрямків державної політики у у сфері інформаційної безпеки.

Аналіз останніх досліджень і публікацій. Серед останніх робіт, які присвячувались інформаційній безпеці на рівні дисертаційних досліджень у сфері права варто зазначити праці: І. І. Недохлєбова («Безпека України в умовах сучасних загроз: організаційно-правові аспекти, 2024 рік); І. О. Вдовіна («Організаційно-правові засади реалізації інформаційної безпеки України, 2024 рік); І. В. Кукіна («Механізми державного управління інформаційною безпекою особистості, 2024 рік); І. А. Сердюк («Організаційні засади публічного управління інформаційною безпекою суспільства в умовах загроз ментальному здоров'ю, 2023 рік) тощо. А також останні дисертаційні дослідження у сфері економіки, що пов'язані з вирішенням правих проблем таких науковців як: С. С. Білько «Формування інформаційної безпеки національної економіки (2024); Л. А. Асєєва «Управління інформаційною безпекою підприємства з використанням методів машинного навчання та нечіткої логіки» (2024) та у сфері управління та комп'ютерно-інтегрованих технологій: В. А. Попель «Інформаційна технологія підвищення живучості об'єктів критичної енергетичної інфраструктури за фактором управління системою інформа-

ційної безпеки» (2024) тощо. В цих та інших працях окреслені організаційно-правові аспекти забезпечення інформаційної безпеки в Україні, висвітлено основні загрози та практики зарубіжного законодавства. а також запропоновані методики оцінки ризиків, які можуть бути застосовані при розробці нормативно-правових актів. Питанню правового забезпечення та перспективам розвитку державної політики у сфері інформаційної безпеки увага була приділена опосередковано.

Викладення основного матеріалу. Правове забезпечення державної політики у сфері інформаційної безпеки ґрунтується, передусім, на проголошених позиціях Основного закону України та Міжнародних документах, ратифікованих нашою державою. Відповідно, Основний Закон України – джерело правових гарантій на безпеку людини від загроз життю, фізичному та психічному здоров'ю, честі, гідності, недоторканості (ст. 3 Конституції України). Так, відповідно до ст. 17 Конституції України наголошено на обов'язку державних органів щодо забезпечення інформаційної безпеки що є однією з найважливіших функцій держави та одночасно справою всього Українського народу. Приналежно, забезпечення інформаційної безпеки конкретизується в Основному законі: 1) у ст. 31 – згідно з положеннями якої, людині гарантується таємниця листування, телефонних розмов, телеграфної та іншої кореспонденції. Порушувати такі правила державні органи можуть лише у виняткових випадках та лише на підставі судових рішень з метою запобігти злочинові чи з'ясувати істину під час розслідування кримінальної справи (якщо іншими способами одержати інформацію неможливо); 2) у ст. 32 – відповідно до якої не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди (крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини). При цьому людині держава гарантує право на захист своїх порушених прав у суді шляхом вимагати спростовувати недостовірну інформації про себе і членів своєї сім'ї та права вимагати вилучення будь-якої інформації, а також право на відшкодування матеріальної і моральної шкоди, завданої збиранням, зберіганням, використанням та поширенням такої недостовірної інформації; 3) у ст. 34 – зазначено право людини на вільне володіння інформацією (збирати, зберігати, використовувати і поширювати інформацію усно, письмово або в інший спосіб); 4) у ст. 50 – наголошено на гарантованому державою права вільного доступу до інформації про стан довкілля, про якість харчових продуктів і предметів побуту, а також право на її поширення (при цьому така інформація не може бути засекречена) [1]. Таким чином, правового забезпечення державної політики базуючись на підґрунті Основного закону у сфері інформаційної безпеки виокремлює дві стратегічні вектори – забезпечення та гарантування права людини на володіння інформацією, та право на захист інформації.

По-друге, це орієнтованість на чинні в Україні міжнародні договори, згода на обов'язковість яких надана Верховною Радою України (ст. 9 Конституції України). Вбачається необхідним тут зазначити Конвенцію «Про захист прав людини і основоположних свобод» (Європейська конвенція з прав людини 1950 року), яка містить важливі положення щодо захисту приватності та права на особисте життя, що включає питання конфіденційності інформації [2]. Не зважаючи на те, що Дана Конвенція не є «спеціальною» у сфері інформаційної безпеки, втім вона слугує основою для розвитку національного законодавства, міжнародного співробітництва та політики у сфері інформаційної безпеки.

Націленість на забезпечення державними органами загальних принципів захисту інформації, встановлюють також стандарти, які сприяють координації дій у відповідь на загрози в кіберпросторі. Приналежно, Конвенція Ради Європи «Про кіберзлочинність» встановлює стандарти для криміналізації різних видів кіберзлочинів, таких як комп'ютерне шахрайство, злочини проти конфіденційності даних, кібертероризм тощо [3]. Державна політика орієнтована на сьогодні зорієнтована на досягнення мети зазначеної у ратифікованої урядом Конвенції ООН «Про захист персональних даних у рамках автоматизованої обробки даних» (Конвенція 108 1981 року) [4], яка є

першою міжнародною угодою, що встановлює принципи захисту персональних даних та інформаційної безпеки під час обробки даних у автоматизованих системах. Варто зазначити у цьому руслі Конвенцію ООН «Про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицину прав людини та біомедичних досліджень» (Ов'єдська конвенція 1997 року) [5]. Хоча акцентування цієї Конвенції робиться на питаннях біомедичних досліджень та прав людини, вона містить положення важливі положення щодо захисту інформації про здоров'я та забезпечення конфіденційності персональних даних у сфері охорони здоров'я.

Основні підходи державної інформаційної політики отримали новий поштовх з огляду на положення ратифікованої Конвенції Організації Об'єднаних Націй «Проти транснаціональної організованої злочинності» (Палермська конвенція 2000 року) [6], яка є не тільки одним із найважливіших міжнародних інструментів у боротьбі з організованою злочинністю, а й спрямована на захист інформації в контексті злочинної діяльності. Так, відповідно до ст. 10 Конвенції у сенсі відповідальності юридичних осіб за злочини, передбачені Конвенцією включені заходи, пов'язані із забезпеченням безпеки та захисту інформації в діяльності юридичних осіб. Стаття 12 Конвенції зобов'язує держав-учасниць забезпечити можливість конфіскації доходів від злочинної діяльності, зокрема тих, що отримані внаслідок кіберзлочинності, де захист інформації є ключовим елементом. Згідно зі ст. 27 Конвенції передбачено обмін інформацією між державами для забезпечення безпеки інформаційних систем і баз даних, які використовуються для боротьби з організованою злочинністю, тощо. Тобто, Конвенція «Проти транснаціональної організованої злочинності» надає загальні рамки для боротьби з транснаціональними злочинами, включаючи ті, що мають інформаційний характер: кіберзлочини, шахрайство з використанням інформаційних технологій, відмивання грошей через електронні системи тощо. Варто зазначити, що хоча дана Конвенція не містить прямої згадки про захист інформації, вона створює правову основу для притягнення до відповідальності за злочини, що можуть бути пов'язані з незаконним використанням або маніпуляцією інформацією, і, таким чином, створювати загрози інформаційній безпеці. Таким чином, Конвенція ООН «Проти транснаціональної організованої злочинності» опосередковано підтримує захист інформації через положення, які спрямовані на боротьбу з різними видами організованих злочинів, включаючи ті, що пов'язані з використанням та маніпуляцією інформацією, що є важливим орієнтиром для державної політики, адже злочинність у цифровому світі дедалі набуває інформаційного характеру.

В цьому руслі можливо зазначити Директиву Європейського Парламенту і Ради (ЄС) «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» (2016) яка встановлює вимоги щодо забезпечення високого рівня кібербезпеки [7].

Перспективним напрямком розвитку державної політики у сфері інформаційної безпеки може слугувати проектна Конвенція ООН з протидії злочинності в сфері інформаційних технологій, робота над якою ще триває. Зазначений документ розробляється під егідою ООН та спрямований на створення новітніх стандартів щодо боротьби з кіберзлочинністю та забезпечення інформаційної безпеки на міжнародному рівні. Метою документу є забезпечення глобального співробітництва в розслідуванні та попередженні злочинів, пов'язаних з інформаційними технологіями [8]. Так само проектним є Рамкова конвенція ООН «Про міжнародну безпеку інформації», робота над якою поки триває, однак ця нова ініціатива спрямована на розробку глобальної рамки для регулювання та забезпечення інформаційної безпеки у різних секторах, включаючи державний і приватний сектори. Відповідним документом планується встановити загальні принципи та стандарти для забезпечення безпеки інформації на міжнародному рівні, що неодмінно має позначитися у відповідному секторі державній політиці України [9].

Положення Конституції України та ратифікованих міжнародних документів відображені у внутрішньому національному законодавстві: Кримінальному кодексі

України (статті, що стосуються відповідальності за кіберзлочини), Кодексі України про адміністративні правопорушення (регулює адміністративну відповідальність за порушення у сфері кібербезпеки); Законах України: «Про основні засади забезпечення кібербезпеки України» (визначає правові та організаційні основи забезпечення кібербезпеки в Україні), «Про національну безпеку України» (включає положення щодо стратегії кібербезпеки), «Про захист персональних даних» (регулює обробку та захист персональних даних, що є важливим аспектом кібербезпеки), «Про електронні довірчі послуги» (встановлює правові основи для надання електронних довірчих послуг, включаючи електронні підписи та сертифікати), «Про інформацію» (визначає правові основи інформаційної діяльності, включаючи захист інформації), «Про телекомунікації» (регулює діяльність у сфері телекомунікацій, що включає аспекти кібербезпеки) тощо; Постановах Кабінету Міністрів України: «Про затвердження Положення про Державну службу спеціального зв'язку та захисту інформації України» (визначає функції та повноваження Держспецзв'язку у сфері кібербезпеки), «Про затвердження Положення про кіберзахист об'єктів критичної інфраструктури» 2016 року (визначає заходи кіберзахисту для об'єктів критичної інфраструктури), «Про затвердження Положення про Державний центр кіберзахисту» 2020 року (регулює діяльність Державного центру кіберзахисту), «Про затвердження Положення про Національний координаційний центр кібербезпеки» 2021 року (визначає функції та повноваження Національного координаційного центру кібербезпеки), «Про затвердження Порядку реагування на кіберінциденти та кіберзагрози» 2021 року (встановлює порядок реагування на кіберінциденти та кіберзагрози) тощо.

З огляду на вище зазначене, можна стверджувати, що перспективи розвитку державної політики України у сфері інформаційної безпеки мають бути комплексними, враховуючи сучасні виклики в цифровому просторі. Актуальні питання розвитку державної політики України у сфері інформаційної безпеки виявлені та закріплені у Державній стратегії кібербезпеки України, яка була затверджена Указом Президента України №447/2021 від 26 серпня 2021 року. Ця стратегія визначає пріоритети національних інтересів у сфері кібербезпеки, наявні та потенційні кіберзагрози, а також цілі та завдання для забезпечення кібербезпеки України з метою створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Основні положення стратегії включають: посилення національної системи кібербезпеки для протидії сучасним кіберзагрозам; інтеграція міжнародного досвіду та співпраця з ЄС і НАТО у сфері кібербезпеки; розробка та впровадження плану реалізації стратегії, який був затверджений Указом Президента України №37/20222 [10].

Варто зазначити, що перспективним підґрунтям для формування державної політики слугує Форум «Інтернет плюс» (Global Forum on Cyber Expertise – GFCE) заснований у 2015 році, який представлений в якості глобальної ініціативи для обміну знаннями з метою зміцнення спроможностей у сфері кібербезпеки шляхом співпраці між урядами, міжнародними організаціями та приватним сектором [11]. В цьому руслі працює «Центр глобальної співпраці з кібербезпеки» (Global Cybersecurity Cooperation Center – GC3) [12] заснований у 2020 році, метою якого є спрямування на об'єднання зусиль різних держав і організацій для покращення міжнародного співробітництва в питаннях кібербезпеки, обміну інформацією та розробки спільних стандартів.

Отже, ключовими напрямками розвитку державної політики у сфері інформаційної безпеки є: по-перше, робота, направлена на вдосконалення правового регулювання, що передбачає розробку нових законів та оновлення діючих нормативно-правових актів з урахуванням новітніх тенденцій та швидкого розвитку технологій. Особливо актуальним тут постає питання про захист персональних даних та регулювання діяльності в кіберпросторі та боротьбу з кіберзлочинністю.

По-друге, це процеси, направлені на посилення інтеграції міжнародних стандартів у внутрішнє законодавство України, що дозволить гармонізувати національну політику з міжнародною практикою.

По-третє, це розробка та вдосконалення існуючих та створення нових стандартів щодо кібербезпеки, з огляду на постійні тенденції щодо вдосконалення злочинів у сфері кіберзагроз. А також постійного моніторингу кіберзагроз та розвиток публічно-приватного партнерства для спільного вирішення проблем кібербезпеки.

По-четверте, це політика, направлена на належну підготовку кваліфікованих кадрів у сфері кібербезпеки, що включатиме оновлення та актуалізацію освітніх програм та постійного підвищення кваліфікації практикуючих спеціалістів.

По-п'яте, це політика направлена на посилення захисту критичних об'єкт інфраструктури, які є найбільш вразливими до кіберзагроз; створення національних координаційних центрів, метою яких має бути допомога у координації зусиль для забезпечення безпеки критичних систем.

По-шосте, це політика щодо посилення міжнародного співробітництва у боротьбі з кіберзлочинністю та участь у глобальних ініціативах і форумах з метою впровадження спільних підходів до інформаційної безпеки.

Таким чином, розвиток державної політики у сфері інформаційної безпеки потребує комплексного підходу, який враховуватиме сучасні виклики і можливості, міжнародну співпрацю, впровадження інновацій та розбудову державних освітніх програм, що дозволить зменшити ризики пов'язані з кіберзагрозами.

Висновки. Підсумовуючи вище зазначене, можна дійти наступних висновків: 1) аналіз державної політики у сфері інформаційної безпеки є критично важливим для забезпечення ефективного захисту даних і систем від кіберзагроз та інших ризиків; 2) державна політика визначає загальні напрямки, стратегії та норми, що дозволить оцінити її ефективність, виявити слабкі місця і розробити рекомендації для покращення захисту інформації, особливо в контексті кіберзлочинності; 3) перспективними напрямками державної політики є: оцінка ефективності реалізації стратегій та заходів щодо інформаційної безпеки; удосконалення чинного законодавства; розробка законодавчих актів з метою інтеграції міжнародних стандартів у внутрішнє законодавство України; виявлення проблем у реалізації державної політики (у тому числі, оцінка впливу зовнішніх і внутрішніх факторів які впливають на ефективність політики).

Література:

1.Конституція України. URL : https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (дата звернення: 01.09.2024)

2.Про захист прав людини і основоположних свобод: Конвенція ООН. Ратифікація 17.07.1997. URL : https://zakon.rada.gov.ua/laws/show/995_004#Text (дата звернення: 01.09.2024)

3.Про кіберзлочинність: Конвенція ООН. Ратифікація 07.09.2005. URL : https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 01.09.2024)

4.Конвенція ООН про захист персональних даних у рамках автоматизованої обробки даних. URL: https://rm.coe.int/1680078b37 (дата звернення: 01.09.2024)

5.Про захист прав і гідності людини щодо застосування біології та медицини: Конвенція про права людини та біомедицин. URL: https://zakon.rada.gov.ua/laws/show/994_334#Text (дата звернення: 01.09.2024)

6.Проти транснаціональної організованої злочинності. Конвенція ООН (Палермська конвенція 2000 року). URL: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf (дата звернення: 01.09.2024)

7.Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу: директива Європейського Парламенту і Ради (ЄС) 2016/1148 від 6 липня 2016 року. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата звернення: 01.09.2024)

8.United Nations Office on Drugs and Crime.(2021). Elaboration of a convention on countering the use of information and communications technologies for criminal purposes. URL: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Cybercrime_input_Switzerland_102021.pdf (дата звернення: 01.09.2024)

9.Про міжнародну безпеку інформації: Конвенція ООН. URL : https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies__(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_United__Kindom.pdf (дата звернення: 01.09.2024)

10. Державна стратегії кібербезпеки України: Указ Президента України №447/2021 від 26 серпня 2021 року. URL: https://www.president.gov.ua/documents/4472021-40013 (дата звернення: 01.09.2024)

11. Global Forum on Cyber Expertise – GFCE.2015. URL : https://thegfce.org/ (дата звернення: 01.09.2024)

12. Global Cybersecurity Cooperation Center.2020. URL : https://gc3.digital/ (дата звернення: 01.09.2024)

References:

1. The Constitution of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text (Accessed September 01,2024).

2. UN Convention for the Protection of Human Rights and Fundamental Freedoms.(1997). Retrieved from: https://zakon.rada.gov.ua/laws/show/995_004#Text (Accessed September 01,2024).

3. United Nations Convention on cybercrime.(2005). Retrieved from: https://zakon.rada.gov.ua/laws/show/994_575#Text (Accessed September 01,2024).

4. The UN Convention for the Protection of Personal Data with regard to Automatic Processing of Personal Information. Retrieved from: https://rm.coe.int/1680078b37 (Accessed September 01,2024).

5. Convention on Human Rights and Biomedicine on the Protection of Human Rights and Dignity of the Human Being with regard to the Application of Biology and Medicine Retrieved from: https://zakon.rada.gov.ua/laws/show/994_334#Text (Accessed September 01,2024).

6. The UN Convention against Transnational Organised Crime.(2000). Retrieved from: https://www.unodc.org/documents/treaties/UNTOC/Publications/TOC%20Convention/TOCebook-e.pdf (Accessed September 01,2024).

7. Directive of the European Parliament and of the Council (EU) № 2016/1148.(2016). Retrieved from: : https://eur-lex.europa.eu/eli/dir/2016/1148/oj (Accessed September 01,2024).

8. United Nations Office on Drugs and Crime.(2021). Elaboration of a convention on countering the use of information and communications technologies for criminal purposes. Retrieved from: https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Cybercrime_input_Switzerland_102021.pdf (Accessed 01.09.2024)

9. UN Convention on International Information Security. Retrieved from: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies__(2021)/ENG_Concept_of_UN_Convention__on_International_Information_Security_Proposal_of_the_United__Kindom.pdf (Accessed September 01,2024).

10. State Strategy of Cybersecurity of Ukraine: Decree of the President of Ukraine No. 447/2021.(2021). Retrieved from: https://www.president.gov.ua/documents/4472021-40013(Accessed September 01,2024).

11. Global Forum on Cyber Expertise – GFCE.(2015). Retrieved from: https://thegfce.org/ (Accessed September 01,2024).

12. Global Cybersecurity Cooperation Center.(2020). Retrieved from: https://gc3.digital/ (Accessed September 01,2024).

Стаття надійшла до друку 07 вересня 2024 року