ПРАВОВЕ РЕГУЛЮВАННЯ КІБЕРБЕЗПЕКИ ЛЮДИНИ НА МІЖНАРОДНОМУ РІВНІ: ПОРІВНЯЛЬНО-ПРАВОВЕ ДОСЛІДЖЕННЯ

ЛУЦЕНКО Юрій Васильович - доктор юридичних наук, доцент, Рада національної безпеки і оборони України
ТАРАСЮК Анатолій Васильович - доктор юридичних наук, доцент
ДЕНИСЕНКО Микола Миколайович - кандидат юридичних наук, Національна академія Служби безпеки України

УДК 336.7:340.5:347.7
DOI 10.32782/NP.2022.3.6

У статті здійснено порівняльно-правове дослідження правових аспектів регулювання кібербезпеки людини на міжнародному рівні в контексті сучасних викликів та загроз. Досліджено питання, які стосуються правового регулювання кібербезпеки людини.

Акцентовано увагу на необхідності розбудови національної системи кібернетичної безпеки, яка буде спроможною ефективно протидіяти викликам та загрозам національній безпеці в кібернетичній сфері. Наголошено, що досить часто на кібернетичні атаки й злочини наражаються державні, фінансові установи, підприємства енергозабезпечення і транспорту та інших об'єктів критичної інфраструктури.

У дослідженні акцентовано увагу на тому, що Україна тісно співпрацює з іноземними державами, їхніми збройними силами, правоохоронними органами і спецслужбами, а також із багатьма міжнародними організаціями. У зв'язку з цим, одним із пріоритетних напрямів міжнародного співробітництва у цій царині вбачається активна діяльність нашої держави у структурах ООН, стратегічне партнерство з Організацією Північноатлантичного договору та Європейським Союзом.

Ключові слова: інформаційна зброя; інформаційні війни; кібертероризм; міжнародна злочинність; інформаційно-психологічний вплив; кібернетичний простір; міжнародна кібербезпека; недоторканність приватного життя

Постановка проблеми

Аналіз міжнародно-правових нормативно-правових актів, національних законодавств, проблеми правового забезпечення кібернетичної безпеки особи ще не отримали достатньої уваги. Нагальна потреба розроблення комплексних заходів для налагодження й удосконалення системи міжнародної кібернетичної безпеки, а також відповідного стратегічного партнерства зумовлена слабкою захищеністю людини в умовах мілітаризації глобального кібернетичного простору, розгортанням потужних інформаційних війн, значним поширенням комп'ютерної злочинності (особливо у фінансовій сфері) та кібертероризму.

З огляду на особливості сучасного стану інформаційних прав і свобод людини вбачається доцільним розроблення й ухвалення відповідної міжнародної угоди у сфері інформації прав, яка стане підґрунтям запровадження в національне законодавство міжнародних зобов'язань стосовно гарантування інформаційних прав і свобод, забезпечення кібернетичної безпеки особи, регулювання низки фундаментальних питань щодо захисту прав суб'єктів персональних даних. Крім того, важливим убачається впровадження ефективних механізмів забезпечення кібернетичної безпеки особи, створення цією метою відповідних національних і міжнародних інституцій.

Аналіз останніх досліджень і публікацій

Дослідженню питань, які стосуються правового регулювання кібербезпеки людини, у тому числі, і на міжнародному рівні у різні часи було присвячено роботи таких науковців, як: О. А. Баранов [1 5], М. Д. Василенко [2 6], О. Д. Довгань [3 9], М. В. Карчевський [4 11], О. В. Таволжанський [5 16; 6 17], О. М. Фролов [7 18] та ін.

Метою статті є порівняльно-правове дослідження правових аспектів регулювання кібербезпеки людини на міжнародному рівні в контексті сучасних викликів та загроз.

Виклад основних положень дослідження

Стабільність, стійкість міжнародного співробітництва у розв'язанні проблем кібернетичної безпеки завжди відігравала важливу роль і в розвитку національного інформаційного законодавства.

Необхідно звернути увагу, що міжнародно-правовими нормами питання безпосереднього гарантування безпеки особи в інформаційній сфері практично не регламентуються, оскільки її правосуб'єктність у міжнародному праві обмежена.

Водночас доцільність розгляду цієї проблематики зумовлена тим, що з огляду на глобалізацію інформаційного (кібернетичного) простору, стабільність наявних у ньому відносин для стійкого існування та розвитку особистості в інформаційному суспільстві, питання міжнародної інформаційної безпеки становлять беззаперечний інтерес. Крім того, інформаційно-безпекові міжнародно-правові норми містять і регламентацію міжнародних аспектів забезпечення інформаційної безпеки людини.

Особливу небезпеку у сфері міжнародної кібербезпеки становлять загрози інформаційного впливу, зокрема таких його крайніх форм, здатних спричинити регіональні та світові конфлікти, руйнівний потенціал яких можна порівняти із дією «традиційних» засобів масового ураження – застосування інформаційної зброї, кібертероризм, інформаційні війни. Яскравим прикладом цього є те, що анексія Російською Федерацією українського Криму, її агресія спочатку на Донбасі, а згодом і на території всієї України готувалася, супроводжувалася й триває досі за допомогою широкомасштабної інформаційної війни проти нашої держави, руйнівним інформаційно-психологічним впливом на значну частину її населення. Відтак, на початку третього тисячоліття кібернетичний простір (поряд із землею, водою, повітрям і космосом) увійшов до сфер ведення воєнних дій, а головними об'єктами в інформаційних війнах є психологія ворожого війська й населення та інформаційна інфраструктура.

Варто зазначити, що світова спільнота ще не виробила єдиного підходу до проблематики міжнародної кібербезпеки, хоча відповідних нормативно-правових актів на сьогодні існує чимало. До них належать насамперед низка основоположних міжнародних документів щодо прав людини: Загальна декларація прав людини, міжнародні пакти про економічні, соціальні й культурні права, про громадянські й політичні права, Європейська конвенція про захист прав людини й основних свобод та інші. Саме ці документи закріпили основні загальносвітові стандарти прав і свобод людини як одну зі складових права особи на кібербезпеку.

Отже, розглянемо детальніше інститут права на недоторканність приватного життя.

Це поняття означає надання людині можливості контролювати поширення інформації про себе, свою родину, житло тощо, перешкоджати зазіханням на її репутацію, честь і гідність, на несанкціоноване оприлюднення (розголошення) своїх персональних даних чи інших відомостей особистого характеру.

У міжнародно-правовому контексті недоторканність приватного життя є категорією «особистих прав, які надають змогу кожній людині стати на заваді розголошенню відомостей особистісного характеру про її життя, що оберігається від втручання держави і сторонніх осіб». Про можливі окремі обмеження цього права в рішеннях щодо застосування положень Європейської конвенції про захист прав людини й основних свобод зазначав Європейський суд з прав людини (ЄСПЛ): «… *приховане спостереження за поштою і зв'язком у разі надзвичайних умов є необхідним у демократичному суспільстві, але за наявності належних*

і ефективних гарантій». Приміром, подібне втручання у приватне життя не суперечить Конвенції, коли воно має на меті запобігання конкретним, найнебезпечнішим злочинам або їхнє припинення (а не якихось дрібних правопорушень), або якщо воно застосовується до суворо обмеженого кола осіб тощо.

Утім на практиці декларування таких правил, на жаль, не може цілковито убезпечити від різноманітних вторгнень у приватну сферу людини. Наприклад, всесвітню увагу привернув Е. Сноуден, американський програміст, який за контрактом працював на Агентство національної безпеки (АНБ) США. Він оприлюднив значний масив секретних матеріалів, із яких випливало, що американські спецслужби відстежували величезні потоки інформації в мережевому просторі багатьох країн, у тому числі Європейського Союзу, встановивши необмежений доступ до серверів глобальних комунікаційних компаній. Так, АНБ і ФБР США перехоплювали трафіки таких Інтернет-гігантів, як Microsoft, Apple, Facebook, Google між їхніми серверами й пересічними користувачами. При цьому без жодних судових дозволів аналітики спецслужб на свій розсуд могли обирати об'єкти для електронного стеження й таємного прослуховування. Деякі американські добровільно «зливали» спецслужбам дані про своїх користувачів, інших примушували до цього.

Як бачимо, навіть найбільш технологічно розвинені країни виявилися не спроможними відвернути подібне втручання. Тому назріла потреба формування єдиного міжнародно-правового режиму забезпечення інформаційної (кібернетичної) безпеки.

Як і в переважній більшості міжнародно-правових питань, особливу роль у питаннях забезпечення права особи на кібербезпеку відіграє ООН – найбільш представницька міжнародна інституція. Зокрема, вже на другий рік свого існування організації, у 1946 році, у резолюції Генеральної Асамблеї ООН містилося важливе, на нашу думку, положення стосовно права особи на кібербезпеку, а саме: «*…свобода інформації є основним правом людини і критеріями всіх видів свободи, захисту котрих Об'єднані Нації себе присвятили; …свобода інформації, безперечно, вимагає від тих, хто користується її привілеями, бажання й уміння не зловживати ними. Основним принципом її є моральний обов'язок прагнути до виявлення об'єктивних чинників і до поширення інформації без злісних намірів…*» [8 13]. Питань кібербезпеки особи торкаються й наступні документи ООН.

Що стосується захисту персональних даних, то на міжнародному рівні це питання було регламентоване в 1981 році Конвенцією Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних (далі – Конвенція), яка містила низку відповідних вимог до держав-учасниць. Це, зокрема, приписи про те, що:

– громадянин має право знати про існування автоматизованих картотек;

– отримувати інформацію про наявність чи відсутність у цих картотеках даних на нього;

– отримувати особисто наявні в картотеках дані;

– у разі незаконності чи невідповідності цих даних вимогам Конвенції вимагати їх виправлення чи видалення, а в разі відмови в цьому – звертатися до вищої інстанції.

Крім того, у документі закріплювалися правила транскордонної передачі персональних даних, гарантії прав щодо обробленння даних стосовно расового походження людини, її політичних переконань, здоров'я, сексуальної орієнтації та інших особливих категорій даних [9 12].

У ст. 6 Декларації ООН про права й обов'язки окремих осіб, груп і органів суспільства заохочувати й захищати загальновизнані права людини й основні свободи закріплено, зокрема, й основоположні права, що стосуються забезпечення безпеки особи в інформаційній сфері:

– знати, розшукувати, здобувати, отримувати й розпоряджатися інформацією про всі права людини й основні свободи, у тому числі доступ до інформації про те, у який спосіб забезпечуються ці права і свободи у внутрішньому законодавстві, у судовій чи адміністративній системах;

– вільно оприлюднювати, передавати чи поширювати серед інших думки, інформацію і знання про всі права людини й основні свободи [10 14].

Що стосується проблем кібербезпеки людини, то початком їхнього всебічного об-

говорення й пошуку шляхів розв'язання на міжнародному рівні можна вважати міжнародну конференцію із глобального інформаційного суспільства (1996, ЮАР), де з-поміж інших розглядалися питання доступу особи до інформації, подолання нерівності в інформаційній сфері, інформаційно-психологічних впливів на людину.

Ухвалена 61-ю сесією Генасамблеї ООН (2005) резолюція 60/45 «Досягнення у сфері інформатизації й телекомунікації в контексті міжнародної безпеки» стала наступним важливим кроком у цьому напрямку, поклала початок формуванню принципово нового загальносвітового міжнародно-правового режиму, спрямованого на регулювання відносин у сфері інформації, інформаційно-телекомунікаційних технологій і методів їхнього застосування й використання [7].

У липні 2000 року в Японії провідні світові держави Великої вісімки підписали так звану Окінавську хартію глобального інформаційного суспільства (надалі – Хартія), де одним із головних напрямів розвитку цього суспільства визначено захист приватного життя під час оброблення особистих даних із одночасним забезпеченням вільного обігу інформації. У Хартії також зазначено, що інформаційно-телекомунікаційні технології є важливим чинником формування сучасного суспільства, а сутність соціальної трансформації, котра стимулюється інформаційно-комунікаційними технологіями, полягає в її здатності сприяти людині й суспільству в застосуванні ідей і знань. При цьому головним завданням своїх учасників Хартія вбачає забезпечення кожному можливості користуватися перевагами глобального інформаційного суспільства, стійкість якого базується на вільному обміну інформацією і знаннями та іншими демократичними цінностями, які стимулюють розвиток людини.

Активна робота під егідою ООН щодо формування основ забезпечення права особи на кібербезпеку триває. Так, у 2001 році в Будапешті держави-учасники Ради Європи підписали Конвенцію про кіберзлочинність (CETS № 185). Положення цієї так званої Будапештської конвенції спрямовані на захист особистих даних, законних інтересів людей у використанні й розвитку інформаційних технологій, боротьбу зі злочинами в кібернетичному просторі, у ній уперше наведена класифікація таких злочинів. У Конвенції – єдиному в теперішній час обов'язковому регіональному міжнародному документі з питань кібербезпеки – зазначено, що вона є першою міжнародною угодою щодо злочинів, вчинених через Інтернет та інші комп'ютерні мережі, стосується мережевої безпеки, порушень авторських прав, кібернетичного шахрайства, дитячої порнографії та ін. Конвенцією також передбачені пошук комп'ютерних мереж, перехоплення даних та інші повноваження й процедури.

Будапештська конвенція встановлює спільну кримінальну політику щодо захисту від кіберзлочинності шляхом прийняття відповідного внутрішнього законодавства та сприяння міжнародному співробітництву. Вона також доповнена Протоколом про «акти ксенофобського та расистського характеру, вчинених через комп'ютерні системи», й Директивною запискою [11].

Наша держава ратифікувала Будапештську конвенцію у 2005 році, проте на сьогодні не всі її положення імплементовані у вітчизняне законодавство, а повна їхня імплементація потребує істотних змін у Кримінальному процесуальному кодексі України.

До числа фундаментальних міжнародно-правових документів, який регулює, зокрема, питання кібернетичної безпеки, належить прийнятий у 1992 році основоположний документ спеціалізованої установи ООН – Статут Міжнародного союзу електрозв'язку (МСЕ) [12], до якого приєдналися всі держави-члени ООН, у тому числі й Україна. Статут регулює комплекс питань міжнародної співпраці у сфері використання телекомунікацій, розвитку засобів та підвищення ефективності відповідних послуг, визначає чинники, котрі заважають функціонуванню існуючих телекомунікаційних мереж тощо.

З метою оцінювання участі держав у галузі кібербезпеки на світовому рівні, підвищення поінформованості про важливість цих проблем та їх різні виміри МСЕ щороку оприлюднює так званий глобальний індекс кібербезпеки, котрий базується на таких критеріях глобального прогресу у цій сфері: законодавчі заходи; технічні заходи; органі-

заційні заходи; розбудова потенціалу; кооперація. Зазначимо, що обґрунтовані висновки МСЕ користуються широкою довірою.

Перша частина спільного законодавства ЄС про кібербезпеку – Директива щодо мережевої та інформаційної безпеки (Директива NIS) була ухвалена Європарламентом у 2016 році [13]. Правові заходи, передбачені Директивою, спрямовані на радикальне підвищення в Європейському Союзі загального рівня кібербезпеки (шляхом проведення відповідних операцій Групою реагування на інциденти, пов'язані з комп'ютерною безпекою, – CSIRT або CERT – та компетентним органом у галузі мереж та інформаційних систем), а також активізацію міжнародної співпраці й розвитку безпекової культури стосовно інформування відповідно до директивних вимог. Задля допомоги якнайшвидшій узгодженій реалізації державами-членами ЄС Директиви вона має додаток, де наведено найефективніший практичний досвід, пояснення та тлумачення, – так званий Інструментарій NIS (NIS Toolkit).

Ця Директива не є обов'язковою для України, яка поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги в правозастосовній практиці, а деякі були частково впроваджені у вітчизняне законодавство. Вбачається, що імплементацію Директиви NIS можна провести в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом. Це стосується і Директиви NIS. Крім того, деякі вимоги Директиви вводить до розроблюваних законопроєктів Державна служба спеціального зв'язку та захисту інформації України. Водночас її фахівці вважають, що при розробці загальних законів у сфері кібербезпеки відповідно до положень Директиви NIS буде вельми потрібною міжнародна допомога.

У виробленні єдиних підходів у сфері забезпечення кібернетичної безпеки як складової національної безпеки держав-учасниць значну роль відіграє Організація Північноатлантичного договору (НАТО). Цей напрям став одним із пріоритетних напрямів діяльності Альянсу з огляду на вразливість вказаної сфери, численність і різноманітність відповідних викликів і загроз [14, с. 42].

На Лісабонському саміті країн-членів НАТО (листопад 2010 року) за участі глав держав та урядів була прийнята нова Стратегічна концепція оборони та безпеки країн-членів блоку. У цьому документі загрози атак у кіберпросторі були фактично прирівняні до загроз із застосуванням війська, що, таким чином, передбачає можливість відсічі подібних масованих атак із застосуванням збройних сил держави, котра зазнала такого нападу. Позаяк останнім часом кібератаки стали чи не найсерйознішою загрозою безпеці, забезпечення кібернетичної безпеки країн-членів НАТО визначено другим за значущістю пріоритетом безпекової політики Альянсу. Водночас, співробітництво з партнерами щодо формування і вдосконалення кібербезпекової системи блоку визнано у Доктрині НАТО з кібербезпеки ключовим механізмом реалізації відповідних заходів [15].

Два роки потому вказані підходи були деталізовані Декларацією Чиказького саміту (травень 2012 року) Ради НАТО, у п. 49 якої йдеться про налаштованість Альянсу на співробітництво з іноземними партнерами для забезпечення власної безпеки й організації адекватних відповідей на кібернетичні виклики й загрози [16]. А остаточне закріплення кіберпростору як арени можливого ведення бойових дій (поряд із землею, морем, повітрям і космосом) відбулося у документах Варшавського саміту країн-членів НАТО (липень 2016 року) [17].

Дії НАТО у сфері забезпечення кібернетичної безпеки мають два пріоритетні напрями. Це, насамперед, захист власних комп'ютерних мереж, рішення стосовно якого було ухвалено на саміті НАТО в Ньюпорті (Вельс, вересень 2014 року). Слід зазначити, що це завдання вбачається досить непростим з огляду на дуже широку присутність суб'єктів блоку в мережах Інтернету. Адже для його виконання слід забезпечити захист усього комплексу інформаційно-комунікаційних систем, задіяних НАТО у своїх операціях і місіях, від численних загроз, що походять з кібернетичного простору.

Другий пріоритетний напрям – сприяння країнам-членам щодо вдосконалення сил і засобів захисту кібернетичного простору. Для цього застосовуються різні механізми,

як-от дворічний план визначення колективних цілей кіберзахисту (наприклад, розробка стратегії кіберзахисту), що їх мають підтримати всі учасники блоку. Шляхи й засоби реалізація цих узгоджених цілей систематично коригуються. Крім того, у межах численних освітніх установ НАТО (наприклад, школа в Обераммергау (ФРН), Кібернетична академія (Португалія), Талліннський кооперативний Центр передового досвіду з кіберзахисту (Естонія) та ін.) провадиться широкий спектр просвітницьких, навчальних і тренувальних заходів. Вказані заходи, спрямовані на посилення блоку за рахунок посилення кожного із членів, їхньої здатності до кіберзахисту, до узгодженого виконання завдання колективної оборони одне одного [18].

Нагальне завдання розбудови національної системи кібернетичної безпеки, спроможної ефективно протидіяти загрозам національній безпеці у кібернетичній сфері, стоїть сьогодні й перед нашою державою. Дедалі частіше на кібернетичні атаки й злочини наражаються державні, фінансові установи, підприємства енергозабезпечення і транспорту та інших об'єктів критичної інфраструктури. І, як засвідчив аналіз стану кібербезпеки в Україні, ця складова національної безпеки має високий ступінь уразливості від кіберзагроз і залишається вельми слабкою.

Відповідно до укладених міжнародних угод у сфері кібербезпеки Україна співпрацює з іноземними державами, їхніми збройними силами, правоохоронними органами і спецслужбами, а також із багатьма міжнародними організаціями. У цьому контексті одним із пріоритетних напрямів міжнародного співробітництва у цій сфері вбачається активна діяльність України у структурах ООН, стратегічне партнерство з Організацією Північноатлантичного договору та Європейським Союзом.

Висновки

Підсумовуючи викладене, необхідно зазначити, що на сьогодні відсутній єдиний, загальний для всієї світової спільноти міжнародно-правовий документ щодо кібернетичної безпеки. Однак керівні принципи щодо методів підвищення рівня безпеки в кібернетичному просторі містять Конвенція ООН проти транснаціональної організованої злочинності (2000 рік) та Статут Міжнародного союзу електрозв'язку (1992 рік), Доповідь ООН про кібербезпеку (2015 рік).

Єдиним регіональним обов'язковим у юридичному сенсі документом є Будапештська конвенція про кіберзлочинність (2001 рік). Наша держава є учасником цієї конвенції, а тому більшість її норм матеріального права імплементувала в національне законодавство. Водночас, на нашу думку, з метою ефективної реалізації всіх положень Будапештської конвенції слід удосконалити кібербезпековий понятійно-термінологічний апарат Кримінального процесуального кодексу України.

Директива NIS не є обов'язковою для України, яка поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у правозастосовній практиці, а деякі були частково впроваджені у вітчизняне законодавство. Вбачається, що імплементацію Директиви NIS можна провести в межах механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом.

Література

1. Баранов О. А. «Інтернет речей» як правовий термін. *Юридична Україна*. № 5-6. 2016. С. 96–103.

2. Василенко М. Д. Підвищення стану кібербезпеки інформаційно-комунікаційних систем: якість в контексті удосконалення інформаційного законодавства. *Юридичний вісник*. 2018. № 3. С. 17–24.

3. Довгань О. Д., Тарасюк А. В. Протидія загрозам кібербезпеці держави на глобальному рівні. *Інформація і право*. 2020. № 2. С. 85–98.

4. Карчевський М. В. Основні проблеми кримінально-правового регулювання у сфері інформатизації. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка*, 2017. № 3. С. 67–78.

5. Таволжанський О. В. Основи державної кіберполітики України: формування та реалізація. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького. Серія : Право*. 2017. № 4. С. 158–164.

6. Таволжанський О. В. Особливості забезпечення кібербезпеки у сучасному світі:

огляд суб'єктів запобігання кіберзлочинності. *Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького: Серія Право*. 2018. Вип. 6(18). С. 154–163.

7. Фролов О. М. Роль ООН в системі міжнародної інформаційної безпеки. *International relations, part «Political sciences»*. № 18–19. 2018р. URL: http://journals.iir.kiev.ua/index.php/pol_n/article/view/3468/3140 (дата звернення 17.09.2022).

8. Резолюція Генеральної Асамблеї ООН від 14 грудня 1946 р. A/RES/59(I). URL: https://undocs.org/ru/A/RES/59(I) (дата звернення 10.09.2022).

9. Конвенція Ради Європи про захист фізичних осіб при автоматизованій обробці персональних даних від 28 січня 1981 р. URL: https://zakon.rada.gov.ua/laws/show/994_326#Text (дата звернення 15.08.2022).

10. Резолюція Генеральної Асамблеї ООН від 9 грудня 1998 р. A /53/ 144. URL: http://www.un.org/ru/documents/decl_conv/declarations/defender.shtml (дата звернення 17.09.2022).

11. Budapest Convention and related standards. Budapest, 23/11/2001. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention (дата звернення 17.08.2022).

12. Constitution of the international telecommunication union. Rev. Marrakesh, 2002). URL: https://www.itu.int/council/pd/constitution.html (дата звернення 17.09.2022).

13. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.EN (дата звернення 17.08.2022).

14. Войціховський А. В. Кібербезпека як напрям євроатлантичної інтеграції України. Право і безпека у контексті європейської та євроатлантичної інтеграції: Зб. сатей та тез наук. повідомл. за матеріалами дискус. панелі II Харків. міжнар. юрид. форуму, м. Харків, 28 верес. 2018 р. / редкол.: Ю. Г. Барабаш, Т. М. Анакіна. Харків: Право, 2018. С. 41–43.

SUMMARY

The article carries out a comparative legal study of the legal aspects of the regulation of human cyber security at the international level in the context of modern challenges and threats. Issues related to the legal regulation of human cyber security have been studied.

Attention is focused on the need to build a national cyber security system that will be able to effectively counter challenges and threats to national security in the cyber sphere. It was emphasized that state, financial institutions, energy supply and transport enterprises and other critical infrastructure objects are quite often exposed to cyber attacks and crimes.

The study focuses on the fact that Ukraine closely cooperates with foreign countries, their armed forces, law enforcement agencies and special services, as well as with many international organizations. In this regard, one of the priority areas of international cooperation in this area is the active activity of our state in the UN structures, strategic partnership with the North Atlantic Treaty Organization and the European Union.

Keywords: information weapon; information wars; cyber terrorism; international crime; informational and psychological influence; cyberspace; international cyber security; inviolability of private life

15. Стратегічна концепція оборони та безпеки членів НАТО від 19 листопада 2010 р. URL: https://www.nato.int/cps/uk/natohq/official_texts_68580.htm (дата звернення 17.08.2022).

16. Декларації Чиказького саміту від 20 травня 2012 р. НАТО. URL: https://www.nato.int/cps/uk/natohq/official_texts_87593.htm?selectedLocale=uk (дата звернення 19.09.2022).

17. Cyber defence / Офіційний сайт Організації Північноатлантичного договору. Організація Північноатлантичного договору. URL: http://www.nato. int/cps/en/natohq/topics_78170.htm (дата звернення 17.09.2022).

18. Зміна підходів до кіберзахисту // Офіційний сайт Організації Північноатлантичного договору / НАТО РЕВЮ. 2016 р. URL: https://www.nato.int/docu/review/2016/Also-in-2016/cyber-defense-nato-security-role/UK/index.htm (дата звернення 29.08.2022).