УДК 340+35.078.3
DOI https://doi.org/10.32837/yuv.v0i3.1948

А. Тарасюк,
головний науковий співробітник наукової лабораторії
забезпечення інформаційної та кібернетичної безпеки
Науково-дослідного інституту інформатики і права
Національної академії правових наук України

ЗАБЕЗПЕЧЕННЯ КІБЕРНЕТИЧНОЇ БЕЗПЕКИ ЛЮДИНИ: МІЖНАРОДНО-ПРАВОВИЙ АСПЕКТ

Постановка проблеми. Аналіз міжнародно-правових документів, дво- й багатосторонніх міжнародних угод, національних законодавств чітко засвідчив, що проблеми правового забезпечення кібернетичної безпеки особи ще не отримали адекватної 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.

Становлення й еволюція світового інформаційного суспільства, динаміка та характер розвитку глобального кіберпростору зумовили виникнення новітніх викликів і загроз, спрямованих, насамперед, на людину як найуразливішу ланку інформаційних відносин. Отже, актуалізувалася проблема формування й удосконалення системи міжнародної кібернетичної безпеки, під якою розуміємо такий стан глобального кібернетичного простору, який гарантує дотримання законних прав людини, а також суспільства та держави під час його використання.

Нагальність теоретико-правового дослідження міжнародно-правових засад кібербезпеки людини в контексті правового забезпечення її інформаційної безпеки та розвитку засадничих положень цього складника інформаційного права не викликає сумнівів.

Стан дослідження. В основу написання даної статті покладено аналіз чинного інформаційного законодавства, законопроєкти, які стосуються предмету дослідження, а також творчий доробок відомих учених, зокрема В. Білоуса, В. Брижка, О. Довганя, І. Дороніна, В. Рубана, Т. Ткачука, В. Фурашева, В. Цимбалюка та ін.

Мета статті – дослідити концептуальні засади правового забезпечення кібернетичної безпеки людини на міжнародному рівні з урахуванням сучасних загроз та перспектив розвитку.

Виклад основного матеріалу. Стабільність, стійкість міжнародного співробітництва у розв'язанні проблем кібернетичної безпеки відіграє важливу роль і в розвитку національного інформаційного законодавства. Вже сьогодні ми маємо всі симптоми та індикатори загроз, оскільки нам доведеться мати справу з новою біозброєю, зламаною ДНК та крадіжками генетичної та біометричної інформації. Ми живемо в експоненційні часи, коли інформація подвоюється кожні два роки, коли ми є технологічно незахищеними, оскільки всіма критичними системами та інфраструктурами керують комп'ютери.

Інформаційна сфера, у тому числі кібернетична безпека, стали визначальним чинником життєдіяльності сучасної світової спільноти та фактично кожної окремої особистості. Це зумовило, крім звичних розробок технічних аспектів проблематики, сплеск філософських, соціологічних, культурологічних, політологічних, економічних, психологічних та інших гуманітарних досліджень. Убачається, що в умовах транскордонного глобалізованого інформаційного суспільства наука інформаційного права мусить звернути особливу увагу на формування уявлень на специфіку та значення реалізації інтересів людини у цій сфері.

Як одну зі складових частин права особи на інформаційну безпеку розглянемо детальніше інститут права на недоторканність приватного життя. Це поняття означає надання людині можливості регулювати, контролювати поширення інформації про себе, свою родину, житло і т. п., 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 дають змогу кожній людині стати на заваді розголошенню відомостей особистісного характеру про її життя, що оберігається від утручання держави і сторонніх осіб». Про можливі окремі обмеження цього права в рішеннях щодо застосування положень Європейської конвенції про захист прав людини і основних свобод зазначав Європейський суд із 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 їх 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 Едвард Сноуден, американський програміст, котрий за контрактом працював на Агентство національної безпеки (АНБ) США. Він оприлюднив значний масив секретних матеріалів, з яких, зокрема, 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 вибирати 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, вочевидь, назріла потреба формування єдиного міжнародно-правового режиму забезпечення інформаційної (кібернетичної) безпеки.

Як і з переважної більшості міжнародно-правових питань, особливу роль у питаннях забезпечення права особи на інформаційну безпеку відіграє Організація Об'єднаних Націй – найбільш представницька міжнародна інституція. Зокрема, вже на другий рік свого існування організації, у 1946 р., у Резолюції Генеральної

Асамблеї ООН містилося важливе, на нашу думку, положення стосовно права особи на інформаційну безпеку, а саме: «*...свобода інформації є основним правом людини й являє собою критерії 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...*» [1]. Питань інформаційної безпеки особи торкаються й наступні документи ООН.

Що стосується захисту персональних даних, то на міжнародному рівні це питання було регламентоване в 1981 р. Конвенцією Ради Європи про захист фізичних осіб під час автоматизованої обробки персональних даних (далі – Конвенція), яка містила низку відповідних вимог до держав-учасниць. Це, зокрема, такі приписи: 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 у цьому – звертатися до вищестоящої інстанції. Крім того, у документі закріплювалися правила транскордонного передання персональних даних, гарантії прав щодо обробки даних стосовно расового походження людини, її політичних переконань, здоров'я, сексуальної орієнтації та інших особливих категорій даних [2].

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

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

– вільно оприлюднювати, передавати чи поширювати серед інших думки, інформацію і знання про всі права людини й основні свободи [3].

Що стосується безпосередньо проблем інформаційної безпеки особи, то початком їх усебічного обговорення й пошуку шляхів розв'язання на міжнародному рівні можна вважати міжнародну конференцію з глобального інформаційного суспільства (1996 р., 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 напрямі, поклала початок формуванню принципово нового загальносвітового міжнародно-правового режиму, спрямованого на регулювання відносин у сфері інформації, інформаційно-телекомунікаційних технологій і методів їх застосування й використання [4].

У липні 2000 р. в Японії провідні світові держави Великої вісімки підписали так звану Окінавську хартію глобального інформаційного суспільства (далі – Хартія), де одним із головних напрямів розвитку цього суспільства визначено захист приватного життя під час оброблення особистих даних з 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 у 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 обміні інформацією і знаннями та іншими демократичними цінностями, які стимулюють розвиток людини.

Активна робота під егідою ООН щодо формування основ забезпечення права особи на інформаційну безпеку триває. Так, у Будапешті держави – члени 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 сьогодні обов'язковому регіональному міжнародному документі з питань кібербезпеки – зазначено, що вона є першою міжнародною угодою щодо злочинів, учинених через Інтернет та інші комп'ютерні мережі, стосується мережевої безпеки, порушень авторських прав, кібернетичного шахрайства, дитячої порнографії та ін. Конвенцією також передбачено 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 [5].

Наша держава ратифікувала Будапештську конвенцію у 2005 р., проте сьогодні не всі її положення інтегровані у вітчизняне законодавство, а повна їх імплементація потребує істотних змін у Кримінальному процесуальному кодексі України.

До числа фундаментальних міжнародно-правових документів, котрий регулює, зокрема, і питання кібернетичної безпеки, належить прийнятий у 1992 р. засадничий документ спеціалізованої установи ООН – Статут Міжнародного союзу електрозв'язку (МСЕ) [6], 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.

Із 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 таких критеріях глобального прогресу у цій сфері: законодавчі заходи; технічні заходи; організаційні 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 р. [7]. 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. Для 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, котра поки що не входить до Євросоюзу, проте окремі її положення беруться до уваги у правозастосовній практиці, а деякі були частково впроваджені у вітчизняне законодавство. Убачається, що імплементацію Директиви NIS можна провести в рамках механізму, встановленого Угодою про асоціацію між Україною та Європейським Союзом. Нині у Верховній Раді України зареєстровано законопроєкт, спрямований на приведення законодавства України у відповідність до європейського. Це стосується й Директиви NIS (аналіз законопроєкту наводиться у розділі «Законодавчий рівень. Закон про кібербезпеку»). Окрім того, деякі вимоги Директиви вводить до розроблюваних законопроєктів Державна служба спеціального зв'язку та захисту інформації України. Водночас її фахівці вважають, що під час розроблення загальних законів у сфері кібербезпеки відповідно до положень Директиви NIS буде вельми потрібною міжнародна допомога.

Усебічне дослідження новітніх викликів і загроз кібербезпеці в умовах транскордонності у глобальному інформаційному суспільстві, а також небезпечних тенденцій у цій сфері дало змогу виокремити критерії їх можливої класифікації: джерело загрози (виклику), залежність від джерела загрози, розташування джерела загрози стосовно об'єкта, характер впливу. На цій основі з метою вдосконалення вітчизняної системи правового забезпечення кібернетичної безпеки людини запропоновано авторську класифікацію видів відповідних викликів і загроз. Зокрема, з огляду на значущість соціальних мереж, визначено джерела загроз в Інтернеті, а саме: сайти, котрі становлять небезпеку для особистості (мають на меті вплив на свідомість індивіда, рекламовані задля отримання зиску та ін.); спам, тотальне розсилання реклами та іншої інформації без бажання користувача тощо.

Окрім того, вивчення сучасних інформаційно-телекомунікаційних технологій дало змогу виявити специфічну групу загроз, пов'язаних із цифровою економікою, фінансово-банківською сферою (зокрема, з обігом електронних грошей, криптовалют – BitCoin, LitCoin, OneCoin та ін.), конфіденційністю персональних даних (загрози від найсучаснішої онлайн-реклами Real-TimeBidding (RTB), спеціальних файлів cookie та ін.).

Таким чином, потреба вдосконалення правової основи, а також розвитку узгоджених організаційних, інформаційно-аналітичних, економічних, науково-технічних та інших заходів щодо прогнозування, попередження, виявлення, протидії інформаційним загрозам і ліквідації наслідків у разі їх здійснення зумовлена кількістю та інтенсивністю викликів і загроз кібернетичній безпеці людини. Сьогодні найбільш нагальним убачається вирішення проблем, пов'язаних із розвитком новітніх технологій (на кшталт універсальної інноваційної платформи Blockchain), удосконалення систем ідентифікації й аутентифікації особи в кібернетичному просторі тощо.

Спираючись на проведене системне наукове дослідження, нами визначено напрями розроблення Концепції інформаційної безпеки особи, її можливі структуру та зміст, а також потребу долучення до її складу документів стратегічного планування України. Запропоноване структурно-змістовне наповнення вказаної Концепції містить головні принципи

формування, завдання, механізми реалізації й очікувані результати державної політики у сфері забезпечення інформаційної безпеки особи. Крім того, обґрунтовано мету гармонізації інформаційних відносин, підвищення відповідальності держави у цій сфері, створення умов для формування сприятливого кібернетичного середовища як стратегічну спрямованість Концепції.

Доцільність розроблення Концепції інформаційної безпеки людини зумовлена, на нашу думку, необхідністю вдосконалення національного законодавства про кібернетичну безпеку в сенсі закріплення поняття «кібернетична безпека людини», правового забезпечення кібернетичної безпеки людини, формування системи забезпечення безпеки особи в інформаційній сфері як сукупності відповідних сил і засобів.

Висновки. З огляду на особливості сучасного стану інформаційних прав і свобод людини, вбачається доцільним розроблення й ухвалення відповідної міжнародної угоди у сфері інформації прав, котра стане підґрунтям запровадження у національні законодавства міжнародних зобов'язань стосовно гарантування інформаційних прав і свобод, забезпечення кібернетичної безпеки особи, регулювання низки фундаментальних питань щодо, зокрема, захисту прав суб'єктів персональних даних (скажімо, про транскордонне передання таких даних). Окрім того, важливим убачається впровадження ефективних механізмів забезпечення кібернетичної безпеки особи, створення задля цього відповідних національних і міжнародних інституцій.

Отже, досягнення завдань даного дослідження потребує уважного вивчення форм і механізмів співробітництва, дієвих правових інструментів протидії існуючим і потенційним інформаційно-безпековим викликам і загрозам, які передбачені чинними угодами про співпрацю у цій сфері.

У статті проаналізовано основні тенденції розвитку кіберпростору, а також визначено пов'язані із цим актуальні проблеми забезпечення кібербезпеки на глобальному та національному рівнях, зокрема у контексті забезпечення безпеки об'єктів критичної інфраструктури, становлення Інтернету речей тощо. За результатами дослідження визначено можливі шляхи вирішення відповідних проблем та підвищення ефективності забезпечення кібербезпеки.

Акцентовано увагу на актуальності для України питань кіберзахисту цивільних ядерних об'єктів та інших об'єктів критичної інфраструктури. Відсутність конкурентоспроможних вітчизняних рішень на ринку змушує використовувати імпортні аналоги обладнання та програмного забезпечення.

Розроблено систему кібернетичних загроз із зазначенням їх джерел та змісту руйнівної дії.

Обґрунтовано, що швидка інформатизація, масштаби потенційних наслідків злочинів у кіберпросторі, недостатня кіберзахищеність об'єктів критичної інфраструктури та ризики, пов'язані з розвитком психологічної Інтернет-залежності, вимагають від національних урядів та міжнародної спільноти серйозної уваги до розвитку систем кібербезпеки на національному та глобальному рівнях. Першочергові кроки у цьому напрямі повинні передбачати розроблення необхідної нормативно-правової бази і підвищення ефективності роботи відповідних інституційних структур з урахуванням зарубіжного досвіду у цій сфері.

На глобальному рівні, зважаючи на те, що не всі кібератаки підпадають під дію існуючих міжнародних механізмів протидії кіберзлочинам, для забезпечення кібербезпекиважливимєпередбачити зобов'язання держав не вдаватися

у кіберпросторі до дій, метою яких є завдання збитків інформаційним системам, процесам і ресурсам іншої держави, критичній інфраструктурі тощо заради здійснення підриву політичної, економічної й соціальної систем, масованої психологічної обробки населення, що здатні дестабілізувати життєдіяльність суспільства й держави.

Ключові слова: кібербезпека, інформаційна безпека, кіберпростір, кіберзагрози, кіберсистема, критична інфраструктура, Інтернет речей.

Tarasyuk A. Ensuring cybernetic human security: international legal aspect

The article analyzes the main trends of cyberspace development and identifies related cyber security issues at the global and national levels, in particular in the context of security of critical infrastructure, the emergence of the Internet of Things, and more. The results of the study identified possible ways to solve the problems and increase the effectiveness of cybersecurity.

Emphasis is placed on the relevance of Ukraine to the issues of cyber defense of civilian nuclear facilities and other critical infrastructure. The lack of competitive domestic solutions in the market forces the use of imported analogues of hardware and software.

A system of cyber threats, indicating their sources and the content of the destructive action, has been developed.

It is substantiated that rapid information, the scale of the potential consequences of cybercrime, the lack of cyber security of critical infrastructure and the risks associated with the development of psychological Internet addiction require national governments and the international community to pay serious attention to the development of cybersecurity systems . The first steps in this direction should include the development of the necessary legal framework and the improvement of the efficiency of the work of the respective institutional structures, taking into account foreign experience in this field.

At the global level, given that not all cyber-attacks are subject to existing international cybercrime mechanisms, it is important for cybersecurity to ensure that states are not obliged to act in cyberspace to damage other information systems, processes and resources. the state, critical infrastructure, etc., for the sake of undermining the political, economic and social systems, massive psychological treatment of the population, which are capable of destabilizing the life of society and the state and you.

Key words: cybersecurity, information security, cyberspace, cyber threats, cybersystem, critical infrastructure, internet of things.

Література

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

2. 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.

3. Резолюція Генеральної Асамблеї ООН від 9 грудня 1998 р. A/53/144. URL: http://www.un.org/ru/documents/decl_conv/declarations/defender.shtml.

4. Резолюція 60/45, ухвалена Генеральною Асамблеєю Організації Об'єднаних Націй, «Досягнення у сфері інформатизації й телекомунікацій у контексті міжнародної безпеки». URL: https://zakon.rada.gov.ua/laws/show/995_e45.

5. Budapest Convention and related standards. URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention.

6. Constitution of the international telecommunication union. URL: https://www.itu.int/council/pd/constitution.html.

7. 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%3AOJ.L_.2016.194.01.0001.01.ENG&toc=OJ%3AL%3A2016%3A194%3ATOC.

8. Ткачук Т.Ю. Інформація з обмеженим доступом на підприємстві: проблеми безпеки та захисту. Право України. 2011. № 3. С. 243–252.

9. Ткачук Т.Ю. Сучасні загрози інформаційній безпеці держави: теоретико-правовий аналіз. Підприємництво, господарство і право. 2017. № 10. С. 182–186.