

РОЗДІЛ 10 МІЖНАРОДНЕ ПРАВО

УДК 341.12 + 341.215.4 + 341.4

DOI <https://doi.org/10.32782/2307-3322.61-2.33>

ВНЕСОК РАДИ ЄВРОПИ У ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ТА ПРОТИДІЮ КІБЕРЗЛОЧИННОСТІ

COUNCIL OF EUROPE'S CONTRIBUTION TO INFORMATION SECURITY AND COMBATING CYBERCRIME

Сироїд Т.Л.,

*доктор юридичних наук, професор,
завідувач кафедри міжнародного і європейського права
Харківського національного університету імені В.Н. Каразіна*

Гавриленко О.А.,

*доктор юридичних наук, професор,
професор кафедри міжнародного і європейського права
Харківського національного університету імені В.Н. Каразіна*

У статті проаналізовано положення правових актів Ради Європи, спрямованих на забезпечення інформаційної безпеки, зокрема, проаналізовано положення Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 р., Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних 2001 р., щодо органів нагляду та транскордонних потоків даних, Протокол про внесення змін до Конвенції про захист фізичних осіб стосовно автоматичної обробки персональних даних (відкритий для підписання 10 жовтня 2018 р.), Керівних принципів щодо штучного інтелекту і захисту даних. Зважаючи на ту обставину, що Організація приділяє суттєву увагу захисту прав людини, зокрема, таким основоположним правам, передбаченим Конвенцією про захист прав і основоположних свобод 1950 р., як право на свободу слова, право на свободу зборів і асоціацій, право на приватне життя і право на ефективний засіб правового захисту під час використання сучасних технологій у діяльності журналістів, у статті висвітлено основні положення Декларації Комітету Міністрів про ризики для основних інформаційно-комунікаційних технологій, зокрема, Інтернет-середовища, використанню прав, пов'язаних з цифровим відстеженням й іншими технологіями спостереження 2013 р., рекомендації Комітету Міністрів Ради Європи CM / Rec (2016) 1 «Про захист й заохочення права на свободу вираження поглядів та право на приватне життя щодо мережевого нейтралітету», рекомендації CM / Rec (2016) 5 Комітету Міністрів держав-членів щодо Інтернет-свободи, рекомендації Комітету Міністрів PE CM/Rec (2016)2 «Інтернет для громадськості», резолюції Парламентської Асамблеї Ради Європи 2001(2014) «Насилля в/через засоби масової інформації», рекомендації CM / Rec (2016)4 Комітету Міністрів держав-членів щодо захисту журналістики і безпеки журналістів та інших медіа-учасників. Акцентуючи увагу на зусиллях, які докладає Рада Європи до протидії протиправному використанню ІКТ, акцентовано на значимості Конвенції про кіберзлочинність. Розкрито сутність рекомендації Парламентської Асамблеї Ради Європи 2070 (2015) щодо зміцнення співробітництва у протидії з кібертероризмом та іншими масовими атаками у мережі Інтернет, рекомендації Парламентської Асамблеї Ради Європи 2077 (2015) «Зміцнення співробітництва у протидії з кібертероризмом та іншими масовими атаками у мережі Інтернет», зроблено відповідні висновки та рекомендації.

Ключові слова: безпека, захист, Інтернет, інформаційно-комунікаційні технології, кіберзлочини, права людини, правопорушення.

The article analyses the provisions of Council of Europe's legal acts aimed at ensuring information security, including the provisions of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 1981, Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data of 2001 regarding supervisory authorities and transborder data flows, Protocol amending the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (open for signature since October 10, 2018), Guidelines on Artificial Intelligence and Data Protection. Considering the fact that the Organization pays close attention to the protection of human rights, in particular to such fundamental rights as enshrined in the Convention for the Protection of Rights and Fundamental Freedoms of 1950, – as the right to freedom of expression, the right to freedom of assembly and association, the right to privacy and the right for an effective remedy, the use of information and communication technologies, particularly, the Internet environment, the use of modern technologies in the activity of journalists – the article outlines the main provisions of the Declaration of the Committee of Ministers on Risks to Fundamental Rights stemming from Digital Tracking and other Surveillance Technologies of 2013, Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality, Recommendation CM/Rec(2016)5 of the Committee of Ministers to member States on Internet freedom, Recommendation CM/Rec(2016)2 of the Committee of Ministers on Internet for citizens, Resolution 2001 (2014) of the Parliamentary Assembly "Violence in and through the media", Recommendation CM/Rec(2016)4 of the Committee of Ministers to member States on the protection of journalism and the safety

of journalists and other media actors. Emphasizing the efforts made by the Council of Europe to counteract the illicit use of information and communication technology, the focus is on the importance of the Convention on Cybercrime. The essence of the Council of Europe Parliamentary Assembly Resolution 2070 (2015) and Recommendation 2077 (2015) on increasing cooperation against cyberterrorism and other large-scale attacks on the Internet is revealed. Relevant conclusions and recommendations are made.

Key words: security, protection, Internet, information and communication technology, cybercrime, human rights, offense.

Постановка проблеми. Останнім часом міжнародне співтовариство стикається з низкою нових і складних загроз безпеці, зокрема й інформаційній, що спонукає до необхідності подальшого синергізму та ще більш тісної співпраці на всіх рівнях. Безперечно, поява інформаційно-комунікаційних технологій (далі – ІКТ), які в широкому розумінні охоплюють усі сфери створення, передачі, зберігання та сприйняття інформації, не обмежуючись лише комп'ютерними технологіями, сприяла прогресивному розвитку міжнародної спільноти загалом, економіки держав, суттєво просунула вперед людську цивілізацію. Разом із тим реалії сьогодення свідчать також про негативну сторону цього процесу – використання злочинцями баз даних для вчинення протиправних діянь, які зачіпають інтереси усіх користувачів послуг, без будь-яких винятків. Загрози стають все більш різноманітними, а також все більш транскордонними і міжсекторальними. Ці загрози вимагають ефективного і скоординованого реагування держав, міжнародних інституцій та світового співтовариства загалом, що спонукає до розробки правового підґрунтя такої діяльності як на міжнародному універсальному, так і на регіональному рівнях.

Стан наукової розробки проблеми. Слід зазначити, що окремі аспекти означеної проблематики, пов'язані з питаннями правового регулювання забезпечення безпеки на універсальному рівні, співробітництва держав в означеній сфері, загальними питаннями забезпечення безпеки, висвітлено в роботах вітчизняних і зарубіжних науковців, зокрема: А.В. Войціховського, Н.М. Ємельянової, І.М. Забари, Л.О. Фоминої, О.М. Фролової, Т.К. Хартлі та інших. Разом із тим означена тематика потребує подальшого дослідження з урахуванням сучасних реалій.

Стаття має на меті розкрити сутність правової основи Ради Європи щодо забезпечення інформаційної безпеки та протидії кіберзлочинності.

Завданнями дослідження є – проаналізувати конвенційні норми, резолюції, рекомендації, якими регламентовано забезпечення інформаційної безпеки та протидії кіберзлочинності в межах Ради Європи; акцентувати увагу на значимості цих актів в аспекті захисту прав людини; зробити відповідні висновки і рекомендації, спрямовані на удосконалення положень означених актів.

Виклад основного матеріалу. Суттєвий внесок у розвиток міжнародно-правового регулювання використання і забезпечення безпеки у сфері ІКТ зроблено на міжнародному регіональному рівні. Так, питання щодо комп'ютерних злочинів знаходиться в центрі уваги міжнародних регіональних організацій, зокрема Ради Європи. Починаючи з 1976 р. Організацією означене питання виносилося на обгово-

рення конференцій з аспектів економічних злочинів; Комітетом Міністрів РЄ було прийнято рекомендації про визнання міжнародного характеру комп'ютерної злочинності (R(89)9), щодо вивчення проблем, які виникають із транснаціональними комп'ютерними злочинами (R(95)13); створено Комітет експертів для обговорення правових аспектів комп'ютерних злочинів (1985 р.); засновано Комітет по боротьбі з кіберзлочинністю (1996 р.) тощо.

У 1981 р. Радою Європи укладено Конвенцію про захист осіб у зв'язку з автоматизованою обробкою персональних даних (ETS № 108), метою якої є забезпечення на території кожної Сторони для кожної особи, незалежно від її громадянства або місця проживання, дотримання прав і основоположних свобод, зокрема права на недоторканість приватного життя, у зв'язку з автоматизованою обробкою персональних даних, що її стосуються. Сфера застосування – це файли персональних даних для автоматизованої обробки й автоматизована обробка персональних даних у державному та приватному секторах. Конвенція містить положення щодо якості персональних даних, безпеки, гарантій; надання взаємної допомоги; передбачає створення Консультативного комітету з метою нагляду за дотриманням положень Конвенції (ст.1, 3) [1]. У 2001 р. прийнято Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних (СЕД № 181), який передбачає, по-перше, створення національних наглядових органів, відповідальних за забезпечення дотримання законів або нормативних актів, прийнятих відповідно до Конвенції, по-друге, поліпшує транскордонні потоки передачі даних третім країнам. Дані можуть передаватися тільки в тому разі, якщо держава-одержувач або міжнародна організація можуть забезпечити адекватний рівень захисту [2].

У 2018 році відкрито Протокол про внесення змін до Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних (СДСЕ № 223), який має на меті модернізувати і вдосконалити Конвенцію (ETS № 108) з урахуванням нових проблем, що виникають у галузі захисту фізичних осіб щодо обробки персональних даних з моменту прийняття Конвенції (йменується «Конвенція 108+»). Оновлення Конвенції, яка є єдиним юридично зобов'язуючим міжнародним інструментом глобального масштабу в цій галузі, вирішує проблеми, пов'язані з дотриманням недоторканості приватного життя, використання нових інформаційних і комунікаційних технологій та зміцнення механізму Конвенції з тим, щоб гарантувати її ефективне здійснення. Протокол встановлює багатосторонню

правову основу, яка є одночасно міцною і гнучкою, покликана сприяти транскордонним потокам даних, пропонуючи при цьому ефективні гарантії у випадку використання персональних даних.

Серед новел протоколу слід зазначити такі: підвищення вимог, що стосуються принципів пропорційності і мінімізації даних, а також законності обробки; розширення каталогу конфіденційних даних, який включає генетичні і біометричні дані, а також дані, що стосуються членства в профспілках та етнічного походження; зобов'язання повідомляти про порушення даних; прозорість щодо обробки даних; нові права надаються фізичним особам у контексті прийняття рішень на основі алгоритмів, що особливо важливо в контексті розвитку штучного інтелекту; посилення відповідальності контролерів даних; обов'язкове застосування принципу «поваги до особистого життя з моменту зачаття»; застосування принципів захисту даних до всієї обробки, включаючи обробку, здійснювану з міркувань національної безпеки (з винятками і можливими обмеженнями відповідно до умов, визначених у Конвенції), що підлягає в усіх випадках незалежному і ефективному контролю та нагляду; встановлення чіткого режиму для транскордонних потоків даних; зміцнення повноважень та незалежності органів із захисту даних, а також правових основ, необхідних для міжнародного співробітництва [3].

Суттєвим доповненням до Конвенції (ETS № 108) стало прийняття Керівних принципів щодо штучного інтелекту і захисту даних, що покликані допомогти особам, які займаються розробкою штучного інтелекту, виробникам і постачальникам послуг у забезпеченні того, щоб програми, які використовують штучний інтелект, не порушували право на захист персональних даних [4].

Комітет з Конвенції підкреслює, що захист прав людини, включаючи право на захист персональних даних, є вкрай важливим під час розробки та затвердження програм, що використовують штучний інтелект, зокрема, коли вони застосовуються у процесах прийняття рішень, і що він повинен ґрунтуватися на принципах оновленої конвенції про захист персональних даних. Крім того, за будь-якої інновації в галузі штучного інтелекту необхідно приділяти пильну увагу тому, щоб запобігати і зменшувати потенційні ризики обробки персональних даних і надавати можливість суб'єктам даних здійснювати реальний контроль за обробкою даних і її наслідками.

Рада Європи постійно удосконалює та розширює правовий простір регулювання в інформаційній сфері. До чого її спонукають зміни, пов'язані саме з широким використанням Internet та Internet-ЗМІ. У зв'язку з цим під егідою Організації прийнято низку резолюцій та рекомендацій, зокрема: резолюція 1191 (1999) «Про інформаційне суспільство та цифровий світ», рекомендація 1332 (1997) «Про науково-технічні аспекти нових інформаційно-комунікаційних технологій», резолюція 1120 (1997), «Про вплив нових інформаційно-комунікаційних техно-

логій на демократію», рекомендація 1314 (1997) «Про нові технології та працю», рекомендація Парламентської Асамблеї Ради Європи (далі – ПАРЄ) № 2075 (2015) «Медіа відповідальність та етика у мінливому медіа-середовищі» тощо.

Особливе місце серед означених актів займають резолюції і рекомендації, які мають на меті регулювання використання ІКТ і захист прав людини, серед яких слід вказати такі: рекомендація 582 (1970) «Про медіа масових комунікацій та права людини», резолюція 428 (1970), резолюція Комітету Міністрів № (74)26 «Про право на відповідь – позиція особи щодо преси», рекомендація 1277 (1995) «Мігранти, етнічні меншини та ЗМІ», рекомендація № (97)21 «Про медіа та сприяння культурі терпимості», рекомендація 1555 (2002), «Про образ жінок у ЗМІ», рекомендація № (2004)16 «Про право на відповідь у новому медіа-середовищі», рекомендація 1882 (2009) «Про сприяння Інтернет та онлайн-медіа послуг для неповнолітніх», декларація Комітету Міністрів про ризики для основних прав пов'язаних з цифровим відстеженням та іншими технологіями спостереження 2013 р. тощо.

Зокрема, рекомендація Комітету Міністрів Ради Європи № CM / Rec (2016) 1 «Про захист й заохочення права на свободу вираження поглядів та право на приватне життя щодо мережевого нейтралітету» закликає держави-члени до вжиття усіх необхідних заходів у співпраці з усіма зацікавленими сторонами, щоб гарантувати принцип мережевого нейтралітету в межах своєї політики з належним урахуванням принципів, викладених у додатку до неї; поширювати ці принципи в інших міжнародних і регіональних форумах, які займаються питанням мережевого нейтралітету. У Додатку 1 до Рекомендації містяться Методичні рекомендації щодо мережевого нейтралітету, якими передбачено права інтернет-користувачів; рівноправність процедур інтернет-трафіку; положення щодо плюралізму і різноманітності інформації; захисту персональних даних; прозорості, сутність якої полягає у наданні користувачам ясної, повної та загальнодоступної інформації щодо будь-яких методів управління трафіком, які могли б уплинути на доступ користувачів до розподілу контенту, додатків і послуг; відповідальність Інтернет-провайдерів у разі порушення принципів, передбачених рекомендацією [5].

Рекомендація CM / Rec (2016) 5 Комітету Міністрів держав-членів щодо Інтернет-свободи містить визначення Інтернет-свободи, під якою розуміється як здійснення і володіння в Інтернеті правами людини й основними свободами, так і їх захист відповідно до Конвенції про захист прав і основоположних свобод (далі – Конвенція). Ці індикатори Інтернет-свободи зосереджуються на праві на свободу слова, праві на свободу зборів і асоціацій, праві на приватне життя і праві на ефективний засіб правового захисту. Вони ґрунтуються на наявних і встановлених стандартах у галузі прав людини й механізмів примусу. Комплексний підхід до Інтернет-свободи враховує всі індикатори, оскільки вони призначені забезпечити

керівництво в проведенні якісної і об'єктивної оцінки і представленні доповідей про свободу Інтернету в державах – членах Ради Європи. Вони не призначені для оцінки рівня свободи Інтернету або в якості засобу порівняння країн.

Рекомендацією акцентовано увагу на зобов'язаннях держав – членів Ради Європи щодо дотримання, захисту і заохочення прав людини й основних свобод в Інтернеті; вжиття активного підходу до імплементації Конвенції та інших стандартів Ради Європи щодо Інтернету; всеосяжності розуміння свободи Інтернету та її гарантування.

Документ містить низку положень, що стосуються нормативного регулювання Інтернет-свободи державами-членами під час розробки національного законодавства, акцентуючи увагу на його повній відповідності Конвенції [6].

Рекомендація Комітету Міністрів РЄ № CM/Rec (2016)2 «Інтернет для громадськості» містить керівництво у формуванні та реалізації політики у сфері Інтернету, рекомендації щодо модернізації закладів культури, перетворення споживачів на креативних громадян, також висвітлює аспекти щодо забезпечення багатосторонньої грамотності з питань доступу, створення та управління цифровою культурою [7].

ПАРЄ у своїй резолюції 2001(2014) «Насилля в/через ЗМІ» зазначила, що за останнє десятиліття медійний простір змінився у зв'язку з величезним розвитком Internet та Internet-ЗМІ. Означена обставина і зближення традиційних ЗМІ та соціальних мереж з можливістю обміну інформацією між користувачами створили нові форми насилля у ЗМІ. Через це існуючі правила та положення щодо насилля в ЗМІ стикаються з проблемами як юридичного, так і практичного характеру. Насилля в/через ЗМІ може набувати різних форм, починаючи з явного або вербального до зображення психологічного або фізичного насилля, у тому числі сексуального. Таке насилля може бути спрямоване на вигаданих персонажів або людей, з урахуванням того, що відмінності між цими двома категоріями стираються завдяки технологічним досягненням у комп'ютерній анімації. Інтерактивність комп'ютерних ігор, можливостей Internet (соціальних мереж, чатів, пошукових систем, купівлі в Internet) і загальна доступність цих медіа (через смартфони) створюють додаткові можливості для користувачів використовувати розкручене в/через ЗМІ насилля та ідентифікувати себе (пп. 2, 3) [8].

Окремої уваги заслуговують акти Ради Європи щодо захисту журналістики і журналістів, які є представниками мас-медіа, що широко застосовують у своїй діяльності ІКТ, серед яких слід зазначити такі: Конвенція щодо захисту журналістів: резолюція 1438 та Рекомендація 1702 (2005) «Про свободу преси та умови роботи журналістів у зонах конфлікту», резолюція 1003 та рекомендація 1215 (1993) «Про журналістську етику», рекомендація 1950 (2011) «Про захист журналістських джерел».

2016 рік ознаменовано прийняттям рекомендації CM / Rec (2016)4 Комітету Міністрів держав-членів

щодо захисту журналістики і безпеки журналістів та інших медіа-учасників, яка містить Керівні принципи, що є невіддільною частиною цієї рекомендації, в яких містяться низка положення стосовно держав-членів щодо прийняття ними відповідних законодавчих, адміністративних та інших заходів з метою зміцнення захисту журналістики і впровадження наявних міжнародних та регіональних стандартів, а також посилення в дотриманні існуючих механізмів моніторингу та ініціатив. Керівні принципи розподілені на чотири групи: запобігання, захист, притягнення до відповідальності (у тому числі звертаючи особливу увагу на співтовариства) та поширення інформації, навчання та підвищення обізнаності, що пропонуються державам-членам для виконання своїх відповідних зобов'язань, поєднуючи правові, адміністративні та практичні заходи [9].

Суттєве значення в цьому аспекті мають положення рекомендації ПАРЄ № 2075 (2015) «Медіа відповідальність та етика у мінливому медіа середовищі», яка рекомендує Комітету Міністрів: закликати держави-члени винести на розгляд питання щодо присутності права на відповідь у своєму внутрішньому законодавстві та запевнити, що це право на відповідь, надане медіа, є офіційно визнаним судами у разі виникнення судового процесу проти цих медіа за ті ж факти; виробити методичні рекомендації для урядів з метою підтримки національної саморегуляції медіа, поважаючи при цьому свободу медіа відповідно до Конвенції про захист прав і основоположних свобод людини; посилити практичну діяльність, спрямовану на підвищення рівня етичних стандартів саморегуляції серед журналістів і представників медіа, у тому числі підтримку професійної підготовки для журналістів та підтримку компаній громадського державного мовлення відповідно до встановлених етичних норм; забезпечити більш практичні напрями діяльності Ради Європи, такі як кампанія молодіжного сектору Ради Європи «Рух проти ненависті», «Роль медіа у зміцненні різноманіття в Європі» (MEDIANE) та програм Європейської Федерації журналістів і Ради Європи «Медіа проти расизму у спорті» (MARS) [10].

Задля забезпечення інформаційної безпеки з метою протидії порушенням у сфері використання ІКТ Радою Європи у 2001 р. було прийнято Конвенцію про кіберзлочинність, яка містить норми матеріального кримінального права щодо видів правопорушень, які охоплюються цим договором, серед яких: незаконний доступ, нелегальне перехоплення, підробка, пов'язана з комп'ютером, шахрайство, пов'язане з комп'ютером, правопорушення, пов'язані зі змістом, правопорушення, пов'язані з порушенням авторських та суміжних прав, тощо; норми кримінально-процесуального права щодо проведення процедури розслідування та переслідування; положення щодо міжнародного співробітництва, які регламентують процедуру екстрадиції, надання взаємної правової допомоги. З метою покращення співпраці, Конвенцією передбачено створення сторонами на

національному рівні органу для здійснення контактів цілодобово з метою надання негайної допомоги для розслідування або переслідування щодо кримінальних правопорушень, пов'язаних із комп'ютерними системами і даними, або з метою збирання доказів у електронній формі, що стосуються кримінального правопорушення. Така допомога включає сприяння або, якщо це дозволяється її внутрішньодержавним законодавством і практикою, пряме: а) надання технічних порад; б) збереження даних відповідно до статей 29 (Термінове збереження комп'ютерних даних, які зберігаються) і 30 (Термінове розкриття збережених даних про рух інформації); та с) збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних (ст. 35) [11]. Конвенція відкрита для підписання для держав, які не є членами Ради Європи, і слугує основою для розвитку міжнародної співпраці у цій галузі. У 2003 р. прийнято Додатковий протокол до Конвенції, спрямований на протидію розповсюдженню через комп'ютерні мережі інформації расистського та ксенофобського характеру, що здійснюється за допомогою інформаційних систем [12].

Негативною ознакою сьогодення стало використання ІКТ у скоєнні терористичних злочинів. У 2015 р. ПАРЕ прийняла рекомендацію № 2070 щодо зміцнення співробітництва у протидії з кібертероризмом та іншими масовими атаками у мережі Інтернет. Рекомендація підкреслює значення Ради Європи у вирішенні глобального виклику, пов'язаного з безпекою комп'ютерних мереж у зв'язку з появою кібертероризму та інших масових атак, що діють на/через комп'ютерні системи, являючи собою серйозну загрозу національній безпеці, громадській безпеці та добробуту країн [13].

Рекомендацією ПАРЕ № 2077 (2015) «Зміцнення співробітництва у протидії з кібертероризмом та іншими масовими атаками у мережі Інтернет» Асамблея рекомендує Комітету Міністрів: запросити Сторони Конвенції про кіберзлочинність та її Додаткового протоколу про кіберзлочинність, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (ETS №185 та 189), дослідити, чи можна реалізувати: проект додаткового протоколу, що визначає загальний рівень криміналізації масових кібератак, у тому числі обтяжуючих обставин цих атак, а також мінімальні стандарти для покарання за ці ж атаки; проект іншого додаткового протоколу про взаємну допомогу щодо слідчих повноважень, які визначені, зокрема, у змісті та застосуванні статті 32 Конвенції, відповідно до Директивної записки Комітету з кіберзлочинності, якого представляють Сторони конвенції; запросити Групу зі збору доказів «хмар», створену при Комітеті з кіберзлочинності, дослідити можливість розробки додаткового протоколу Конвенції про кіберзлочинність з питань доступу кримінального судочинства до бази даних «хмарних серверів»; проект правових стандартів про міжнародну відповідальність держав щодо вживання усіх доцільних заходів

для запобігання масовим кібератакам, які були скоєні особами, що своєю чергою підпадають під юрисдикцію своєї держави або, виходячи з території своєї держави, борються з комп'ютерними системами іншої держави; збільшити допомогу та моніторинг дій для імплементації Конвенції про кіберзлочинність відповідно до внутрішнього законодавства та практик, а також практичних заходів і співробітництва у боротьбі з масовими кібератаками, зокрема, на користь держав-членів, які стикаються з труднощами практичної імплементації Конвенції з кіберзлочинності тощо [14].

Висновки. З огляду на вищезазначене маємо можливість дійти висновку, що активне впровадження та застосування «високих технологій» у багатьох сферах суспільного життя є невіддільним складником сучасного світу. Це значно полегшує транскордонний обмін даними та сприяє їх ефективній систематизації, створює широкі можливості для пошуку інформації та її обробки тощо. Разом з тим використання ІКТ породжує нові загрози, стає глобальним викликом, пов'язаним з безпекою комп'ютерних мереж, у зв'язку із появою кібертероризму та інших масових атак, що вчиняються через комп'ютерні системи, представляючи серйозну загрозу національній безпеці, громадській безпеці, правам людини та добробуту країн.

Будучи невіддільним складником міжнародної інформаційної системи забезпечення безпеки, Рада Європи, з моменту свого створення, вносить істотний внесок до її розвитку шляхом розробки і вдосконалення її правової та інституційної основи. Разом з тим варто зазначити, що ефективність регіональних норм як підґрунтя інформаційної безпеки й колективної відповідальності держав перед людством має ґрунтуватися на конструктивному співробітництві учасників міжнародного спілкування у вирішенні двох основних завдань: перше з них пов'язане із забезпеченням функціонування того механізму підтримання, яким міжнародне співтовариство вже володіє, друге має полягати у виробленні нових правових норм. З огляду на це Рада Європи, розробивши низку актів, що зачіпають такі важливі напрями, як забезпечення всеосяжної інформаційної безпеки, дотримання прав людини, протидії зловживанням у сфері ІКТ тощо, постійно працює над удосконаленням як правового, так і інституційного складника, про що свідчить відкриття для підписання у 2018 р. Протоколу про внесення змін до Конвенції про захист фізичних осіб у зв'язку з автоматизованою обробкою персональних даних, створення Спеціального комітету з питань штучного інтелекту тощо. Разом з тим з огляду на стрімкий розвиток ІКТ та їхнє активне використання як окремими особами, так і в діяльності державних і міжнародних структур, нагальним є питання співпраці міжнародного співтовариства, обмін науковими дослідженнями у цій галузі, які повинні слугувати на користь міжнародній спільноті та сприяти забезпеченню інформаційної безпеки, як складнику всеосяжної безпеки людства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28 січня 1981 р. URL: http://zakon4.rada.gov.ua/laws/show/994_326 (дата звернення 20.03.20).
2. Додатковий протокол до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних щодо органів нагляду та транскордонних потоків даних від 8 листопада 2001 р. URL: http://uazakon.com/documents/date_6/pg_gswaww.htm (дата звернення 23.03.20).
3. Protocole d'amendement à la Convention pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel. URL: <https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016808ac919>. (дата звернення 2.04.20).
4. Consultative Committee of the Convention for the protection of individuals with regard to automatic processing of personal data (Convention 108) Guidelines on artificial intelligence and data protection. URL: <https://rm.coe.int/guidelines-on-artificial-intelligence-and-data-protection/168091f9d8> (дата звернення 2.04.20).
5. Recommendation CM/Rec(2016)1 of the Committee of Ministers to member States on protecting and promoting the right to freedom of expression and the right to private life with regard to network neutrality. URL: <https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec%282016%291&Language=lanEnglish&Ver=original&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true> (дата звернення 27.03.20).
6. Рекомендація CM / Rec (2016) 5 Комітету Міністрів держав-членів щодо Інтернет-свободи. URL: [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2016\)5](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)5) (дата звернення 20.03.20).
7. Recommendation CM/Rec(2016)2 of the Committee of Ministers to member States on the Internet of citizens. URL: [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2016\)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)2&Language=lanEnglish&Ver=original&Site=CM&BackColorInternet=C3C3C3&BackColorIntranet=EDB021&BackColorLogged=F5D383&direct=true) (дата звернення 20.03.20).
8. Резолюція Парламентської асамблеї Ради Європи 2001 (2014) «Насилля в та через 3МІ». URL: [http://w1.c1.rada.gov.ua/pls/mpz/docs/1967_rez_2001_\(2014\).htm](http://w1.c1.rada.gov.ua/pls/mpz/docs/1967_rez_2001_(2014).htm) (дата звернення 25.03.20).
9. Рекомендація CM / Rec (2016)4 Комітету Міністрів держав-членів стосовно захисту журналістики і безпеки журналістів та інших медіа учасників. URL: [https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec\(2016\)4](https://wcd.coe.int/ViewDoc.jsp?p=&Ref=CM/Rec(2016)4) (дата звернення 29.03.20).
10. Рекомендація Парламентської Асамблеї Ради Європи № 2075(2015) «Медіа-відповідальність та етика у мінливому медіа-середовищі». URL: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21961&lang=en> (дата звернення 20.03.20).
11. Конвенция о киберпреступности. URL: <http://conventions.coe.int/Treaty/EN/Treaties/Html/185.htm> (дата звернення 25.03.20).
12. Дополнительный протокол к Конвенции о киберпреступности относительно криминализации деяний расистского и ксенофобского характера, совершаемых при помощи информационных систем. URL: <http://conventions.coe.int/Treaty/RUS/Treaties/Html/189.htm> (дата звернення 25.03.20).
13. Резолюция 2070 (2015) Расширение сотрудничества в борьбе с кибертерроризмом и другими широкомасштабными агрессивными действиями в Интернете (стр. 67–70). URL: <https://rm.coe.int/168062f8d9>
14. Рекомендація Парламентської Асамблеї Ради Європи № 2077(2015) «Зміцнення співробітництва у протидії з кібертероризмом та іншими масовими атаками у мережі Інтернет». URL: <http://assembly.coe.int/nw/xml/XRef/Xref-XML2HTML-EN.asp?fileid=21976> (дата звернення 20.03.20).