УДК 341
DOI https://doi.org/10.32850/2414-4207.2019-10.20

ОСОБЛИВОСТІ КОНВЕНЦІЙНОГО МЕХАНІЗМУ МІЖНАРОДНОГО СПІВРОБІТНИЦТВА В БОРОТЬБІ ЗІ ЗЛОЧИННІСТЮ В ЄВРОПЕЙСЬКОМУ СОЮЗІ (НА ПРИКЛАДІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ)

Нуруллаєв Ількін Садагат огли,
кандидат юридичних наук,
керівник Генеральної інспекції
(Генеральна прокуратури України,
м. Київ, Україна)

Стаття присвячена дослідженню деяких особливостей регіонального міжнародно-правового співробітництва в боротьбі зі злочинністю держав ЄС. У статті зазначено, що специфікою міжнародно-правового співробітництва в боротьбі зі злочинністю на регіональному рівні в межах ЄС є те, що воно здійснюється державами цього регіону під егідою міжнародних регіональних організацій, членами яких вони є. У таких випадках, відповідно до укладених угод, також передбачається створення спеціальних конвенційних органів міжнародно-правового співробітництва, які можуть діяти на додаток до постійно діючих міжнародних організаційно-правових інструментів міжнародно-правової співпраці. У процесі такої співпраці останніми роками простежується тенденція активізації взаємодій у цьому напрямі шляхом укладення основоположних для цього питання регіональних угод, створюючи не тільки юридичні механізми боротьби зі злочинністю, а й практичні, що втілюються в роботі різних спеціальних регіональних інституцій.

Автор досліджує особливості створення й діяльності регіональних конвенційних органів боротьби зі злочинністю на прикладі запобігання кіберзлочинності й боротьби з нею. Це відносно новий напрям міждержавного співробітництва держав ЄС.

Необхідність у дослідженні правових особливостей конвенційних регіональних механізмів боротьби з міжнародною злочинністю в межах ЄС на прикладі протидії кіберзлочинності вбачається в тому, що, з одного боку, національне законодавство держав-членів ЄС є відносно «старим» і найчастіше не ухвалене з урахуванням особливостей злочинів, що здійснюються в кіберпросторі, а з іншого – ураховуючи транснаціональний характер цього злочину, держави не здатні захистити свій правопорядок без взаємодії з іншими учасниками міжнародних відносин. Основою проблемою в цьому стосунку стала складність застосування чинних норм кримінального права до кіберзлочинів. У цьому контексті актуальним є питання розвитку міжнародно-правового регулювання, спрямованого на боротьбу з кіберзлочинністю, і втілення механізмів їх імплементації, спрямованих на гармонізацію кримінального законодавства держав-членів ЄС у цій сфері.

Зазначається, що однією з основних проблем співробітництва держав ЄС у боротьбі з кіберзлочинністю є те, що Конвенція про кіберзлочинність 2001 року досі не підписана й не ратифікована багатьма державами, навіть ті з них, які взяли її норми за основу для встановлення відповідальності за комп'ютерні злочини на національному рівні, ще не здійснили криміналізації всіх правопорушень, визначених цим документом. До того ж комп'ютерні технології продовжують розвиватися й удосконалюватися, що найближчим часом може призвести до необхідності встановлення кримінальної від-

повідальності за нові види правопорушень у цій сфері. Автор висловлює сподівання, що належна реалізація Конвенції з кіберзлочинності 2001 року виправить недоліки боротьби з високотехнологічними злочинами, забезпечивши ефективну координацію дій правоохоронних органів різних держав. Наскільки ефективною виявиться ця координація насправді, а також чи вартує вона тієї ціни, яку доведеться заплатити громадянам, таємниця приватного життя яких опинилася під загрозою завдяки Конвенції, покаже час.

Ключові слова: міжнародна злочинність, кіберзлочинність, конвенційний механізм міжнародного співробітництва, Європейський Союз, Рада Європи.

PECULIARITIES OF THE CONVENTIONAL MECHANISM OF INTERNATIONAL COOPERATION ON CRIME IN THE EUROPEAN UNION (ON AN EXAMPLE OF CYBER CRIME)

Nurulayev Ilkin Sadagat Ogli,
Candidate of Law,
Head of the General Inspectorate
(Prosecutor General's Office of Ukraine,
Kyiv, Ukraine)

The article is devoted to the research of some features of regional international legal cooperation of the countries of the European Union in the fight against crime. The article states that the specificity of international legal cooperation in combating crime at the regional level within the European Union is that it is carried out by the countries of the region under the auspices of the international regional organizations of which they are members. In such cases, in accordance with the agreements concluded, it may also provide for the establishment of special convention bodies of international legal cooperation, which may act in addition to the permanent international legal and international instruments of international legal cooperation. In the course of such cooperation, in recent years, there has been a tendency to intensify interactions in this direction by concluding regional agreements that are fundamental to this issue, creating not only legal mechanisms for combating crime, but also practical ones that are embodied in the work of various special regional institutions.

The author explores the peculiarities of creation and activity of regional convention bodies for fighting crime on the example of cybercrime prevention and fight. This is a relatively new area of EU interstate cooperation.

The need to study the legal features of conventional regional mechanisms for combating international crime within the European Union, on the example of combating cybercrime, shows that, on the one hand, the national legislation of the EU Member States is relatively "old" and most often has not been approved, committed in cyberspace, and on the other, given the transnational nature of the crime, states are incapable of defending their rule of law without interacting with other participants in zhnarodnyh relations. The main problem in this regard was the complexity of applying existing criminal law rules to cybercrime. In this context, the issue of the development of international legal regulation aimed at combating cybercrime and the implementation of mechanisms for their implementation aimed at harmonizing the criminal legislation of the EU Member States in this area became urgent.

The article states that one of the major problems of EU countries' cooperation in the fight against cybercrime is that the 2001 Convention on Cybercrime has not yet been signed and ratified by many states, and even those that have adopted its norms as a basis for establishing those responsible for computer crimes at national level have not yet criminalized all offenses identified in this document. In addition, computer technology continues to evolve

and improve, which may in the near future lead to the need for criminal liability for new types of offenses in this area. Author hopes that the proper implementation of the 2001 Cybercrime Convention should remedy the shortcomings of the fight against high-tech crimes by ensuring effective coordination of law enforcement agencies in different countries. How effective this coordination will actually be, and whether it is worth the price it will have to pay to citizens whose privacy has been compromised by the Convention, time will tell.

Key words: international crime, cybercrime, conventional regional organization, international cooperation, European Union, Council of Europe.

Специфікою міжнародно-правового співробітництва в боротьбі зі злочинністю на регіональному рівні в межах Європейського Союзу (далі – ЄС) є те, що воно здійснюється державами цього регіону під егідою міжнародних регіональних організацій, членами яких вони є. У процесі такої співпраці останніми роками простежується тенденція активізації взаємодій у цьому напрямі шляхом укладення основоположних для цього питання регіональних угод, створюючи не тільки юридичні механізми боротьби зі злочинністю, а й практичні, що втілюються в роботі різних спеціальних регіональних інституцій.

Актуальність необхідності в дослідженні правових особливостей конвенційних регіональних механізмів боротьби з міжнародною злочинністю в межах ЄС на прикладі протидії кіберзлочинності убачається в тому, що, з одного боку, національне законодавство держав-членів ЄС не написане з урахуванням особливостей злочинів, що здійснюються в кіберпросторі, а з іншого – ураховуючи транснаціональний характер цього злочину, держави не здатні захистити свій правопорядок без взаємодії з іншими учасниками міжнародних відносин. Основою проблемою в цьому стосунку стала складність застосування чинних норм кримінального права до кіберзлочинів. У цьому контексті актуальним є питання розвитку міжнародно-правового регулювання, спрямованого на боротьбу з кіберзлочинністю, і втілення механізмів їх імплементації, спрямованих на гармонізацію кримінального законодавства держав-членів ЄС у цій сфері.

Варто зауважити, що ще в 1982 році в Парижі Організація Економічного співробітництва та розвитку (далі – ОЕСР) вирішила створити комітет експертів для вивчення і розгляду концепції комп'ютерних злочинів і проаналізувати потребу в реформуванні кримінальних законів держав цього регіону. Уже в 1986 році комітет експертів в Аналізі політики ОЕСР з юридичних питань зазначив, що, відповідно до активізації комп'ютерної злочинності міжнародного характеру, виявлено важливі питання, які потребують міжнародного співробітництва щодо контролю такої активності й боротьби з незаконними діяннями. Держави-учасниці повинні самі визначити межі, до яких відповідні покарання за діяння повинні бути передбачені в кримінальному законодавстві. До переліку таких діянь зараховано комп'ютерне шахрайство, комп'ютерну підробку документів, шкоду, що заподіяна комп'ютерним даним і програмам, і неавторизоване посягання на захищені комп'ютерні програми й неавторизований доступ до або перехоплення комп'ютерних систем [1].

Разом із тим однією з перших міжнародних регіональних організацій, які розпочали роботу в напрямі встановлення кримінальної відповідальності за комп'ютерні правопорушення, стала Рада Європи. У період з 1985 по 1989 роки при ній працював Окремий комітет експертів з комп'ютерних злочинів. За підсумками його роботи 13 вересня 1989 року Комітетом міністрів Ради Європи видається Резолюція № R (89) 9, у якій уперше використано такий термін, як «злочин, пов'язаний із використанням комп'ютерних технологій». Цей документ містив перелік рекомендованих до обов'яз-

кового включення в національне кримінальне законодавство діянь. Також у ньому наводився перелік тих діянь, щодо яких не досягнуто згоди у визнанні необхідності їх криміналізації в законодавстві всіх держав [2, с. 859].

Очевидно, що рекомендовані заходи лише частково враховують особливості збирання доказів у глобальних комп'ютерних мережах. У зв'язку з цим Рада Європи прийняла низку інших документів, у яких розглядаються ці питання, а саме:

– Рекомендацію № R (87) 15 про регулювання використання персональних даних у поліцейському секторі [3];

– Рекомендацію № R (95) 4 про захист персональних даних у сфері телекомунікаційних послуг, пов'язаних із телефонними переговорами [4];

– Рекомендацію № R (88) 2 про боротьбу з піратством у сфері авторського права й суміжних прав [5];

– Рекомендацію № R (95) 13 щодо проблем кримінально-процесуального права, пов'язаних з інформаційними технологіями [6].

Особливий інтерес становить останній із названих документів, оскільки в ньому вперше рекомендовано таке: «Слідчі органи повинні мати повноваження змушувати осіб, що мають у своєму розпорядженні комп'ютерні дані, надавати всю необхідну інформацію для доступу до комп'ютерів і даних, що там зберігаються. Кримінально-процесуальні органи повинні мати повноваження видавати відповідні ордери особам, що мають знання про те, як функціонують комп'ютерні системи і як забезпечується безпека даних, що зберігаються в них. На операторів громадських і приватних мереж, що надають телекомунікаційні послуги, мають бути накладені зобов'язання забезпечення всіх технічних засобів для перехоплення телекомунікацій слідчими органами».

Проте рекомендаційний характер приписів цих документів не сприяв вирішенню колізій, що виникають на практиці, для цього потрібні повноцінні міжнародно-правові документи.

Зростання комп'ютерної злочинності й необхідність погодженого підходу держав до вироблення кримінально-правових і кримінально-процесуальних приписів, спрямованих на боротьбу з нею, стало спричинило формування Комітетом Міністрів Ради Європи в лютому 1997 року Комітету експертів із злочинності в кіберпросторі, перед яким було поставлено завдання провести доскональне вивчення юридичних проблем, що виникають під час розслідування злочинів, здійснених із використанням комп'ютерних технологій. За результатами їх вивчення розроблено проект Європейської конвенції про кіберзлочинність, варіант якої представлений Радою Європи для публічного обговорення у квітні 2000 року [7].

Після широкого обговорення він був допрацьований з урахуванням вимог посилення гарантій недоторканності приватного життя під час розслідування комп'ютерних злочинів і підготовлений до обговорення виконавчими органами Ради Європи [8]. У період з 18 по 22 червня 2001 року проект обговорений на засіданні Європейського комітету з проблем злочинності, яким унесені деякі зміни і прийнято рішення про винесення проекту Конвенції для прийняття й підписання Комітетом Міністрів Ради Європи [9].

23 листопада 2001 року на конференції в Будапешті була підписана Конвенція Ради Європи про кіберзлочинність [10], яка стала юридичною основою для боротьби з кіберзлочинами із посяганнями на інформаційні системи включно. Особливістю цієї Конвенціє є те, що всі майбутні документи укладалися з огляду на її положення, а деякі з них – із прямим посиланням на Конвенцію. Наприклад, у Директиві ЄС 2013/40 про посягання на інформаційні системи [11]. У її преамбулі наголошено: «Нова стратегія

повинна бути розроблена державами-членами й Комісією, беручи до уваги зміст Конвенції Ради Європи про кіберзлочинність від 2001 року». Отже, ця Конвенція стала фундаментом боротьби з кіберзлочинністю, заклавши основи співробітництва, стандарти криміналізації кіберзлочинів і вимоги до процесуального права не тільки для країн-членів Ради Європи, а й усієї світової спільноти.

Особливістю є те, що Конвенція містить положення з матеріальних питань кримінального права, процесуальні норми й положення про міжнародну співпрацю.

Станом на грудень 2009 року ця конвенція була підписана 46 державами та ратифікована 26 з них, уже станом на грудень 2018 року Конвенцію про кіберзлочинність підписали 62 країни (25 із яких не є членами РЄ, ще 4 підписали, але не ратифікували) [12]. Це свідчить не тільки про якість самого договору, а й про бажання держав долучатися до співробітництва та впроваджувати у своє законодавство норми, які дадуть можливість ефективно здійснювати протидію кіберзлочинами та боротьби з ними.

Щодо структури Конвенції РЄ про кіберзлочинність від 2001 року, то вона складається з преамбули й 4 розділів. Розділ І включає використання термінів (комп'ютерні системи, комп'ютерні дані, постачальник послуг, дані про рух інформації). Варто ще раз наголосити, що відсутнє, власне, визначення кіберзлочину чи кіберзлочинності. Розділ ІІ містить заходи, які повинні вжити держави на національному рівні, що стосуються матеріального права, процесуального права та юрисдикції. Норми процесуального права мають застосовуватися до злочинів, передбачених Конвенцією, будь-якого злочину, що вчинений із використанням комп'ютерних систем, а також до збирання цифрових доказів кримінального правопорушення. Процесуальні норми включають термінове збереження комп'ютерних даних, які зберігаються, порядок представлення, збирання комп'ютерних даних у реальному масштабі часу й питання юрисдикції. Розділ ІІІ, присвячений міжнародному співробітництву, передбачає принципи екстрадиції, загальні принципи міжнародної співпраці, процедури, пов'язані із запитами про взаємну допомогу в разі відсутності відповідних міжнародних угод, питання, пов'язані зі взаємною допомогою щодо тимчасових заходів і щодо повноважень на розслідування, положення про цілодобову мережу. Розділ ІV охоплює прикінцеві положення, більшість із яких є типовими для конвенцій РЄ [10].

Загалом Конвенція виділяє 4 групи суспільно небезпечних діянь:

1. Правопорушення проти конфіденційності, цілісності й доступності комп'ютерних даних і систем: незаконний доступ (ст. 2), нелегальне перехоплення (ст. 3), втручання в дані (ст. 4), втручання в систему (ст. 5), зловживання пристроями (ст. 6).

2. Правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами (ст. 7), шахрайство, пов'язане з комп'ютерами (ст. 8).

3. Правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9), – вироблення, розповсюдження, передача, здобуття дитячої порнографії за допомогою комп'ютерних систем, володіння дитячою порнографією в комп'ютерній системі або на комп'ютерному носії інформації.

4. Правопорушення, пов'язані з порушенням авторських і суміжних прав (ст. 10), коли дії вчинені свідомо, у комерційних розмірах і за допомогою комп'ютерних систем [2].

Також у ст. 12 передбачається можливість несення кримінальної відповідальності юридичною особою за злочин, учинений на її користь.

Як злочинні наслідки перерахованих діянь Конвенцією визнається порушення прав законних користувачів комп'ютерної інформації, комп'ютерів, їх систем або мереж. Установлення як обов'язкової ознаки об'єктивної сторони тяжких наслідків (матеріального збитку, протиправного використання отриманої комп'ютерної інфор-

мації тощо) залишене на розсуд держав. Загалом норми Конвенції не передбачають обов'язковість настання шкідливих наслідків для кожного з указаних діянь.

Виходячи з практики, що складається в різних країнах, ст. 12 Конвенцій вимагає встановлення відповідальності за правопорушення, передбачені нею, не лише для фізичних осіб, а й для юридичних осіб. Умовами настання відповідальності юридичної особи є здійснення дії з метою отримання вигоди на користь юридичної особи її посадовою особою, що займає керівну посаду, з використанням її повноважень за уявленням юридичної особи, ухваленням рішень або здійсненням контролю за її діяльністю. Крім того, Конвенція пропонує встановлювати відповідальність юридичних осіб і у випадках здійснення протиправних дій іншим працівником під керівництвом посадовця, що займає керівний пост, з метою отримання вигоди на користь юридичної особи [10].

Згідно з ч. 1 ст. 13 Конвенції, установлення конкретних санкцій за здійснення вказаних діянь зараховано до відання держав. На їхній розсуд може встановлюватися кримінальна відповідальність для фізичних осіб, а також кримінальна, цивільно-правова або адміністративна відповідальність для юридичних осіб. Передбачені внутрішньодержавним законодавством санкції мають бути ефективні, пропорційні й переконливі [10].

Набір принципів для формування правової основи міжнародної співпраці у сфері розслідування кіберзлочинів міститься, зокрема, в главі III Конвенції Ради Європи про кіберзлочинність. У цій главі говориться про значення, що зростає, міжнародної співпраці (ст. ст. 23–35) і про доцільність використання швидкодіючих засобів зв'язку, включаючи факсимільний зв'язок та електронну пошту (п. 3 ст. 25). Крім того, кожній стороні Конвенції пропонується створити в себе контактний пункт, який повинен щодня й у будь-який час доби реагувати на звернення держав по допомогу (ст. 35). Інші можливі підходи викладені в проекті міжнародної конвенції про посилення захисту від кіберзлочинності й тероризму, а також у підготовленій Міжнародним союзом електрозв'язку (МСЕ) підбірці матеріалів для розроблення законодавства про кіберзлочинність [13].

Що стосується норм цієї Конвенції, які визначають створення інституційного механізму протидії цим різним видам кіберзлочинів, то, наприклад, відповідно до ст. 46 Конвенції, засновано Комітет з кіберзлочинності, метою якого є консультації щодо сприяння імплементації та ефективного застосування Конвенції, забезпечення обміну інформацією та впровадження майбутніх доповнень. У 2017 році Комітетом прийнято рішення розробити проект Другого протоколу до Конвенції про кіберзлочинність, зокрема, для вирішення таких категорій питань: заходи щодо ефективного взаємного співробітництва (спрощення режиму для взаємної правової допомоги щодо запиту інформації, запити про міжнародне співробітництво, безпосереднє співробітництво між судовими органами у взаємній правовій допомозі, об'єднані розслідування й об'єднані розслідувальні групи, запити англійською мовою, аудіо-, відеоконференції із залученням свідків, потерпілих та експертів, заходи швидкого реагування у взаємній правовій допомозі); заходи, що забезпечують безпосереднє співробітництво з провайдерами в інших юрисдикціях задля запитів інформації щодо користувачів, збереження інформації та невідкладних запитів: більш точне формулювання й інтенсивніше забезпечення чинних практик щодо транскордонного доступу до даних; заходи, спрямовані на забезпечення захисту даних [14].

Окрім цього, при Раді Європи в Бухаресті (Румунія) діє Офіс програми з кіберзлочинності (C-PROC), завданням якого є допомога державам посилити їхні юридичні механізми щодо відповіді загрозам кіберзлочинності й функціонування електронних

доказів відповідно до Конвенції з кіберзлочинності. Офіс займається реалізацією низки проектів, диференційованих за регіональною ознакою, щоб більш ефективно виявити потреби правових систем і забезпечувати необхідні консультації [15].

Отже, можна стверджувати, що в межах ЄС, а саме в рамках Ради Європи, проведена значна робота і прийнята низка важливих документів у сфері встановлення кримінальної відповідальності за кіберзлочини. Одним із таких документів є Конвенція про кіберзлочинність 2001 року. Конвенція стала проривом у боротьбі з кіберзлочинністю. Саме вона задала напрям для майбутньої універсалізації відповідних норм. Конвенція застосовує нейтральну щодо технологій юридичну техніку, тому, відповідно, передбачає застосування як щодо сучасних правопорушень, так і щодо таких, які можуть виникнути в майбутньому з розвитком технологій [16].

Однак однією з основних проблем є те, що Конвенція про кіберзлочинність 2001 року не підписана й не ратифікована багатьма державами, і навіть ті з них, які взяли її норми за основу для встановлення відповідальності за комп'ютерні злочини на національному рівні, ще не здійснили криміналізації всіх правопорушень, визначених цим документом. До того ж комп'ютерні технології продовжують розвиватися й удосконалюватися, що найближчим часом може призвести до необхідності встановлення кримінальної відповідальності за нові види правопорушень у цій сфері. Проте є сподівання, що належна реалізація Конвенції з кіберзлочинності 2001 року виправить недоліки боротьби з високотехнологічними злочинами, забезпечивши ефективну координацію дій правоохоронних органів різних держав. Наскільки ефективною виявиться ця координація насправді, а також чи вартує вона тієї ціни, яку доведеться заплатити громадянам, таємниця приватного життя яких завдяки Конвенції знаходиться під загрозою, покаже час.

Список використаних джерел:

1. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. 2008. : http://cybercrimela/v.net/documents/cybercrimejhistory/pdf.

2. Матвієнко А.Р. Стандарти Ради Європи щодо встановлення відповідальності за кіберзлочини. *Верховенство права очима правників-початківців.* 2012. С. 859–861.

3. Recommendation № R (87) 15 of the Committee of Ministers of the Council of Europe to member States for the regulating the use of personal data in the police sector(Adopted by the Committee of Ministers on 17 September 1987 at the 410th meeting of the Ministers' Deputies). Strasbourg, 1987.

4. Recommendation № R (95) 4 of the Committee of Ministers of the Council of Europe to member States for the protection of personal data in the area of telecommunication services, with particular reference to telephone services(Adopted by the Committee of Ministers on 7 February 1995 at the 528th meeting of the Ministers' Deputies). Strasbourg, 1995.

5. Recommendation № R (88) 2 of the Committee of Ministers of the Council of Europe to member States for the piracy in the field of copyright and neighbouring rights. Strasbourg, 1988.

6. Recommendation № R (95) 13 of the Committee of Ministers of the Council of Europe to member States for the concerning problems of criminal procedural law connected with Information Technology (Adopted by the Committee of Ministers on 11 September 1995 at the 543rd meeting of the Ministers' Deputies). Strasbourg, 1995.

7. Draft Convention on Cyber – crime (Draft № 24 REV. 2). – Prepared by the Secretariat Directorate General I (Legal Affairs). – Public version – Declassified, PC-CY(2000) Draft №. 24 Rev. 2. Strasbourg, 19 November 2000. URL: http: // conventions. coe. int/ Treaty/ EN/ Projets/ cyber(draft no 24). htm >.

8. Draft Convention on Cyber – crime and Explanatory memorandum related there to. – Prepared by Committee of Experts on Crime in Cyber – Space (PC – CY) Submitted to European Committee on Crime Problems(CDPC) at its 50th plenary session(18–22 June 2001). – Prepared by the Secretariat Directorate General of Legal Affairs. – Restricted, CDPC (2001) 2 rev. Strasbourg, 25 May 2001. URL: < http: // conventions. coe. int/ Treaty/ EN/ Projets/ cyber(draft). htm >.

9. Draft Convention on Cyber-crime and Explanatory memorandum related thereto: final activity report. – Prepared by Committee of Experts on Crime in Cyber-Space (PC-CY) Submitted to European Committee on Crime Problems (CDPC) at its 50th plenary session (18–22 June 2001). Secretariat Memorandym prepared by the Directorate General of Legal Affairs. Restricted, CDPC (2001) 2 rev 2. Strasbourg, 20 June 2001.

10. Про кіберзлочинність : Конвенція від 23.11.2001 № 994789. URL: https://zakon.rada.gov.ua/laws/show/994_575.

11. Directive 2013/40/EU of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. *EUR-Lex*. 2013. URL: https://eur-lex.europa.eu/legal-content EX TXT/ PDF/[9]uri=CELEX:32013L0040&from=EN.

12. Chart of signatures and ratifications of Treaty 185. Convention on Cybercrime. *Council of Europe.* URL: https://www.coe.int/en/veb/conventions/full-Iist/-''conventions/ treaty/185/signatures?p_auth=j5hEAdZ2.

13. Дванадцятий Конгрес Організації Об'єднаних Націй із запобігання злочинності й кримінального правосуддя. Distr.: General 22 February 2009 Russian. Original: English. Сальвадор, Бразилія, 12–19 квітня 2010 року.

14. Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime. *Cybercrime Convention Committee (T-CY).* 2017. URL: https://rm.coe.int/terms-of-reference-for-the-preparation-of-a-draft-2nd-additional-pro-to/l 68072362b.

15. Cybercrime Programme Office (C-PROC). *Council of Europe*. UEL: https:// wwvv.coe.int/en/web/cybercrime/cybercrime-office-c-proc-.

16. Schjolberg S. The History of Global Harmonization on Cybercrime Legislation – The Road to Geneva. 2008. URL: http://cybercrimelaw.net/documents/cybercrimejiistory.pdf.