DOI: https://doi.org/10.33994/kndise.2022.67.21
УДК 343.141

Наталія Миколаївна Ахтирська
кандидат юридичних наук, доцент,
доцент кафедри кримінального процесу та криміналістики
Навчально-наукового інституту права

ORCID: https://orcid.org/0000-0003-335-7722
E-mail: Akhtyrska.n@gmail.com

Київський національний університет імені Тараса Шевченка
Навчально-науковий інститут права

ОДЕРЖАННЯ ДОКАЗІВ В ЕЛЕКТРОННІЙ ФОРМІ В СВІТЛІ ДРУГОГО ДОДАТКОВОГО ПРОТОКОЛУ ДО КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИНІСТЬ

Стаття присвячена аналізу новел міжнародного співробітництва щодо збору доказів в електронній формі, відповідно до ухваленого Радою Європи Другого додаткового протоколу Конвенції про кіберзлочинність, який забезпечує правову основу для розкриття інформації про реєстрацію доменних імен, для прямого співробітництва з постачальниками послуг для одержання інформації про абонентів, про трафік, співробітництво в надзвичайних ситуаціях, оновлює процедуру відео-конференцій.

Ключові слова: *докази в електронній формі, дані про рух інформації, транскрибування.*

Постановка проблеми. Усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, держави-члени Ради Європи визнали необхідність спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва. Таке рішення було зумовлене необхідністю зупинення дій, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, шляхом встановлення кримінальної відповідальності за таку поведінку, надання повноважень, достатніх для ефективної боротьби з такими кримінальними правопорушеннями шляхом сприяння їхньому виявленню, розслідуванню, як на національному, так і на міжнародному рівнях, і укладення домовленостей щодо швидкого і надійного міжнародного співробітництва.

Аналіз останніх досліджень і публікацій. Докази в електронній формі розглядали В. Волзов, Н. Джонс, Е. Джорж, О. Косаревська, Ф. Меріда, У. Расмусен та інші автори.

Мета дослідження. Внесення пропозицій до кримінального процесуального законодавства України відповідно до нових міжнародних стандартів збору доказів в електронній формі, створення відповідних органів, уповноважених на проведення консультацій та контролю за виконанням запитів на негайне надання інформації у надзвичайних ситуаціях.

Викладення основного матеріалу. Практично будь-який злочин в наші дні швидше за все пов'язаний з електронним пристроєм, який має пам'ять або якусь форму програмування. Навіть якщо такий пристрій не використовувався безпосередньо в контексті злочину, дії особи, що вчинила злочин, цілком ймовірно могли бути зафіксовані або записані на камеру відеоспостереження або за допомогою пристрою глобальної системи позиціонування (GPS), що встановлений на мобільному пристрої або в транспортному засобі. Забезпечення отримання електронних доказів за допомогою цифрової криміналістичної експертизи та слідства стало основним інструментом притягнення злочинців до відповідальності. Поширення Інтернету та його застосування призвело до того, що докази можна знайти не лише на персональних комп'ютерних пристроях, але й на веб-сайтах, у соціальних мережах, електронних листах та месенджерах. Розвиток «хмарних» обчислень (де програми та дані зберігаються віддалено, за межами країни та в невизначених місцях) означає, що обробка потенційних електронних доказів відповідно до перевірених принципів та практики стає важливішою, ніж будь-коли.

Дискусії науковців та практиків щодо термінологічного визначення «електронних доказів» не є предметом даної статті, а тому для цілей дослідження використаємо поняття надане в Посібнику з питань електронних доказів для співробітників правоохоронних органів, прокурорів та суддів, розробленому в 2020 р., згідно з яким електронні докази – це будь-яка інформація, що генерується, зберігається або передається в цифровій формі, яка згодом може знадобитися для підтвердження або спростування факту, оскаржуваного в межах провадження. Попри те, що в різних юрисдикціях норми можуть відрізнятися, загалом під час оцінювання електронних доказів для судового розгляду слід враховувати такі критерії: автентичність, повнота, надійність, переконливість, пропорційність [1, с. 12].

23.11.2001 була прийнята Радою Європи Конвенція про кіберзлочинність, яка мала на меті підвищення ефективності розслідувань кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, а також надання можливості збирання доказів в електронній формі [2]. Для цілей Конвенції були сформульовані визначення окремих понять (комп'ютерна система, комп'ютерні дані, постачальник послуг, дані про рух інформації), а також передбачені заходи, які мають здійснюватися на національному рівні (Розд. II), що стосуються матеріального кримінального права та *процедурного (процесуального) права.* Враховуючи особливості способів вчинення кіберзлочинів з використанням мережі Інтернет та дистанційного запуску шкідливих програм, питанням міжнародного співробітництва присвячений окремий розділ Конвенції (Розд. III), в якому визначено загальні принципи міжнародного співробітництва; принципи екстрадиції; загальні принципи взаємної допомоги; процедури, пов'язані із запитами про

взаємну допомогу у разі відсутності відповідних міжнародних угод. Упродовж двадцяти років цей документ, відомий як «Будапештська конвенція», залишається найбільш актуальною міжнародною угодою, що передбачає інструменти процесуального права для збору електронних доказів та міжнародного співробітництва під час кримінального провадження. Втім еволюція інформаційних та телекомунікаційних технологій відкрила безпрецедентні можливості для людства, водночас створила значні труднощі у галузі кримінального правосуддя, оскільки електронні докази зберігаються все частіше на серверах в іноземних (або в невідомих) юрисдикціях, в мінливих або множинних юрисдикціях, тобто в «хмарному сховищі», а повноваження правоохоронних органів обмежені територіальними кордонами.

На конференції Ради Європи, присвяченій 20-річчю Будапештської конвенції, яка відбулася в листопаді 2021 р. *(автор статті є учасником даного заходу*) було зазначено про необхідність забезпечення виконання конвенційних положень шляхом створення загальної системи моніторингу, розробки *нових юридичних обов'язкових стандартів*, що зумовлені новими викликами. 17.11.2021 Комітет міністрів Ради Європи прийняв Другий додатковий протокол до Конвенції про кіберзлочинність, який скерований на розширення міжнародного співробітництва та розкриття електронних доказів [3]. Протокол скерований на вирішення низки питань, зокрема: 1) як домогтися більш ефективного використання облікового запису або інтернет-протоколу, який використовується для вчинення злочину; 2) як та на яких умовах здійснювати співробітництво з постачальником послуг, який перебуває на території іншої держави, для одержання електронних доказів; 3) як без зволікань домогтися розкриття даних, включаючи дані про зміст, від іншої держави в надзвичайних ситуаціях; 4) як зробити міжнародне співробітництво більш ефективним та чи можна надати правоохоронним органам додаткові інструменти для збору електронних доказів.

Підставами для прийняття Другого додаткового протоколу стали:

1) зростання випадків використання інформаційно-комунікаційних технологій, включаючи Інтернет-послуги, зростання кіберзлочинності, що ставить під загрозу демократію та верховенство права;

2) збільшення кількості потерпілих від кіберзлочинів та важливість забезпечення правосуддя для захисту прав потерпілих;

3) обов'язок держави нести відповідальність за захист суспільства та фізичних осіб не тільки в реальному світі, але й в Інтернеті, у тому числі шляхом ефективного розслідування кіберзлочинів та судового провадження;

4) докази злочину зберігаються в електронній формі в комп'ютерних системах, які перебувають під юрисдикцією іноземних, досить часто декількох держав.

Аналіз Другого додаткового протоколу свідчить про те, що ним створено правову основу для *прямого співробітництва з постачальниками послуг* (ст.ст. 6,7), *прискорених форм співробітництва для розкриття інформації про абонента та дані трафіку* (ст. 8), *прискореного співробітництва та розкриття інформації у надзвичайних ситуаціях* (ст.ст. 9, 10),

передбачені *додаткові інструменти взаємної допомоги* (ст.ст. 11, 12), *захист даних та інші гарантії верховенства права* (ст.ст. 13, 14).

Перш за все, варто зазначити, що метою прийняття Другого додаткового протоколу стало, зокрема, розширення співробітництва щодо боротьби з кіберзлочинністю та збору доказів *у будь-якому кримінальному провадженні в електронній формі* з використанням додаткових інструментів задля сприяння підвищення ефективності взаємної допомоги та інших форм співробітництва між компетентними органами. Дане формулювання значно розширює можливості використання способів співробітництва та інструментів при розслідуванні не тільки конвенційних кіберзлочинів, або злочинів, передбачених Розд. XVI КК України, що зумовлює внесення змін до національного процесуального законодавства у якості загальних норм збору електронних доказів у будь-якому кримінальному провадженні.

По-друге, для цілей Другого додаткового протоколу було ряд понять, зокрема: «надзвичайна ситуація», якою визнається ситуація, що створює значний та неминучий ризик для життя або безпеки будь-якої фізичної особи; «персональні дані» – інформація, що має відношення до ідентифікації особи; «передаюча Сторона» – Сторона, яка передає дані у відповідь на запит або у рамках спільної слідчої групи на території якої знаходиться постачальник послуг щодо передачі даних або організація, що надає послуги з реєстрації доменних імен. З огляду на це варто зазначити, що в ст. 541 КПК України дається роз'яснення термінів «запитуюча сторона» (п. 4 ч. 1) та «запитувана сторона» (п. 5 ч. 1), однак у випадку, зокрема, застосування *принципу надання доказової інформації за власною ініціативою* держава виступає у якості *передаючої сторони*, однак даний термін відсутній в чинному законодавстві України. Отже, з урахуванням вказаного та положень Другого додаткового протоколу доцільно доповнити ст. 541 КПК України терміном «передаюча сторона», під яким слід розуміти державу, що передає дані у відповідь на запит або у рамках спільної слідчої групи на території якої знаходиться постачальник послуг щодо передачі даних або організація, що надає послуги з реєстрації доменних імен, а також державу, яка надає доказову інформацію за власною ініціативою без запиту.

По-третє, одержання доказів у рамках міжнародного співробітництва було ускладнене низкою факторів, окремі з яких усунені прийняттям даного документу. Так, відповідно до Другого додаткового протоколу, не визнається *підставою для відмови у міжнародному співробітництві*: 1) відсутність такого складу правопорушення в законодавстві запитуваної держави; 2) інше термінологічне визначення діяння; 3) віднесення діяння до іншої категорії тяжкості.

По-четверте, Другим додатковим протоколом передбачається процедура, що сприяє розширенню *прямого співробітництва з постачальниками послуг та суб'єктами, що перебувають на території іншої сторони, а також між органами з питань розкриття збережених комп'ютерних даних.* Даний спосіб одержання електронних доказів скерований на оперативне використання даних. Водночас, згідно зі ст. 545 КПК України центральними органами міжнародного співробітництва є Офіс

Генерального прокурора, Національне антикорупційне бюро України та Міністерство юстиції. Згідно зі ст. 35 Конвенції про кіберзлочинність вимагається створення цілодобової мережі (24/7) для надання негайної допомоги для розслідування або переслідування стосовно кримінальних правопорушень, пов'язаних з 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: надання технічних порад; збереження даних відповідно до ст.ст. 29 і 30; збирання доказів, надання юридичної інформації і встановлення місцезнаходження підозрюваних. Однак, незважаючи на це, в Законі України «Про ратифікацію Конвенції про кіберзлочинність» зазначено, що Міністерство внутрішніх справ України є органом, на який покладаються *виключно повноваження щодо створення та функціонування* цілодобової контактної мережі [4], тобто інший орган не визначено у якості центрального для такого міжнародного співробітництва. На виконання доручення Президента України від 03.12.2010 № 02/78475-01 МВС України було створено контактний пункт з реагування на кіберзлочини у структурі Департаменту боротьби з кіберзлочинністю і торгівлею людьми МВС України. На підставі Постанови Кабінету Міністрів України від 13.10.2015 № 831 утворено Департамент кіберполіції як міжрегіональний територіальний орган Національної поліції [5]. Наразі Департамент кіберполіції Національної поліції України здійснює реагування на запити зарубіжних партнерів, які надходять по каналах Національної Цілодобової мережі контактних пунктів. Очевидною є неузгодженість національного законодавства з конвенційними положеннями, оскільки більшість запитів, які надсилаються та надходять каналами національного контактного пункту, стосуються отримання інформації, яка знаходиться в операторів та провайдерів телекомунікацій про зв'язок, абонента, надання телекомунікаційних послуг, у тому числі отримання послуг, їх тривалості, змісту, маршрутів передавання, так як ця інформація здебільшого має суто технічний характер та є первинною інформацією при проведенні перевірки за будь-яким фактом учинення кримінального правопорушення. Проте, відповідно до чинного законодавства, виконання запитів від органів досудового розслідування інших держав не входять до його компетенції [6, с. 154]. Крім цього, на відміну від ряду держав, в Україні згідно зі ст. 121 Закону України «Про електронні комунікації», доступ до інформації про споживача, факти надання електронних комунікаційних послуг, у тому числі до даних, що обробляються з метою передачі такої інформації в електронних комунікаційних мережах, здійснюється виключно на підставі рішення суду, слідчого судді у випадках та порядку, передбачених законом [7]. Рішенням цього питання є внесення доповнення до ст. 545 КПК України щодо визнання повноважень Департамент кіберполіції Національної поліції України щодо виконання запитів у рамках кримінального провадження та внесення змін до Положення про Департамент [8]. Другий додатковий протокол передбачає вищий рівень оперативності та доцільність прискореної процедури шляхом одержання даних безпосередньо від

суб'єкта, який володіє інформацією, або під контролем якого вона перебуває, тобто без опосередкованого звернення до контактного центру, що зумовлює доцільність детального вивчення таких способів одержання електронних доказів перед його ратифікацією.

За міжнародними стандартами, до процедур, що сприяють розширенню прямого співробітництва з постачальниками послуг та суб'єктами, що перебувають на території інших держав, відноситься: 1) *запит на надання інформації, що має відношення до реєстрації доменних імен; 2) розкриття інформації про абонента.* Держави мають прийняти законодавство та інші заходи, які можуть бути необхідними для надання компетентним органам права та повноважень для цілей кримінального провадження направляти запит організації, що надає послуги з реєстрації доменних імен на території іншої держави, щодо надання інформації, що перебуває у володінні або під контролем даної організації, в цілях ідентифікації особи, яка зареєструвала те чи інше доменне ім'я, або встановлення контакту з такою особою. Водночас має бути прийняте законодавство, що дозволяє суб'єктам, що перебувають на території держави, розкривати таку інформацію на запит, що надійшов від компетентних органів іншої держави. Запит включає в себе: дату складання запиту, а також ідентифікаційні та контактні дані компетентного органу, що надіслав запит; доменне ім'я, щодо якого запитується інформація, та детальний перелік запитуваної інформації, включаючи конкретні елементи таких даних; заяву про те, що запит виданий у відповідності з Другим додатковим протоколом, що необхідність одержання інформації виникла у зв'язку з її безпосереднім відношенням до конкретного кримінального провадження, та що дана інформація буде використана виключно для цілей даного кримінального провадження; строк та порядок розкриття інформації, а також будь-які інші процедурні інструкції.

У випадку прийнятності для даної організації, запит може бути надісланий в електронній формі, при цьому має бути забезпечений відповідний рівень безпеки та підтверджена дійсність. У випадку відмови організації від співробітництва запитуюча сторона має право звернутися з проханням вказати причину, з якої не розкривається запитувана інформація. Запитуюча держава також має право на звернення за *консультацією* до держави, на території якої знаходиться організація, що відмовила в розкритті інформації, з тим, щоб встановити, наявність заходів забезпечення одержання запитуваної інформації. Для цього під час ратифікації Другого додаткового протоколу до Конвенції про кіберзлочинність держави мають визначити орган, уповноважений для проведення консультацій.

Щодо розкриття інформації про абонента, то кожна держава приймає законодавство та має вжити інших заходів, які скеровані на забезпечення механізму надання компетентним органам прав та повноважень видавати розпорядження, які направляються безпосередньо постачальнику послуг, що перебуває на території іншої держави, з тим, щоб забезпечити розкриття певних збережених даних про абонента, які перебувають у власності або під контролем даного постачальника послуг, за умови, що така

інформація є необхідною у даному кримінальному провадженні. Також на законодавчому рівні має бути закріплено право постачальника послуг розкривати такі дані про абонента. Розпорядження про надання інформації має бути видано або прокурором, або судом, або іншим компетентним органом під наглядом останніх, або під іншим незалежним наглядом. В розпорядженні на розкриття інформації про абонента вказуються: назва органу, що видав розпорядження, та дата; заява про те, що розпорядження надіслано відповідно до Другого додаткового протоколу; назва та адреса постачальника послуг, якому дане розпорядження необхідно вручити; правопорушення, яке підлягає розслідуванню чи судовому розгляду; назва органу, який потребує одержання таких даних про конкретного абонента; детальний опис даних про конкретного абонента. Таке розпорядження супроводжується додатковою інформацією: описом внутрішніх правових підстав наділення органу правом та повноваженнями звертатися з таким розпорядженням; посиланням на правові норми та вказівкою санкцій за дане кримінальне правопорушення; контактною інформацією органу, якому належить передати дані про абонента, та у якого постачальник послуг може запросити додаткову інформацію; інформацією щодо строків та порядку передачі даних про абонента; інформацією про те, чи застосовувалися раніше заходи для збереження даних, включаючи дату прийняття рішення; будь-якими процедурними інструкціями та інформацією, яка може сприяти забезпеченню розкриття даних. Також може надаватися інформація про певні обставини, факти, пов'язані з розслідуванням чи судовим розглядом. Для організації виконання такого способу одержання даних держава має визначити орган, якому надсилаються такі розпорядження для відома, а також уповноважений для консультацій орган.

У випадку відмови від виконання розпорядження без наведення причин через 30 днів після надсилання розпорядження або строку визначеного в розпорядженні, держава має право вимагати розкриття даних відповідно до ст. 8 «*Виконання розпорядження стосовно надання даних про абонента та технічних параметрів трафіку в прискореному порядку»*. Сутність новел полягає в тому, що держави зобов'язані ухвалити законодавство, яке дозволяло б компетентним органам звертатися із запитом з тим, щоб зобов'язати постачальника послуг, який знаходиться на території запитуваної держави, надати певні збережені дані: 1) дані про абонента; 2) технічні параметри трафіку, які перебувають у власності або під контролем даного постачальника послуг для цілей конкретного кримінального провадження. В запиті вказується: назва органу, що звертається з запитом; заява про те, що розпорядження ґрунтується на Другому додатковому протоколі до Конвенції про кіберзлочинність; найменування та адреса постачальника послуг, якому необхідно вручити розпорядження; опис правопорушення, у зв'язку з яким виникла необхідність одержання інформації; назва компетентного органу, який проводить розслідування (судовий розгляд), якщо це не співпадає з органом, який направляє запит.

Також в якості додаткової інформації може надаватися опис правових підстав для звернення даного органу з запитом; опис правових норм та

санкції за правопорушення, яке є предметом кримінального провадження; підстава, яка дає привід вважати, що даний постачальник послуг володіє відповідними даними або контролює їх тощо. Запит надсилається в електронній формі. З дати одержання запиту запитувана держава докладає розумних зусиль для надання запитуваних даних *не пізніше двадцяти днів* у випадку надання даних про абонента; *не пізніше сорока п'яти днів* у випадку надання технічних параметрів трафіку. У випадку неможливості вчасного виконання запиту, запитувана держава невідкладно повідомляє запитуючу державу та вказує умови виконання. Під час ратифікації Другого додаткового протоколу держави мають визначити орган, який буде уповноважений на реалізацію такого інструменту міжнародного співробітництва (чи то центральний орган міжнародного співробітництва, вказаний при ратифікації Конвенції про кіберзлочинність чи інший).

Передбачається також прискорена процедура розкриття збережених комп'ютерних даних у надзвичайній ситуації (ст. 9). З цією метою держави мають ухвалити законодавство, *у* відповідності з яким у надзвичайних ситуаціях контактні центри в мережі, які працюють 24 години на добу 7 днів на тиждень (відповідно до ст. 35 Конвенції), можуть передавати запит запитуючої держави контактному центру запитуваної держави з проханням про надання невідкладної допомоги в забезпеченні того, щоб постачальник послуг, який знаходиться на території запитуваної держави, розкрив та надав збережені комп'ютерні дані за відсутності запиту про взаємну правову допомогу.

В запиті окрім загальної інформації вказуються факти, які достатньою мірою свідчать про наявність надзвичайної ситуації та яке відношення запитувані дані мають для кримінального провадження; детальний опис запитуваних даних; будь-яка інша інформація, яка може сприяти забезпеченню розкриття даних. Запит приймається в електронній формі. Держави мають право приймати запит навіть *переданий усно* та вимагати підтвердження в електронній формі.

Додаткової регламентації зазнав порядок проведення відео-конференції. Зокрема, запитуюча держава має право запросити, а запитувана держава дозволити одержати показання свідків або експертів в режимі відео-конференції. Під час попередніх консультацій вирішуються питання: яка держава буде головувати (проводити допит); які органи та особи будуть присутні під час проведення допиту; одна чи обидві держави будуть складати присягу, роз'яснювати права та обов'язки експерта; порядок допиту свідка та експерта; порядок належного забезпечення прав свідка та експерта; порядок розгляду заяв про привілеї та імунітет; порядок розгляду заперечень на питання або відповіді; одна чи обидві держави будуть забезпечувати письмовий переклад, усний переклад та транскрибування. Центральні органи міжнародного співробітництва підтримують прямий зв'язок, запитувана держава має право прийняти запит, направлений в електронній формі.

Обов'язок забезпечити участь особи, показання якої або заяви запитуються, покладаються на запитувану державу. Без шкоди для юрисдикції у відповідності до внутрішнього законодавства запитуючої держави, у тих

випадках, коли під час проведення відео-конференції свідок або експерт: 1) дає завідомо неправдиві свідчення, в той час коли у відповідності з нормами внутрішньодержавного законодавства запитуваної держави запитувана держава зобов'язала таку особу давати правдиві показання; 2) відмовляється давати показання, у той час, коли у відповідності з нормами національного законодавства запитуваної держави запитувана держава зобов'язала таку особу давати показання; 3) вчиняє інші неправомірні дії, заборонені нормами запитуваної держави, то на таку особу можуть бути накладені санкції на території запитуваної держави таким же чином, як би такі порушення (діяння) були вчинені у ході її внутрішнього розслідування (кримінального провадження).

За загальним правилом, запитувана держава несе всі витрати, пов'язані з виконанням запиту за виключенням: гонорару експерта, який дає показання; витрат на усний та письмовий переклад, а також *транскрибування;* витрати надзвичайного характеру. Деталізація діяльності щодо перекладу свідчить про підвищення вимог до якості зафіксованої інформації, зокрема, виходячи з вимоги щодо транскрибування (від лат. transcribo – переписую), тобто способу запису усного мовлення з метою найточнішого передавання на письмі усіх відтінків вимови (звуків) з тими змінами, яких звук зазнає у процесі мовлення, за допомогою спеціальних графічних знаків. Цю спеціальну систему письма використовують для точного запису звучання слів тієї чи іншої мови незалежно від її графічних та орфографічних норм, тому до транскрибування вдаються, коли виникає потреба позначити звучання слова, відмінне від його написання [9]. Правила проведення відеоконференції за взаємною згодою держав застосовуються для цілей проведення аудіоконференції, для ідентифікації осіб та об'єктів. Для проведення слідчих дій за участю підозрюваного або обвинуваченого вимагаються додаткові умови та гарантії.

За взаємною згодою компетентні органи двох або більше держав мають право створити спільну слідчу групу та забезпечити її функціонування на їхніх територіях з метою надання сприяння у проведенні кримінальних розслідувань та судового розгляду у тих випадках, коли є достатні підстави вважати, що посилена координація дій має особливе значення. Компетентні органи визначаються зацікавленими державами.

Процедура та умови, що регулюють діяльність спільних слідчих груп, такі як визначення конкретних задач; склад, функції, тривалість, умови та періоди продовження повноважень; місцеперебування; організаційна структура, умови збору, передачі та використання інформації або доказів; умови збереження конфіденційності; умови залучення органів однієї держави до слідчих дій, що проводяться на території іншої держави встановлюються за погодженням компетентних органів. У випадку необхідності проведення слідчих дій на території однієї з зацікавлених держав компетентні органи цієї держави, що входять до складу спільної слідчої групи, проводять такі дії *без запиту* у відповідності з національним законодавством. Одержана інформація або докази можуть бути використані державами за попереднім погодженням: для цілей, які визначені угодою про

створення спільних слідчих груп чи провадження спільного розслідування; для виявлення, розслідування та судового розгляду *інших правопорушень,* які не були предметом даного співробітництва та не передбачені даною угодою про створення спільних слідчих груп; для запобігання надзвичайним ситуаціям. Виключення полягає лише в тому, що одержання згоди не вимагається, якщо основоположні принципи законодавства держави, яка використовує інформацію або докази, передбачає розкриття інформації чи доказів для захисту прав обвинуваченого в кримінальному провадженні. Створення спільних слідчих груп та проведення спільного розслідування може базуватися на підставі угод та за визначених умов для *кожного конкретного випадку.*

У відповідності зі ст. 15 Конвенції про кіберзлочини кожна держава має забезпечити, щоб встановлення, виконання та застосування повноважень та процедур, передбачених Протоколом, здійснювалося у відповідності з умовами та гарантіями, передбаченими внутрішньодержавним законодавством, що забезпечує належний захист прав та свобод людини. В першу чергу це стосується *захисту персональних даних*. Якщо на момент одержання персональних даних держави не уклали угоду, яка б встановлювала рамкову домовленість про захист персональних даних, що передаються задля запобігання, виявлення, розслідування та судового розгляду кримінального провадження, держави можуть здійснювати співробітництво на підставі інших угод або домовленостей. При цьому кожна держава має бути переконаною, що обробка персональних даних відповідає її нормативно-правовій базі щодо захисту персональних даних при міжнародній передачі. Другий додатковий протокол до Конвенції про кіберзлочини не обмежує держави укладати угоди з більш жорсткими умовами щодо конфіденційності та більш суворих гарантій при обробці персональних даних.

В цьому аспекті для України існують певні ризики, пов'язані з прогалинами щодо приєднання до міжнародних угод. Зокрема, 10.10.2018 був відкритий для підписання Протокол про внесення змін до Конвенції про захист фізичних осіб під час автоматичної обробки персональних даних (ETS № 108) [10], метою якого стала модернізація цієї Конвенції (ETS № 108+) [11], з урахуванням нових викликів у сфері захисту фізичних осіб при обробці персональних даних, що виникли після прийняття Конвенції (ETS № 108) у 1980 р. Протокол забезпечує належну та всебічну правову основу для сприяння обміну даними через кордони при ефективних гарантіях використання. Особлива увага приділяється правам осіб в контексті алгоритмічного прийняття рішень, які особливо актуальні у зв'язку з розвитком штучного інтелекту. Однак Україна в числі інших держав (Туреччина, Молдова, Румунія, Азербайджан) не підписала та не ратифікувала модернізовану Конвенцію («108+») (2018 р.), що стане перешкодою до використання електронних доказів у міжнародному співробітництві, оскільки такі держави можуть потрапити до чорного списку.

Щодо конфіденційних даних, то обробка персональних даних, які розкривають расове або етнічне походження, політичні погляди, релігійні чи інші переконання, членство в профспілковій організації, генетичні дані,

біометричні дані, які визнаються конфіденційними з огляду на обумовлення ними фактору ризику, або персональних даних, які стосуються стану здоров'я або сексуального життя здійснюється виключно за наявності відповідних гарантій, що забезпечують захист від ризику необґрунтованого упередженого впливу внаслідок використання таких даних, зокрема від незаконної дискримінації.

Дискусійним є питання строків збереження даних, оскільки не існує єдиних стандартів в країнах ЄС, а тому кожна держава зберігає персональні дані виключно у продовж такого періоду часу, який є необхідним та доцільним з точки зору цілей обробки даних. З метою забезпечення даного зобов'язання в національному законодавстві має бути встановлено конкретні строки збереження таких даних, або має бути визначений порядок періодичного перегляду доцільності подальшого зберігання таких даних. Доцільно в Закон України «Про електронні комунікації» внести доповнення щодо строків зберігання даних.

Важливим є застереження щодо уникнення ризиків при прийнятті так званих автоматизованих рішень. Рішення, які суттєво негативно впливають на відповідні інтереси фізичної особи, не можуть бути засновані виключно на результатах автоматизованої обробки персональних даних.

Прозорість роботи з електронними даними, забезпечується тим, що кожна держава має сповіщати фізичну особу, персональні дані якої були зібрані, та зазначати: правові підстави та цілі обробки даних; строки збереження інформації та перегляду тривалості збереження в залежності від обставин; одержувачів даних яким вони розкриті; наявні засоби забезпечення доступу, виправлення помилок та відшкодування завданої шкоди. Персональне оповіщення особі не здійснюється у випадку, коли запитуюча держава звернулася з проханням зберегти конфіденційність передачі даних (у випадку, коли це матиме негативні наслідки для цілей розслідування, загрожуватиме національній безпеці тощо).

Висновки. Ефективність міжнародного співробітництва під час кримінального провадження щодо збору доказів в електронній формі потребує від України приєднання до «Конвенції 108+»; підписання та ратифікації Другого додаткового протоколу до Конвенції про кіберзлочинність; внесення змін та доповнень до КПК України щодо визначення суб'єктів міжнародного співробітництва під час кримінального провадження; визначення строків зберігання даних в законі щодо електронної комунікації тощо.

Перелік посилань

1. Джордж Е., Меріда Ф; Расмуссен У., Волзов В., Джонс Н. Посібник з питань електронних доказів: базовий посібник для співробітників правоохоронних органів, прокурорів та суддів. Версія 2.1. Відділ протидії кіберзлочинності. Генеральний директорат з прав людини та верховенства права. Страсбург, Франція. 2020. 218 с.

References

1. George, E., Merida, F, Rasmussen, W., Volzov, V., Jones, N. (2020). Handbook on Electronic Evidence: A Basic Handbook for Law Enforcement Officials, Prosecutors, and Judges. Version 2.1. Department for Combating Cybercrime. Directorate-General for Human Rights and the Rule of Law. Strasbourg, France. 218 p. (in Ukrainian).

2. Конвенція про кіберзлочинність від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/ show/994_575#Text (дата звернення 22.02.2022).

3. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. URL: https://rm.coe.int/1680a49dab (дата звернення 24.02.2022).

4. Про ратифікацію Конвенції про кіберзлочинність: Закон України. URL: https://zakon.rada.gov.ua/laws/show/2824-15#Text (дата звернення 24.02.2022).

5. Про утворення територіального органу Національної поліції: постанова Кабінету Міністрів України від 13.10.2015 № 83. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF (дата звернення 24.02.2022).

6. Косаревська О. В. Пріоритетні напрямки діяльності кіберполіції у сфері протидії кіберзлочинності в Україні. URL: http://dspace.oduvs.edu.ua/bitstream/123456789/545/1/ilovepdf_com-153-156%5B1%5D.pdf (дата звернення 24.02.2022).

7. Про електронні комунікації: Закон України від 16.12.2020 № 1089-IX (Із змінами). URL: https://zakon.rada.gov.ua/laws/show/1089-20#n2246

8. Про затвердження Положення про Департамент кіберполіції Національної поліції України: наказ Національної поліції України від 10.11.2015 № 85. URL: http://tranzit.ltd.ua/nakaz/(дата звернення 24.02.2022).

9. Українська бібліотечна енциклопедія. URL: https://ube.nlu.org.ua/article/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%86%D1%96%D1%8F (дата звернення 24.02.2022).

10. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних від 28.01.1981 (ETC 108). URL: https://zakon.rada.gov.ua/laws/show/

2. Cybercrime Convention as of 23 November 2001. Retrieved from: https://zakon.rada.gov.ua/laws /show/994_575#Text. (in Ukrainian).

3. Second Additional Protocol to the Convention on Cybercrime on enhanced cooperation and disclosure of electronic evidence [Strasbourg, 12.V.2022]. Retrieved from: https://rm.coe.int /1680a49dab. (in English).

4. On ratification of the Convention on Cybercrime: Law of Ukraine. Retrieved from: https://zakon.rada.gov.ua/laws/show/2824-15#Text. (in Ukrainian).

5. On the establishment of a territorial body of the National Police: Resolution of the Cabinet of Ministers of Ukraine as of 13.10.2015 No. 83. Retrieved from: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF. (in Ukrainian).

6. Kosarevska, O. V. Priority activities of cyber police in the field of combating cybercrime in Ukraine. Retrieved from: http://dspace.oduvs.edu.ua/bitstream/123456789/545/1/ilovepdf_com-153-156%5B1%5D.pdf. (in Ukrainian).

7. On electronic communications: Law of Ukraine as of 16.12.2020 No. 1089-IX (With changes made in accordance with Law No. 1971-IX as of 16.12.2021). Retrieved from: https://zakon.rada.gov.ua/laws /show/1089-20#n2246. (in Ukrainian).

8. On approval of the Regulation on the Cyber Police Department of the National Police of Ukraine: Order of the National Police of Ukraine dated 10.11.2015. No. 85. Retrieved from: http://tranzit.ltd.ua/nakaz/. (in Ukrainian).

9. Ukrainian Library Encyclopedia. Retrieved from: https://ube.nlu.org.ua/article/%D0%A2%D1%80%D0%B0%D0%BD%D1%81%D0%BA%D1%80%D0%B8%D0%BF%D1%86%D1%96%D1%8F. (in Ukrainian).

10. Convention for the Protection of Individuals regarding Automatic Processing of Personal Data as of 28 January 1981 (ETC 108). Retrieved from:

994_326#Text (дата звернення 24.02.2022).

11. Convention 108+: Convention for the protection of individuals with regard to the processing of personal data. Council of Europe, June 2018. URL: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1 (дата звернення 24.02.2022).

https://zakon.rada.gov.ua/laws/show/994_326#Text (in Ukrainian).

11. Convention 108 +: Convention for the protection of individuals with regard to the processing of personal data. Council of Europe, June 2018. Retrieved from: https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1. (in English).

OBTAINING OF EVIDENCE IN ELECTRONIC FORM UNDER THE SECOND ADDITIONAL PROTOCOL TO THE CONVENTION ON CYBERCRIME

N. Akhtyrska

The article is devoted to the analysis of international cooperation in the collection of evidence in electronic form, in accordance with the Second Additional Protocol to the Cybercrime Convention approved by the Council of Europe, which provides a legal basis for disclosure of domain name registration traffic, cooperation in emergencies, updates the video conferencing procedure.

The analysis of the Second Additional Protocol shows that it created a legal basis for direct cooperation with service providers, accelerated forms of cooperation for disclosure of subscriber information and traffic data, accelerated cooperation and disclosure of information in emergency situations, additional instruments of mutual assistance, data protection and other guarantees of the rule of law.

Taking into account the above and the provisions of the Second Additional Protocol, it is advisable to supplement Art. 541 of the CPC of Ukraine, the term “transferring party”, should be understood as the state that transmits data in response to a request or within a joint investigation team in which the data service provider or organization providing domain name registration services, as well as a state that provides evidence on its own initiative without request. The purpose of the Second Additional Protocol was, inter alia, to increase cooperation in the fight against cybercrime and the collection of evidence in any criminal proceedings electronically using additional tools to facilitate mutual assistance and other forms of cooperation between competent authorities. According to the Second Additional Protocol, the following shall not be recognized as grounds for refusal of international cooperation: 1) the absence of such an offense in the legislation of the requested State; 2) another terminological definition of the act; 3) assignment of the act to another category of severity.

Key words: evidence in electronic form, data on the movement of information, transcription.