УГОЛОВНЫЙ ПРОЦЕСС, КРИМИНАЛИСТИКА

УДК 343.14

СТРАТЕГІЯ КІБЕРБЕЗПЕКИ ТА ЇЇ РЕАЛІЗАЦІЯ В КРИМІНАЛЬНОМУ СУДОЧИНСТВІ УКРАЇНИ

Наталія АХТИРСЬКА,
кандидат юридичних наук, доцент,
доцент кафедри правосуддя юридичного факультету
Київського національного університету імені Тараса Шевченка

SUMMARY

The article analyzes the legislation of Ukraine on combating cybercrime,which is being reformed in accordance with European standards. It considers positions of scientists on the improvement of procedural legislation for the purpose of collecting electronic evidence, as well as the need to maintain a balance between human rights and state security. Based on the analysis of judicial practice demonstrated complex practice of assessment evidence in this category of crimes. The author proves the expediency of adopting a special law on the fight against cybercrime with standard specifics of international cooperation in this field, and at the international level UN Convention or Protocol to the Convention against transnational crime.

Key words: cybercrime, information security, hacking, electronic evidence, international cooperation during criminal proceedings.

АНОТАЦІЯ

У статті аналізується чинне законодавство України щодо боротьби з кіберзлочинністю, яке реформується відповідно до європейських стандартів. Висвітлено позиції науковців щодо вдосконалення процесуального законодавства з метою збору електронних доказів, а також необхідності дотриманням балансу між правами людини та безпекою держави. На підставі аналізу судової практики продемонстрована неодностайна практика оцінювання доказів у даній категорії проваджень. Автор доводить доцільність прийняття спеціального закону про боротьбу з кіберзлочинністю з унормуванням специфіки міжнародного співробітництва в цій сфері, а на міжнародному рівні – спеціальної Конвенції ООН або Протоколу до Конвенції проти транснаціональної злочинності.

Ключові слова: кіберзлочинність, інформаційна безпека, хакерські атаки, електронні докази, міжнародне співробітництво під час кримінального провадження.

Постановка проблеми. Інтернет-ресурси переважно аналізуються з точки зору впливу на інтелектуальне збагачення людства, накопичення знань та передачі їх новому поколінню. Однак переваги сучасного цифрового світу та розвиток інформаційних технологій зумовили виникнення нових загроз національній та міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість та потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб. Сучасні виклики та недостатність контролю за кіберпростором призводить до Інтернет-шахрайства, залякування та переслідування, вербування до вчинення злочинних дій. За перше десятиліття XXI століття кількість користувачів Інтернету зросла від 350 млн. до понад 2 млрд., що зумовило прийняття державами відповідних стратегій кібербезпеки, якими визначені напрями вдосконалення чинного національного законодавства та вектори міжнародного співробітництва.

Метою статті є висвітлення сучасних тенденцій у законодавстві України щодо виконання міжнародних зобов'язань у боротьбі з кіберзлочинністю та виявлення прогалин, що ускладнюють розслідування злочинів та судовий розгляд.

Виклад основного матеріалу. Угодою про асоціацію України з Європейським Союзом Сторони домовилися співробітничати в боротьбі з кримінальною та незаконною організованою чи іншою діяльністю, а також з метою її попередження. Таке співробітництво, зокрема, спрямовується на вирішення проблем боротьби з кіберзлочинністю (п.f) ч. 2 ст. 22) [1].

На національному рівні розроблена достатня правова база для розкриття, розслідування та притягнення до відповідальності осіб, винних у вчиненні даної категорії кримінальних правопорушень: Закони України «Про інформацію», «Про телекомунікації», «Про доступ до публічної інформації» та ін. Кримінальний кодекс України містить Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Кваліфікуючою ознакою шахрайства в ст. 190 КК України визначено вчинення шляхом незаконних операцій із використанням електронно-обчислювальної техніки, а ст. 200 КК України передбачає відповідальність за незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення.

Однак сучасні виклики та загрози зумовили потребу переосмислення значення інформаційного простору, встановлення певного контролю за ним із боку держави з метою забезпечення безпеки.

У Стратегії національної безпеки України, затвердженій Указом Президента України 26 травня 2015 р., особливе значення приділено загрозам кібербезпеці і безпеці інформаційних ресурсів, серед яких названо уразливість об'єктів критичної інфраструктури, державних інформаційних ресурсів до кібератак; фізична і моральна застарілість системи охорони державної таємниці та інших видів інформації з обмеженим доступом. Зазначене створює актуальні загрози національній безпеці України,

в тому числі безпеці критичної інфраструктури: критична зношеність основних фондів об'єктів інфраструктури України та недостатній рівень їх фізичного захисту; недостатній рівень захищеності критичної інфраструктури від терористичних посягань і диверсій; неефективне управління безпекою критичної інфраструктури і систем життєзабезпечення.

Пріоритетами забезпечення інформаційної безпеки визначено: забезпечення наступальності заходів політики інформаційної безпеки на основі асиметричних дій проти всіх форм і проявів інформаційної агресії; створення інтегрованої системи оцінки інформаційних загроз та оперативного реагування на них; протидія інформаційним операціям проти України, маніпуляціям суспільною свідомістю і поширенню спотвореної інформації, захист національних цінностей та зміцнення єдності українського суспільства; розробка і реалізація скоординованої інформаційної політики органів державної влади; виявлення суб'єктів українського інформаційного простору, що створені та/або використовуються Росією для ведення інформаційної війни проти України, та унеможливлення їхньої підривної діяльності; створення і розвиток інститутів, що відповідають за інформаційно-психологічну безпеку, з урахуванням практики держав-членів НАТО; вдосконалення професійної підготовки у сфері інформаційної безпеки, впровадження загальнонаціональних освітніх програм із медіакультури із залученням громадянського суспільства та бізнесу [2].

Пріоритетами забезпечення кібербезпеки і безпеки інформаційних ресурсів є: розвиток інформаційної інфраструктури держави; створення системи забезпечення кібербезпеки, розвиток мережі реагування на комп'ютерні надзвичайні події (CERT); моніторинг кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізація; розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів; забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, відмова від програмного забезпечення, зокрема антивірусного, розробленого в Російській Федерації; реформування системи охорони державної таємниці та іншої інформації з обмеженим доступом, захист державних інформаційних ресурсів, систем електронного врядування, технічного і криптографічного захисту інформації з урахуванням практики держав-членів НАТО та ЄС; створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони; розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікація співпраці України та НАТО, зокрема, в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки.

Із метою виконання міжнародних зобов'язань Указом Президента України від 15 березня 2016 р. затверджена Стратегія кібербезпеки України, якою передбачається, що забезпечення кібербезпеки України як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися на принципах: верховенства права і поваги до прав та свобод людини і громадянина; забезпечення національних інтересів України; відкритості, доступності, стабільності та захищеності кіберпростору; державно-приватного партнерства, широкої співпраці з громадянським суспільством у сфері забезпечення кібербезпеки та кіберзахисту; пропорційності та адекватності заходів кіберзахисту реальним та потенційним ризикам; пріоритетності запобіжних заходів; невідворотності покарання за вчинення кіберзлочинів; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях.

Серед напрямів реалізації Стратегії виокремлюються підвищення спроможності суб'єктів боротьби з кібертероризмом щодо протидії кібератакам на державні електронні інформаційні ресурси, об'єкти критичної інфраструктури, а також розвідувально-підривної діяльності іноземних спецслужб, організацій, груп та осіб проти України в кіберпросторі; розмежування кримінальної відповідальності за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, вчинені щодо державних та інших інформаційних ресурсів, щодо об'єктів критичної інформаційної інфраструктури та інших об'єктів, а також відповідне розмежування підслідності.

Боротьба з кіберзлочинністю передбачає: створення ефективного і зручного контакт-центру для повідомлень про випадки кіберзлочинів та шахрайства в кіберпросторі, підвищення оперативності реагування на кіберзлочини правоохоронних органів, зокрема їх регіональних підрозділів; удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, вдосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; запровадження блокування операторами та провайдерами телекомунікацій визначеного (ідентифікованого) інформаційного ресурсу (інформаційного сервісу) за рішенням суду; унормування порядку внесення обов'язкових до виконання операторами та провайдерами телекомунікацій приписів про термінове фіксування та подальше зберігання комп'ютерних даних, збереження даних про трафік; урегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю; підготовку суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в електронній формі, з урахуванням особливостей кіберзлочинів; запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів [3].

Про результативність застосування чинного законодавства свідчать дані судової статистики.

Так, у 2014 році за статтями 361-363-1 КК України (злочини у сфері використання електронно-обчислювальних машин (комп'ютерів) систем та комп'ютерних мереж) було засуджено 37 осіб, з яких 35 громадян України, 2 іноземці, 1 жінка, 8 осіб вчинили злочини в складі групи. У 2015 році засуджено 31 особу, з яких 30 – громадяни України, 1 іноземець, 4 жінки, 6 осіб вчинили злочин у складі групи. За перше півріччя 2016 року засуджено відповідно 14 осіб, 13 з яких – громадяни України, 1 іноземець, 1 жінка, 5 осіб вчинили злочин у складі групи [4]. Очевидно, що наведені дані не відображають рівень кіберзлочинності, а це, у свою чергу, потребує з'ясування причин такого стану.

Так, у результаті хакерської атаки був заблокований сайт Міністерства фінансів України, заблокована офіційна інтернет-сторінка Державного казначейства. Під час спроби зайти на сторінку відомства відбувалась переадресація на ресурс хакерів, де містилось повідомлення: «Привіт. Це знову ми. Битва почалась, але війна далеко не закінчена. Ви не можете перестати бути маріонетками, навіть якщо

не бачите ниток». На думку експерта з кібербезпеки В.Якушева, в Україні відбуваються позитивні зміни в бік зменшення кіберуразливості, однак, попри це, державні органи захищені на 3,5-4 бали з 10 можливих [5]. Причинами такого стану є те, що необхідний обсяг заходів для максимального захисту інформації в Україні не проводиться. Відсутній незалежний аудит компаній та відомств, не проводяться тести на можливість проникнення в ресурси державних органів, включаючи веб-ресурси, внутрішні ресурси, бази даних тощо. Програмно-апаратним захистом частково займаються постачальники комп'ютерного обладнання, що відбувається нерегулярно та на недостатньому рівні. Зі схожими проблемами стикаються й інші країни. Так, у листопаді 2016 р. 900 тисяч клієнтів німецької компанії Deutsche Telecom залишились без підключення до Інтернету після атак на мережу хакерів, які намагались за допомогою шкідливого програмного забезпечення Mirai заразити комп'ютери користувачів, щоб у майбутньому використовувати їх для більш масштабних атак [6]. У Німеччині розглядається питання про створення спеціального відділу для боротьби з хакерами, фахівці якого будуть мати повноваження та технічні можливості у випадку здійснення атаки на атомну станцію чи систему водопостачання знешкодити технічне обладнання хакерів та вивести з ладу їхні сервери за кордоном.

Відслідковування інформації в режимі он-лайн розглядається як засіб забезпечення безпеки за умови дотримання прав людини (конфіденційності) уповноваженими на те органами на підставі закону та під контролем суду. Так, у Великобританії з 30 листопада 2016 року Палата лордів затвердила законопроект, що передбачає можливість контролю за телефонними розмовами, sms-повідомленнями, електронною поштою, а також створення архіву сайтів, що відвідуються користувачем, та збереження вказаної інформації упродовж року. Вказаний контент та маршрутизація визнаються належними електронними доказами в кримінальному провадженні, що одержані в законний спосіб. Цей закон визнають більш жорстким, ніж закон про кібербезпеку КНР.

Встановлення відповідних «фільтрів» для виявлення злочинної діяльності, на кшталт «тероризм», не звільнятиме правоохоронні органи та суд від клопіткої діяльності щодо оцінки та тлумачення електронної інформації. Так, користувач Twitter у Великобританії був затриманий за використання на власній сторінці нового слова, яке правоохоронцями було розтлумачене як заклик до замаху на життя британського парламентаря, яка була заступником міністра в справах бізнесу, інновацій та кваліфікованих кадрів. Затриманий у соціальних мережах згадав ім'я іншого депутата Джо Кокс, яка виступала проти виходу Британії з Євросоюзу та була вбита в 2015 р. Підозрюваний закликав «заджококсити члена парламенту» Субрі (в англійській мові поширено використання в якості жартів неологізмів у вигляді переводу слів з однієї частини мови в іншу) [7].

Чинний Кримінальний процесуальний кодекс України не містить визначення електронних доказів та особливостей їх збирання та оцінювання, що не сприяє одностайній слідчій та судовій практиці. Прикладом того є випадок, коли слідчий у клопотанні, поданому слідчому судді, зазначив, що з кримінального провадження провадяться слідчі дії, у зв'язку із чим виникла необхідність в отриманні доступу до документів, які перебувають в адміністрації соціальної мережі: «www.facebook.com», розташованому за адресою: FacebookInc. 10 BrockStreet, NW1 3FG London, UnitedKindom 1601 WillowRoadMenloPark, CA 94025 UnitedStates. Слідчий суддя розглянув дане клопотання у відсутність особи, у володінні якої знаходяться речі і документи на підставі ч. 2 ст. 163 КПК України. Відповідно до ч. 5 ст. 163 КПК України слідчий суддя, суд постановляє ухвалу про надання тимчасового доступу до речей і документів, якщо сторона кримінального провадження у своєму клопотанні доведе наявність достатніх підстав вважати, що ці речі або документи: перебувають або можуть перебувати у володінні відповідної фізичної або юридичної особи; самі по собі або в сукупності з іншими речами і документами кримінального провадження, у зв'язку з яким подається клопотання, мають суттєве значення для встановлення важливих обставин у кримінальному провадженні; не становлять собою або не включають речей і документів, які містять охоронювану законом таємницю. Слідчий суддя, заслухавши пояснення слідчого, дійшов висновку про наявність підстав для задоволення клопотання, оскільки вказана інформація та документи мають суттєве значення для встановлення важливих обставин у кримінальному провадженні, а іншими способами неможливо довести обставини, які передбачається довести за допомогою цих документів. Суд прийняв рішення надати начальнику відділу прокуратури Києва право тимчасового доступу до документів, а саме даних щодо акаунтів http://www.facebook.com/, якими користувався підозрюваний, які перебувають в адміністрації соціальної мережі «www.facebook.com», та зобов'язати адміністрацію соціальної мережі «www.facebook.com», розташованої за адресою FacebookInc. 10 BrockStreet, NW1 3FG London, UnitedKindom 1601 WillowRoadMenloPark, CA 94025 UnitedStates, виготовити та надати в електронному вигляді документи, що містять дані щодо акаунтів, якими користувалися підозрювані.

В ухвалі слідчого судді було вказано: «Службовим особам адміністрації соціальної мережі «www.facebook.com» надати (забезпечити) тимчасовий доступ до речей і документів, особам, які здійснюють досудове розслідування в кримінальному провадженні, та/або оперативним підрозділам органів внутрішніх справ, які здійснюють слідчі (розшукові) дії в кримінальному провадженні за письмовим дорученням слідчого, прокурора, та надати їм можливість вилучити зазначені в ухвалі копії документів. У разі невиконання ухвали про тимчасовий доступ до речей і документів слідчий суддя, суд за клопотанням сторони кримінального провадження, якій надано право на доступ до речей і документів на підставі ухвали, має право постановити ухвалу про дозвіл на проведення обшуку згідно з положеннями Кримінального процесуального Кодексу з метою відшукання та вилучення зазначених речей і документів». Указане рішення є теоретично правильним, однак складність виконання його є очевидною. Перш за все, США надають таку інформацію лише у випадку, коли вона стосується не громадян США. Якщо в запиті є загроза порушення прав громадянина США, уповноважений на те орган здійснює перевірку та відкриває провадження на території своєї держави. Варто зазначити, що умовою відкриття кримінального провадження є завдання шкоди в розмірі більше 200 тисяч доларів США, тероризм, вбивство та ін.

Зняття інформації з транспортних телекомунікаційних мереж полягає в негласному проведенні із застосуванням відповідних технічних засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні і фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду).

Під час кримінального провадження допускається можливість зняття інформації з транспортних телекомунікаційних мереж, яке поділяється на:

1) контроль за телефонними розмовами, що полягає в негласному проведенні із застосуванням відповідних

технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, спостереження, відбору та фіксації змісту телефонних розмов, іншої інформації та сигналів (SMS, MMS, факсимільний зв'язок, модемний зв'язок тощо), які передаються телефонним каналом зв'язку, що контролюється;

2) зняття інформації з каналів зв'язку, що полягає в негласному одержанні, перетворенні і фіксації із застосуванням технічних засобів, у тому числі встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передаються каналами зв'язку мережі Інтернет, інших мереж передачі даних, що контролюються.

Зняття інформації з електронних інформаційних систем без відома їх власника, володільця або утримувача (ст. 264 КПК України) полягає в одержані інформації, в тому числі із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютер), автоматичних системах, комп'ютерній мережі.

Незалежно від тяжкості злочину проводиться: 1) зняття інформації або її частини з електронних інформаційних систем, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов'язаний із подоланням системи логічного захисту (ч. 2 ст. 264 КПК України). Полягає в одержанні інформації з електронних інформаційних систем, що містять відповідну інформацію, в тому числі із застосуванням технічного обладнання; 2) встановлення місцезнаходження радіоелектронного засобу (ст. 268 КПК України) полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, в тому числі мобільного терміналу, систем зв'язку та інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття змісту повідомлень, що передаються, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження.

Актуальні питання доказів у кримінальних провадженнях щодо кіберзлочинів досліджували М.В. Салтевський , О.Г. Волевод, Б.В. Андреєв, П.Н. Пак, В.П.Хорст , В.О. Голубєв, Т.А. Сайтарли та інші. Разом із тим слід вказати, що у вітчизняній науці кримінального процесу та криміналістики недостатньо приділено уваги розробці концепції кібердоказів, незважаючи на те, що слідча та судова практика вкрай потребує не тільки правового визначення, тлумачення, але й науково-методичного забезпечення кримінального провадження в даній категорії злочинів, а особливо у сфері міжнародного співробітництва. Відповідно до ст. 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому законом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд встановлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню (ч. 1). Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів (ч. 2). У ст. 99 КПК України дається визначення, згідно з яким документом є спеціально створений із метою збереження інформації матеріальний об'єкт, який містить зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, що можуть бути використані як доказ факту чи обставин, які встановлюються під час кримінального провадження (ч. 1). Зокрема, до документів можуть належати: 1) матеріали фотозйомки, звукозапису, відеозапису та інші носії інформації (в тому числі електронні); 2) матеріали, отримані внаслідок здійснення під час кримінального провадження заходів, передбачених чинними міжнародними договорами, згоду на обов'язковість яких надано Верховною Радою України (ч. 2). Наведене свідчить, що законодавець допускає використання електронних носіїв інформації, проте уточнює, що доказ має бути матеріальним об'єктом. Цифрові технології використовують віртуальний простір, а тому носієм (фіксатором) інформації може бути беззаперечно матеріальний об'єкт, однак при цьому варто уточнити, що навіть сама інформація у віртуальному просторі також має визнаватися доказовою.

Одержання електронних доказів із ресурсів, які знаходяться під юрисдикцією інших держав, є можливим за допомогою двох способів: із відкритих джерел (реєстрів) та на запити уповноважених органів. На практиці виникають проблеми в оцінці інформації, що міститься у відкритих джерелах: чи потрібно її одержання дублювати надсиланням запитів, чи потрібно її легалізувати, в який спосіб її фіксувати. Так, за повідомленням викривача, особа, яка займає відповідальне становище та має обмеження щодо занять іншими видами діяльності, на території іншої країни Європейського Союзу очолює раду директорів корпорації, є бенефіціаром, одержує значні прибутки. Порушуючи встановлені вимоги щодо фінансової прозорості, в поданій декларації особа не вказала суми доходів від забороненого виду діяльності.

Уповноважені на те органи, використавши відкриті джерела – електронний Реєстр юридичних осіб указаної країни Євросоюзу – встановили факт, викладений у повідомленні. Вважається, що інформація, одержана з офіційного джерела, має визнаватися доказом, а тому не потребує дублювання в письмовому вигляді. Надсилання запиту, зволікання з відповіддю може спричинити перешкоди в проведенні розслідування та доведенні вини підозрюваного.

Складнощі для ефективної боротьби з вказаними злочинами зумовлюються також тим, що Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року застосовується лише до окремої групи злочинів, та не завжди її положення можуть бути застосовані під час розслідування та судового розгляду злочинів, пов'язаних із кібербезпекою. Так, до Єдиного реєстру досудових розслідувань внесена інформація про відкриття кримінального провадження за ознаками шахрайства. Потерпілим через Yahoo надходили листи від незнайомців, на які ті відповідали, не вбачаючи загрози. Через деякий час із рахунків потерпілих зникали кошти. Прокуратурою було об'єднані численні випадки в одне провадження. Для одержання інформації дописувачів прокурор звернувся із запитом до директорату Yahoo в Каліфорнії (США). Директорат відмовив у наданні інформації, посилаючись на те, що повноваження національного прокурора не мають поширюватися на юридичних осіб інших держав. Для забезпечення належної оперативної співпраці під час кримінального провадження між країнами необхідно прийняти Конвенцію ООН проти кіберзлочинності або Протокол до неї, де визначити порядок такої співпраці, обов'язки провайдерів тощо.

Висновки. Згідно з положеннями Додаткового протоколу до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, необхідно забезпечувати повне та ефективне дотримання всіх прав людини без будь-якої дискримінації або розділення, як це гарантується європейськими та іншими міжнародними документами [8].

Суди також повинні мати на увазі, що до конфіденційної віднесено, зокрема, інформацію про національність особи, її освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адресу проживання, дату і місце народження (частина друга статті 11 Закону України «Про інформацію») [9; 10]. Незважаючи на це, в Єдиному реєстрі

судових рішень непоодинокими є випадки оприлюднення судових рішень із порушенням даного обмеження (єврей, чеченець тощо). Дані факти можуть бути визнані порушенням конвенційних прав осіб та обмежень, встановлених Додатковим протоколом.

Як свідчить судова практика, актуальними в даній сфері є такі питання:

1) процесуальні питання одержання та використання електронних доказів із відкритих ресурсів та ресурсів з обмеженим доступом;

3) правові підстави для тимчасового доступу до електронних документів (ресурсів), які перебувають під юрисдикцією інших держав;

4) використання спеціальних знань у кримінальних провадженнях (відсутність єдиної європейської стандартизації методик проведення судових експертиз, що призводить до неоднозначного тлумачення можливості використання висновків іноземних експертів та висновків національних експертних установ під час судового розгляду транснаціональних кримінальних правопорушень);

5) відсутність спеціального розділу в Кримінальному процесуальному кодексі України щодо особливостей використання електронних доказів, про що свідчать рекомендації Ради Європи;

6) зволікання з прийняттям спеціального Закону України «Про боротьбу з кіберзлочинністю», який був підданий експертній оцінці фахівців ЄС.

В Україні запроваджена єдина національна система електронної дистанційної ідентифікації фізичних і юридичних осіб BankID, яка встановлює порядок функціонування Єдиної національної системи електронної дистанційної ідентифікації фізичних і юридичних осіб BankID, здійснення банками України електронної дистанційної ідентифікації клієнтів (користувачів) із метою отримання ними адміністративних послуг на Єдиному державному порталі адміністративних послуг або від суб'єктів надання адміністративних послуг та доступу користувачів до інформаційно-телекомунікаційних систем державних органів. Отже, сфера цифрових технологій розширюється, що створює нові можливості для одержання доказової інформації та вимагає належного правового унормування.

На думку Сноудена, країни світу все сильніше обмежують права своїх громадян. Він стверджує, що цей період є переломним в історії людства. Усталені межі того, що люди пов'язують з особистим простором, здвигаються [11]. Однак це зумовлено транснаціональною загрозою тероризму, тому баланс безпеки і дотримання прав людини є предметом наукових дискусій та правових компромісів.

Список використаної літератури:

1. Угода про асоціацію між Україною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони, від 27.06.2014 р. // Офіційний вісник України від 26.09.2014р., № 75, том 1, стор. 83, стаття 2125/.

2. Стратегія національної безпеки України, затверджена Указом Президента України, від 26 травня 2015 року № 287/2015 // Офіційний вісник Президента України від 03.06.2015 р. – № 13. – С. 50.

3. Стратегія кібербезпеки, затверджена Указом Президента України, від 15 березня 2016 року № 96/2016 // Офіційний вісник Президента України від 05.04.2016 р. № 10. – С. 39.

4. Звітність судів першої інстанції щодо здійснення судочинства [Електронний ресурс]. – Режим доступу : court.gov.ua.

5. Эксперт по кибербезопасности: по 10-балльной шкале Украина защищена максимум на 3,5-4 балла [Електронний ресурс]. – Режим доступу : http://gordonua.com/news/society/ekspert-po-kiberbezopasnosti-po-10-ballnoy-shkale-ukraina-zashchishchena-maksimum-na-35-4-balla-162607.html.

6. МВД Германии намерено создать специальный отдел для борьбы с хакерами [Електронний ресурс]. – Режим доступу : http://gordonua.com/news/worldnews/mvd-germanii-namereno-sozdat-specialnyy-otdel-dlya-borby-s-hakerami-162198.html.

7. В Великобритании мужчину арестовали за провокационное сообщение в Twittere [Електронний ресурс]. – Режим доступу : https://news.rambler.ru/world/35478982/?utm_content=news&ut.

8. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, від 28.01.2003р. [Електронний ресурс]. – Режим доступу : http://zakon2.rada.gov.ua/laws/show/994_687.

9. Закон України «Про інформацію» від 02.10.1992 № 2657-XII [Електронний ресурс]. – Режим доступу : http://zakon4.rada.gov.ua/laws/show/2657-12.

10. Постанова Пленуму Вищого адміністративного суду України від 29.09.2016р. № 10 «Про практику застосування адміністративними судами законодавства про доступ до публічної інформації» [Електронний ресурс]. – Режим доступу : http://zakon3.rada.gov.ua/laws/show/v0010760-16.

11. Сноуден: в Британии закон о слежке будет жёстче, чем в Китае [Електронний ресурс]. – Режим доступу : // http://pronedra.ru/internet/2016/11/18/slezhka-britaniya/.