CHAPTER «LAW SCIENCES»

THE STATUS OF IMPLEMENTATION OF THE CYBER CRIME CONVENTION IN EASTERN EUROPE

СТАН ВПРОВАДЖЕННЯ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ У КРАЇНАХ СХІДНОЇ ЄВРОПИ

Andrii Zakharko[1]
Oleksii Boiko[2]

DOI: https://doi.org/10.30525/978-9934-26-190-9-7

Abstract. The monograph analyzes the status of reform of criminal procedure legislation of Ukraine and other Eastern European countries to implement the procedural provisions of the International Convention on Cybercrime in order to determine the procedural powers of pre-trial investigation authorities to collect electronic evidence. The relevance of the research topic is substantiated by statistical data on the rapid growth of the number of criminal offenses, the method of committing which is inextricably linked with the use of computers and computer data processing. The monograph consists a systematic analysis of the procedural powers of pre-trial investigation bodies which are provided for in the Convention on Cybercrime and aimed at increasing the effectiveness of pre-trial investigation bodies in documenting criminal activity, taking into account the specific form of factual data that need to be collected as evidence in these investigations. It is stated that the need to supplement the procedural powers of pre-trial investigation bodies in the investigation of computer crimes is determined by such factors as: technological ability to change, distort, modify and destroy electronic data quickly after using them in computer crimes; technological possibility of placing such electronic data

[1] PhD in Law, Associate Professor,
Associate Professor of the Criminal Procedural Law Department,
Dnipropetrovsk State University of Internal Affairs, Ukraine
[2] PhD in Law, Associate Professor of the Criminal Procedural Law Department,
Dnipropetrovsk State University of Internal Affairs, Ukraine

outside the territorial jurisdictions of individual states and outside the location of continents, etc. It has been established that in order to ensure the effectiveness of pre-trial investigations into computer crimes, the powers of the prosecution need to be supplemented by the following procedural possibilities, provided for in the Cybercrime Convention: the possibility for the competent authority to issue an order for the urgent retention of certain computer data, including data on the movement of information stored by the computer system, in particular when there are grounds to believe that such computer data is particularly vulnerable to loss or modification; the obligation of the person who controls the relevant computer data to kept and maintain the integrity of such computer data for a certain period of time which is necessary to obtain permission from the competent authority to disclose such data; the obligation of the person who must keep such computer data on the order of the competent authority, to maintain the confidentiality of the fact of such procedures for a certain period; ensuring the possibility of urgent storage of data on the movement of information, regardless of the number of service providers involved in the transmission of such information; ensuring the possibility of urgent disclosure of information on the movement of information, to the competent authority. Such amount of information is sufficient to identify service providers and the route of the information`s transmission; search and seizure of computer data, etc. A systematic analysis of the criminal procedure legislation of Eastern European countries has shown that Ukraine's neighbors have also not fully signed and ratified the procedural provisions of the Convention on Cybercrime. Only Hungary, Romania and the Republic of Bulgaria have secured the most effective powers of the analyzed states. In particular, the criminal procedure law of these states provides for such powers of the prosecution as: issuing a warrant for the urgent preservation of certain e-data; the person's responsibility to maintain the integrity of stored e-data; seizure of data, computer system, part or medium; copying and saving a copy of such e-data; preserving the integrity of stored e-data; extracting e-data from a computer system, etc.

1. Вступ

1 липня 2004 року набрала чинності Міжнародна конвенція про кіберзлочинність (далі – Конвенція), відкрита для підписання в Будапешті 23 листопада 2001 року [1]. Головна мета Конвенції полягає в

проведенні спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, особливо шляхом прийняття відповідного законодавства та сприяння міжнародному співробітництву. 7 вересня 2005 року Конвенція була ратифікована відповідним Законом України [2] та вступила в законну силу на території України з 1 липня 2006 року [3]. Згідно ст. 14 зазначеної Конвенції, кожна Сторона вживає необхідних законодавчих та інших заходів з метою конкретних кримінальних розслідувань або переслідувань, зокрема, до визначених Конвенцією кримінальних правопорушень, інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем, та збору доказів у електронній формі стосовно кримінального правопорушення. Імплементація і застосування повноважень і процедур мають регулюватися умовами і запобіжними заходами, передбаченими внутрішньодержавним правом Сторони, які б забезпечували адекватний захист прав і свобод людини. Такі умови і запобіжні заходи мають включати відповідні повноваження, судовий або інший незалежний нагляд, підстави, які виправдовують застосування, обмеження терміну таких повноважень тощо.

Аналізуючи актуальність боротьби з кіберзлочинністю в Україні, доцільно звернути увагу на наступні статистичні дані. Протягом 2018 року, в порівнянні з даними 2014 року, кримінальних правопорушень, передбачених у ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» КК України збільшилося більш, ніж втричі. А саме, слідчими підрозділами органів Національної поліції у січні-грудні 2018 року обліковано – 1007 таких злочинів, вручено повідомлення про підозру – 630, направлено до суду обвинувальних актів – 477. За ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» КК України кількість зареєстрованих кримінальних правопорушень збільшилося більш, ніж у тринадцять (!) разів. А саме, слідчими підрозділами органів Національної поліції у січні-грудні 2018 року обліковано – 134 таких злочинів, вручено повідомлення про підозру – 81, направлено до суду обвинувальних актів – 79. За ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах

(комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї» КК України збільшилося більш, ніж у чотирнадцять (!) разів. А саме, слідчими підрозділами органів Національної поліції у січні-грудні 2018 року обліковано – 1042 таких злочинів, вручено повідомлення про підозру – 948, направлено до суду обвинувальних актів – 729 [4; 5]. Протягом січня-грудня 2020 року динаміка поширення в Україні кримінальних правопорушень, передбачених у ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» КК України, продовжує стабільно зростати: обліковано – 1146 (у порівнянні з 2018 роком +139) таких кримінальних правопорушень, вручено повідомлення про підозру 680 (у порівнянні з 2018 роком +50), направлено до суду обвинувальних актів 618 (у порівнянні з 2018 роком +141) [6]. Отже, актуальність оптимізації повноважень органів досудового розслідування в сфері кіберзлочинності є такою, що вимагає ретельної парламентської уваги з метою стримати зріст кримінальних правопорушень цих категорій. Ефективна боротьба з кіберзлочинністю передбачає активну міжнародну співпрацю в цьому напрямку.

Проблематика підвищення ефективності боротьби з кіберзлочинами стоїть не лише перед українськими правоохоронними органами. Наприклад, під час проведення міжнародної конференції у Нікосії (Республіка Кіпр) за тематикою: «Кіберзлочинність: тенденції і загрози», що відбулася 11-12 червня 2018 року, начальник поліції Кіпра З. Хризостому зазначив, що діяльність кіберзлочинців коштує світовій економіці в 600 мільярдів доларів на рік, а згідно статистичних даних, жертвами кіберзлочинів щорічно становляться два із трьох інтернет-користувачів [7]. THE DEVELOPMENT OF THE IDEA OF the необхідності підсилення ресурсу правоохоронних можливостей для успішного розслідування комп'ютерних злочинів набрала актуальності світового масштабу, що підтверджується систематичним проведенням таких заходів, як: онлайн-семінари та практичні заняття в рамках Спільного проекту Європейського Союзу та Ради Європи CyberEast [8], CyberSouth [9], iPROCEEDS-2 тощо.

Метою монографії є дослідження кримінального процесуального законодавства держав східної Європи для з'ясування, чи достатньо

уваги приділяється імплементації необхідних процедурних положень Конвенції про кіберзлочинність у національні кримінальні процесуальні закони зазначених держав.

В країнах східної Європи набуття законної сили цією Конвенцією характеризується наступним чином. Російська Федерація досі не підписала Конвенцію; Республіка Білорусь – у списку підписань та ратифікації на парламентському сайті України відомості відсутні; Республіка Молдова – підписала 21 листопада 2001 року й досі не ратифікувала; Румунія – Конвенція вступила в законну силу 1 вересня 2004 року; Болгарія –вступила в законну силу 1 серпня 2005 року; Угорщина – вступила в законну силу 1 липня 2004 року; Чеська Республіка – підписала Конвенцію 9 лютого 2005 року й досі не ратифікувала; Словаччина – підписала Конвенцію 4 лютого 2005 року й досі не ратифікувала; Польща – підписала Конвенцію 23 листопада 2001 року й досі не ратифікувала; Естонія – Конвенція вступила в законну силу 1 липня 2004 року; Латвія – підписала Конвенцію 5 травня 2004 року й досі не ратифікувала її; Литва – Конвенція вступила в законну силу 1 липня 2004 року. Таким чином, серед країн східної Європи протягом 2004 – 2006 років Конвенція про кіберзлочинність набрала законної сили в Естонії, Литві, Україні, Угорщині, Румунії і Болгарії.

2. Дослідження кримінального процесуального законодавства держав східної Європи щодо запровадження положень Конвенції про кіберзлочинність

Дослідження проблематики підвищення ефективності досудових розслідувань кримінальних правопорушень у сфері кіберзлочинності уявляється правильним розпочати з аналізу стану імплементації в українське кримінальне процесуальне законодавство положень, викладених у згаданій вище Конвенції про кіберзлочинність.

Тож проаналізуємо сьогоднішній стан імплементації процедурних положень Конвенції в кримінальне процесуальне законодавства України та інших зазначених вище держав.

Для ефективного збирання доказів у електронній формі ст.ст. 16, 17 Конвенції передбачається:

1) можливість компетентного органу видати ордер на термінове збереження визначених комп'ютерних даних, включаючи дані про

рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації;

2) обов'язок особи, під контролем якої знаходяться відповідні комп'ютерні дані, зберігати і підтримувати цілісність таких комп'ютерних даних протягом певного періоду, необхідного для отримання в компетентного органу дозволу на розкриття таких даних;

3) обов'язок особи, яка має зберігати такі комп'ютерні дані за ордером компетентного органу, зберігати конфіденційність факту проведення таких процедур протягом певного періоду;

4) забезпечення можливості термінового збереження даних про рух інформації, незалежно від кількості постачальників послуг, які залучалися до передачі такої інформації;

5) забезпечення можливості термінового розкриття компетентному органові обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і маршруту, яким була передана інформація.

Згідно з Конвенцією, передбачається можливість адресувати вимогу про збереження й надання відповідних комп'ютерних даних як особам, у володінні чи під контролем яких зберігаються такі комп'ютерні дані, так і постачальникам послуг – про надання інформації стосовно відповідного користувача послуг.

Згідно ст. 19 «Обшук і арешт комп'ютерних даних, які зберігаються» Конвенції, кожна Сторона має забезпечити своїм компетентним органам повноваження для обшуку або подібного доступу до: комп'ютерної системи або її частини і комп'ютерних даних, які зберігаються в ній; та комп'ютерного носія інформації, на якому можуть зберігатися комп'ютерні дані на її території. Крім того, кожна Сторона має забезпечити необхідні заходи для того, щоб у випадку, коли її компетентні органи здійснюють обшук або подібний доступ до конкретної комп'ютерної системи або її частини, і мають підстави вважати, що дані, які розшукуються, зберігаються у іншій комп'ютерній системі чи її частині, яка знаходиться на її території, і до таких даних можна здійснити законний доступ з першої системи чи вони є доступними першій системі, такі компетентні органи мали право терміново поширити обшук або подібний доступ на іншу систему. Тобто, на комп'ютерну систему чи її частину, яка фізично розташована за межами об'єкта, де

проводиться обшук, але в межах території держави, на яку поширюються правоохоронні повноваження органу досудового розслідування, прокурора, яким проводиться обшук.

Кожна Сторона має забезпечити своїм компетентним органам повноваження арештовувати або вчиняти подібні дії щодо комп'ютерних даних, до яких був здійснений попередній доступ. Такі повноваження включають в себе: арешт або подібні дії щодо комп'ютерної системи або її частини або комп'ютерного носія інформації; копіювання і збереження копії таких комп'ютерних даних; збереження цілісності відповідних збережених комп'ютерних даних; заборону доступу або вилучення цих комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ. Для проведення вищезазначених дій у компетентних органів мають бути повноваження вимагати від будь-якої особи, яка знає про функціонування комп'ютерної системи або про заходи, які були здійснені для захисту комп'ютерних даних, які містяться у ній, надавати, наскільки це можливо, необхідну інформацію. На жаль, в КПК України досі не внесено достатніх і конкретних положень, які б надавали слідчому, прокурору повноваження (не слід плутати схожі з переліченими положеннями про збирання комп'ютерних даних у реальному масштабі часу, перелічені в заголовку 5 Конвенції, які дійсно імплементовані в КПК України, але до глави 21 «Негласні слідчі (розшукові) дії». В цій доповіді здійснено спробу відшукати необхідні специфічні процесуальні засоби збирання доказів стороною обвинувачення у контексті гласних слідчих (розшукових) дій та заходів забезпечення кримінального провадження), що кореспондували б вище переліченим зобов'язанням України за Конвенцією. Погоджуємося з позицією Ю. Ю. Орлова, С. С. Чернявського про доцільність внесення відповідних змін до КПК України [10].

Піддаючи критичному аналізу чинний КПК України, уявляється доцільним не погодитися з позицією, викладеною С. А. Буяджи з приводу того, що аналіз ст. 84 КПК України, якою встановлено поняття доказів у кримінальному процесі «засвідчив, що у ній відсутнє положення, яке б розширювало сутність даного явища за допомогою доказів у електронній формі» [11, с. 103]. Здійснюючи системний аналіз даного питання слід враховувати, що в ч. 2 ст. 84 КПК України визначені процесуальні джерела доказів, серед яких перелічено документи.

А в ст. 99 КПК України зазначається, що до документів можуть належати інші носії інформації, в тому числі електронні [12]. Уявляється, законодавець допустив плутанину: носій інформації, наприклад, флеш-карту пам'яті навряд чи правильно було б називати документом. Втім, електронні документи, як в контексті означеної ст. 99 КПК України, так і з урахуванням ст. 8 ЗУ «Про електронні документи та електронний документообіг» [13], на мою думку, все ж таки є видом документів і слід вважати, що охоплюються терміном «документи» в зазначеній вище ст. 84 КПК України. Адже згідно ст. 8 ЗУ «Про електронні документи та електронний документообіг» допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму [13].

Буяджи С. А. зазначає, що відповідно до закону Сполучених Штатів Америки «Про об'єднання та зміцнення США» будь-яка дія, що спричиняє порушення в роботі чи призводить до незаконного проникнення в комп'ютер, класифікується як тероризм. В свою чергу провайдер зобов'язаний надати всю відому йому інформацію про користувача на першу вимогу Федерального бюро розслідувань [11, с. 151].

Аналізуючи законодавство Франції, С. А. Буяджи звертає увагу на обов'язкову реєстрацію власників сайтів у Франції та про кримінальну відповідальність провайдерів за надання хостингу не ідентифікованим користувачам, обов'язок провайдерів надавати відомості про авторів сайтів будь-яким третім особам, за порушення якого передбачається кримінальна відповідальність. При чому, за усі сайти, авторство яких не встановлено, відповідальність несе провайдер, а можливою мірою покарання є позбавлення волі строком на пів року [11, с. 166]. Згідно з законом Франції про внутрішню безпеку 2003 року дозволяється проводити обшуки в інформаційній мережі, якщо інформаційні системи розташовані на території Франції, і, крім того, шляхом укладення міжнародних угод, у Франції передбачено можливість надання дозволу проводити віддалений обшук інформаційних ресурсів, без одержання попереднього дозволу країни, де розміщено сервер [11, с. 168].

В КПК України також нічого не сказано про порядок виконання тимчасових заходів у контексті міжнародного співробітництва:

– термінового збереження комп'ютерних даних, які зберігаються за допомогою комп'ютерної системи, яка знаходиться на території іншої

держави і відносно якої ініціатор має намір надіслати запит про взаємну допомогу щодо обшуку чи подібного доступу (ст. 29 Конвенції);

– термінового розкриття збережених даних про рух інформації у обсязі, достатньому для ідентифікації постачальника послуг і шляху передачі такої інформації (ст. 30 Конвенції);

– транскордонного доступу до публічно доступних комп'ютерних даних, які зберігаються, незважаючи на те, де такі дані знаходяться географічно, а також даних за законною і добровільною згодою особи, яка має законні повноваження розкривати такі дані за допомогою такої комп'ютерної системи (ст. 32 Конвенції) тощо.

Аналогічна ситуація склалася, наприклад, в кримінальному процесуальному законі Естонської Республіки. На актуальності цієї проблеми та способах її вирішення наголошувалося А.-М. Осулою в дисертації за темою: «Дистанційний пошук та вилучення екстериторіальних даних» [14]. Авторкою, зокрема, наголошується про доцільність використання альтернативних заходів доступу до екстериторіально розташованих даних із дозволом прямого доступу до таких даних або IP-адреси без попереднього дозволу іншої держави. Втім, констатується необхідність подальшого забезпечення допустимості отриманих доказів за допомогою подальших законних підстав або згоди, що мають випливати з міжнародного договору. В іншому випадку ситуацію можна розглядати як порушення територіального суверенітету [14, с. 64; 15]. Загалом, проблема юридичного обслуговування транскордонності розміщення й передачі електронних даних має світовий масштаб і, вірогідно, не вирішена у зручний повною мірою для правоохоронних органів спосіб у жодній з держав світу. Д. Шурсон, враховуючи очевидне переважання американських постачальників послуг у секторах хмарних розрахунків та інтернет комунікацій, аргументовано звертає увагу на необхідність вивчення відповідного законодавства в державі реєстрації постачальників послуг (на прикладі США це, передусім, Закон про хмарні технології – Розділ II Закону про конфіденційність електронних комунікацій) та наявність відповідних Двосторонніх угод між державою постачальника послуг і державою правоохоронних органів – замовника відомостей про електронні комунікації [16]. Дослідженню окремих процедурних повноважень органів досудового розслідування щодо закріплення електронних доказів і

подальшого їх використання в судових стадіях кримінального процесу присвятили свої праці D. Skrtic [17], Lopez-Barajas Perea, Inmaculada [18], K. Klevtsov [19] та інші вчені.

Згідно ч. 2 ст. 1 КПК України, міжнародні договори, згода на обов'язковість яких надана Верховною Радою України, є частиною кримінального процесуального законодавства України. Більше того, згідно з ч. 4 ст. 9 КПК України, у разі якщо норми КПК України суперечать міжнародному договору згода на обов'язковість якого надана Верховною Радою України, застосовуються положення відповідного міжнародного договору України.

Але задекларовані Україною зобов'язання створити вище перелічені можливості компетентним органам не можна ототожнювати з конкретними повноваженнями органів досудового розслідування, прокурора. Тому наразі органи досудового розслідування не можуть застосовувати вище перелічені положення Конвенції, бо немає кореспондуючих їм відповідних повноважень.

Аналіз порядку денного десятої сесії Верховної Ради України восьмого скликання [20] показав, що питання посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю в Україні не залишаються поза увагою законодавця. В зазначеному порядку денному, зокрема, наявні проекти Закону про внесення змін до деяких законів України: № 2133а від 19 червня 2015 року [21], № 2133а-1 від 30 вересня 2016 року [22]. Окремої уваги заслуговує проект Закону про внесення змін до деяких законодавчих актів України № 6688 від 12 липня 2017 року [23]. В зазначеному порядку денному є й інші проекти Законів, спрямовані на посилення захисту інформаційних та інформаційно-телекомунікаційних систем, але з урахуванням відсутності в них спрямованості на імплементацію процедурних положень Конвенції про кіберзлочинність, залишимо ці інші законопроекти поза увагою.

На підставі вищевикладеного аналізу чинного КПК України, інших законів та законопроектів, що наразі знаходяться на порядку денному в Верховній Раді України, маємо підстави узагальнити, що парламентом на сьогодні не створено належних умов для ефективної роботи компетентних органів України в контексті більшості з передбачених Конвенцією операцій із комп'ютерними даними та адміністраторами web-ресурсів.

Звернемося до компаративістичного аналізу кримінального процесуального законодавства держав східної Європи та підписантів Конвенції (EXAMPLES OF DOMESTIC CRIMINAL PROCEDURAL LAW), у яких остання, як і в Україні, вже вступила в силу.

У ст. 126-4 КПК Естонської Республіки (далі – ЕР) передбачене проведення оперативно-розшукових заходів з можливістю таємного проникнення до комп'ютерної системи з дозволу судді попереднього слідства [24]. Серед оперативно-розшукових заходів, передбачених у главі 3-1 КПК ЕР є таємне прослуховування та перегляд інформації, що передається мережами електронного зв'язку загального користування (ст. 126-7 КПК). Термін «комп'ютерні дані» в КПК ЕР не використовується. Випадків регламентації у КПК ЕР інших процесуальних дій пізнавального характеру, що безпосередньо передбачали б роботу з електронними даними, комп'ютерними системами, мережею Інтернет для здобуття доказів у результаті проведеного нами аналізу не знайдено.

У ст. 154 КПК Литовської Республіки передбачається контроль, запис та зберігання інформації, переданої мережами електронного зв'язку [25]. Втім зазначені засоби доказування мають характер негласних слідчих (розшукових) дій. В контексті ж імплементації положень Конвенції про кіберзлочинність щодо гласних засобів доказування при роботі з електронними даними, нами не віднайдено в КПК Литовської Республіки таких процесуальних повноважень сторони обвинувачення.

У ст. 158/А Закону XIX Венгрії про кримінальне судочинство передбачається надсилання запиту резервувати дані, що зберігаються в системі обробки інформації. Такий запит тягне за собою тимчасове обмеження права розпоряджатися електронними комп'ютерними даними в інтересах розслідування злочинів. Це може здійснюватися за запитом суду чи сторони обвинувачення, зокрема, з метою з'ясування місцезнаходження підозрюваного чи його ідентифікації. За таким запитом зобов'язана сторона має резервувати дані, що зберігаються в системі обробки інформації, визначені в запиті в незмінюваній формі, гарантувати їх безпечне зберігання, у випадку необхідності окремо від інших файлів з даними. Ця сторона має запобігати модифікації, видаленню, руйнуванню комп'ютерних даних, їх передаванню та неправомірному копіюванню, неправомірному доступу до цих даних. Сторона,

за запитом якої резервуються дані, може прикріпити електронний підпис безпеки до даних, які треба зберігати. Якщо резервування даних у місці первинного розташування значно перешкоджатиме діяльності зобов'язаної сторони, щоб обробляти, керувати, зберігати або передавати ці дані, зобов'язана сторона може з дозволу запитувача цих даних гарантувати резервування через копіювання даних в інше середовище даних або інформаційну систему. Після того, як копія була зроблена, запитувач даних може повністю або частково скасувати обмеження стосовно середовища даних та інформаційної системи в якій спершу розміщувалися відповідні дані. Протягом терміну чинності запиту на зберігання зазначених даних, ці дані можуть бути доступні винятково суду та стороні обвинувачення (чи іншому уповноваженому ініціатору цього запиту), а управляти цими даними можна лише з їх відповідного дозволу. Інші суб'єкти можуть отримувати доступ до цих даних виключно з дозволу ініціатора запиту щодо цих даних. Зобов'язана сторона повинна негайно повідомляти ініціатора запиту про випадки виявлення ознак спроби зміни, видалення, копіювання, передання чи перегляду збережених даних без відповідного дозволу. Після видання запиту стосовно резервування даних, ініціатор запиту має без затримки переглянути ці дані і, залежно від результатів перегляду, ініціювати конфіскацію цих даних через їх копіювання в систему обробки інформації або інше середовище даних, або ж скасувати їх подальше резервування. Тривалість обов'язку резервування даних не може перевищувати трьох місяців, а також закінчується в зв'язку із завершенням судового розгляду з урахуванням дотримання винесених судом рішень [26]. У ст. 158/B Закону XIX Венгрії про кримінальне судочинство з метою попередження чи зупинення злочину передбачається можливість за розпорядженням суду зробити електронні дані тимчасово недоступними. Це може бути зроблено через тимчасове видалення електронних даних, або ж через тимчасове припинення доступу до електронних даних. Особа, яка виконує відповідну постанову суду, має повідомити користувачів про юридичні підстави видалення відповідних даних або припинення до них доступу з посиланням на відповідне судове рішення. Розпорядження на тимчасове обмеження доступу до електронних даних та їх резервування можуть віддаватися одночасно. У ст. 158/C Закону XIX Венгрії про кримінальне судочинство перед-

бачено повноваження суду надати постачальнику відповідних послуг розпорядження про тимчасове унеможливлення доступу до визначених електронних даних. В такому разі провайдер послуг протягом одного робочого дня зобов'язаний виконати відповідну постанову суду. Однією з підстав судового розпорядження про унеможливлення доступу до визначених електронних даних, згідно ст. 158/D аналізованого Закону, є факт попереднього не виконання протягом 30 днів іноземним постачальником послуг відповідного звернення. Постачальники електронних комунікацій зобов'язані унеможливлювати доступ до визначених електронних даних за розпорядженням суду. Відповідні розпорядження суду можуть надсилатися електронною поштою навіть у разі, коли не встановлено особу розпорядника електронних даних. Суд також негайно надсилає електронне повідомлення Національним засобам інформації та Інформаційно-комунікаційним органам щодо виданих ним розпоряджень унеможливлення доступу до визначених електронних даних. Зазначені органи контролюють виконання відповідного розпорядження, реєструють ці розпорядження в центральній базі даних судових рішень та негайно повідомляють постачальників електронних комунікацій стосовно зазначених рішень суду. Постачальник електронних комунікацій має один робочий день на виконання відповідного судового рішення. У випадку відмови постачальника електронних комунікацій виконувати зазначені судові розпорядження, Національні засоби інформації та Інформаційно-комунікаційні органи (NMIA) негайно повідомляють суди про такі факти для вжиття заходів реагування у вигляді штрафів [26].

У КПК Румунії процесуальній регламентації правил роботи з електронними даними та комп'ютерними системами й мережами приділено також значну увагу. Доступ до комп'ютерної системи передбачається, як один із спеціальних методів спостереження або розслідування в ст. 138 КПК Румунії. Цією статтею передбачається прослуховування, доступ, моніторинг, збір або запис комунікацій через телефон, комп'ютерну систему або будь-який інший пристрій зв'язку. Згідно з ч. 3 ст. 138 КПК Румунії, доступ до комп'ютерної системи означає проникнення в комп'ютер або інший пристрій зберігання даних, безпосередньо або на відстані, через спеціалізовані програми або через мережу з метою ідентифікації доказів [27]. До ознак комп'ютерної

системи в ч. 4 ст. 138 КПК Румунії відносять функціональну пов'язаність пристроїв та забезпечення автоматичної обробки даних за допомогою комп'ютерних програм. Комп'ютерні дані визначаються в ч. 5 ст. 138 КПК Румунії так само, як і в Конвенції про кіберзлочинність: будь-яке представлення фактів, інформації чи концепцій у формі, придатній для обробки комп'ютерною системою, включаючи програму, здатну активувати виконання певних функцій комп'ютерною системою. До повноважень прокурора, передбачених у ст. 141 КПК Румунії, зокрема, належить: виготовлення та збереження копії комп'ютерних даних, ідентифікованих за допомогою доступу до комп'ютерної системи, заборона доступу до таких комп'ютерних даних або їх видалення з комп'ютерної системи [27]. Копії виготовляються за допомогою технічних пристроїв та процедур, що забезпечують технічну цілісність вилучених комп'ютерних даних. Правила здійснення електронного нагляду, відібрання копій з носіїв комп'ютерних даних тощо регламентовані в ст. 143 КПК Румунії. Окремий розділ V у КПК Румунії присвячений регламентації правил збереження комп'ютерних даних. У ст. 154 КПК Румунії, зокрема, передбачено повноваження прокурора наказати негайно зберегти комп'ютерні дані на строк до 60 днів, включаючи дані, що стосуються інформаційного трафіку, які зберігались за допомогою комп'ютерної системи, що знаходиться у власності або під контролем постачальника публічних електронних мереж зв'язку або постачальника електронних послуг зв'язку, у разі наявності ризику втрати чи зміни цих даних. Крім того, провайдер зобов'язаний надати органам кримінального переслідування відомості для ідентифікації всіх елементів використовуваного ланцюгу спілкування, в разі його наявності. У ст. 156 КПК Румунії, зокрема, передбачено можливість проводити обшук в комп'ютері. Регламентації обшуку комп'ютерної системи присвячена окрема ст. 168 КПК Румунії. В ній визначено процедуру розслідування, виявлення, ідентифікації та здору доказів, що зберігаються в комп'ютерній системі або в комп'ютерному сховищі даних, що виконується за допомогою адекватних технічних пристроїв та процедур із забезпеченням цілісності отримуваної інформації. В ч. 8 ст. 168 КПК Румунії передбачено право прокурора в разі виявлення під час обшуку комп'ютерної системи факту, що шукані комп'ютерні дані зберігаються в іншій комп'ютерній системі або на

комп'ютерному носії даних і є доступними із початкової комп'ютерної системи на негайне замовлення збереження та копіювання ідентифікованих комп'ютерних даних і повинен вимагати в суду видачі відповідного ордера в екстреному порядку. Крім того, в ст. 170 КПК Румунії передбачено право органу досудового розслідування та суду вимагати від будь-якої особи, в тому числі постачальника послуги електронного зв'язку, передати їм конкретні комп'ютерні дані, якщо це необхідно для відвернення правопорушення або коли ці дані можуть використовуватися як доказ в суді [27]. Таким чином, можемо констатувати результативність імплементації процедурних положень Конвенції про кіберзлочинність до КПК Румунії.

В ст. 159 КПК Республіки Болгарія передбачається, зокрема, що за запитом суду або органів досудового розслідування будь-які установи, юридичні чи посадові особи, громадяни мають зберігати та видавати комп'ютерні інформаційні дані, відомості про рух цих даних, відомості стосовно користувачів, що знаходяться в їх розпорядженні та мають значення для розслідуваного випадку. «Відомості про рух» таких даних розкрито в КПК як всі дані, пов'язані з проходженням крізь комп'ютерну систему повідомлень, сигналів, відомості про їх виникнення, призначення, рух, тривалість, розмір даних, з'єднання з провайдером [28]. У ст. 160 КПК Республіки Болгарія зазначено: за наявності достатніх підстав вважати, що в комп'ютерних системах обробки інформації містяться важливі для розслідуваного випадку комп'ютерні інформаційні дані, то має бути проведено їх пошук, встановлення й відбір. В ч. 7 ст. 163 КПК Республіки Болгарія передбачається конфіскація комп'ютерних інформаційних даних. В ч. 3 ст. 172 КПК Республіки Болгарія передбачається обов'язок провайдерів комп'ютерних даних у разі необхідності виявлення злочинів надавати допомогу суду й досудовим органам у збиранні та реєстрації комп'ютерних інформаційних даних із застосуванням спеціальних технічних засобів [28]. У рішенні ЄСПЛ «Ілля Стефанов проти Болгарії» від 22 травня 2008 року констатується, зокрема, порушення ст. 8 ЄКПЛ у зв'язку з тим, що обшук офісу адвоката був пов'язаний із вилученням цілого ряду речей та документів: комп'ютер, монітор, принтер, інші периферійні пристрої, тридцять три дискети, аркуш паперу з п'ятьма реєстраційними номерами автомобілів, довідка з мовної школи про

проходження заявником курсів англійської та німецької мов (п. 16). Такий перелік вилученого під час обшуку майна був зумовлений надто широкими формулюваннями, вжитими в ордері на проведення обшуку. Зокрема, комп'ютер заявника (адвоката) та всі його гнучкі диски були вилучені на два місяці й тому становили надмірне втручання поліції у професійну таємницю заявника. Лише через тиждень після проведення обшуку й вилучення комп'ютера й гнучких дисків, ці речі були передані експерту для здійснення відбору файлів за критерієм ключових слів. Ще через 10 днів експерт повідомив поліцейському, що застосуванням спеціальної комп'ютерної програми не виявлено на досліджуваних носіях інформації релевантних за відомими ключовими словами файлів [29]. Таким чином, можна припустити, що в разі якщо б слідчі провели під час обшуку офісу адвоката такі процесуальні дії, як обшук комп'ютера та відбір комп'ютерних даних, то ЄСПЛ би не констатував в цій справі надмірного втручання поліції у професійну таємницю заявника, та, мабуть, не було б і самого позову до ЄСПЛ.

Аналіз кримінального процесуального закону держав, у яких Конвенція про кіберзлочинність досі залишається не ратифікованою, надав підстави для таких висновків: у чинній редакції Кримінально-процесуальних кодексів Російської Федерації [30], Республіки Білорусь [31], Чеської Республіки [32], Республіки Польща [33], Латвійської Республіки [34] юридична конструкція «комп'ютерні дані» досі взагалі не використовується.

Можливо, саме недостатньо детальна кримінальна процесуальна регламентованість дій слідчого сприяла винесенню рішення ЄСПЛ «Юдицька та інші проти Росії» від 12 лютого 2015 року ЄСПЛ. У цьому рішенні ЄСПЛ, зокрема, зазначив: постанова суду про проведення обшуку не була чітко сформульованою, що надало слідчим необмежену свободу розсуду при проведенні обшуку. Відповідно до прецедентної практики Суду постанови про проведення обшуку мають бути складені за можливості так, щоб спричинені ними наслідки були передбачуваними. Надмірна розпливчатість формулювань постанови призвела до того, як було здійснено обшук: слідчі вилучили усі настільні та портативні комп'ютери заявників та скопіювали вміст усіх жорстких дисків. Зазначені комп'ютери були повернуті через тиждень. Зокрема, що стосується електронних даних, які зберігалися на

комп'ютерах заявників, що були вилучені слідчим, то очевидно, під час обшуку не дотримувалися жодних процедур фільтрації. Суд дійшов висновку, що обшук торкнувся професійної таємниці тією мірою, яка є неспівмірною переслідуваній законній меті [35]. Іншими словами, дії слідчих вийшли за межі «необхідних у демократичному суспільстві».

Продовжуючи аналізувати кримінальне процесуальне законодавство держав, які підписали, втім досі не ратифікували Конвенцію, доцільно в порівняльному аспекті звернути увагу на таких нормах. У ст. 118 КПК Республіки Молдова регламентуються деякі правила огляду комп'ютерних систем та пристроїв для зберігання комп'ютерних даних [36], втім безпосередньо процедурних положень, схожих за змістом на ті, що передбачені Конвенцією про кіберзлочинність, в результаті аналізу чинної редакції КПК Республіки Молдова виявлено не було. У ст. 90 КПК Республіки Словаччина передбачені такі процедурні прокурорські повноваження як: наказати фізичній особі та постачальнику комп'ютерних даних зберігати комп'ютерні дані та підтримувати їх цілісність, дозволити виготовлення або збереження копії таких даних, перешкоджати доступу до таких даних, видалити комп'ютерні дані з комп'ютерної системи, передати (здати) комп'ютерні дані для цілей кримінального провадження [37]. Тобто, навіть не ратифікувавши Конвенцію, парламент Республіки Словаччина надав своїм органам досудового розслідування вищезазначені процедурні повноваження.

3. Висновки

На підставі вищевикладеного маємо підстави стверджувати:

1) серед держав східної Європи на сьогодні Конвенція про кіберзлочинність набрала законної сили в Естонській Республіці, Литовській Республіці, Україні, Угорщині, Румунії і Республіці Болгарія;

2) із вище перелічених держав лише Угорщина, Румунія і Республіка Болгарія забезпечили свої органи досудового розслідування передбаченими в їх кримінальних процесуальних законодавствах повноваженнями, спрямованими на ефективне розслідування кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

3) менша увага імплементації процедурних положень приділена в Естонській Республіці, Литовській Республіці та Україні;

4) аналіз кримінальних процесуальних законів держав, у яких Конвенція про кіберзлочинність досі залишається не ратифікованою, показав, що у чинній редакції Кримінально-процесуальних кодексів Російської Федерації [30], Республіки Білорусь [31], Чеської Республіки [32], Республіки Польща [33], Латвійської Республіки [34] юридична конструкція «комп'ютерні дані» досі взагалі не використовується;

5) у Республіці Словаччина, яка досі не ратифікувала Конвенцію про кіберзлочинність, наразі передбачені такі процедурні прокурорські повноваження як: наказати фізичній особі та постачальнику комп'ютерних даних зберігати комп'ютерні дані та підтримувати їх цілісність, дозволити виготовлення або збереження копії таких даних, перешкоджати доступу до таких даних, видалити комп'ютерні дані з комп'ютерної системи, передати (здати) комп'ютерні дані для цілей кримінального провадження (ст. 90 КПК Республіки Словаччина);

6) у національному кримінальному процесуальному законодавстві України доцільно передбачити правові підстави та процесуальний порядок застосування системи процедурних повноважень органів досудового розслідування, передбаченої Конвенцією про кіберзлочинність, і наведеної вище у відповідній табличці процедурних повноважень.

Подальші наукові розвідки планується присвятити порівнянню стану імплементації відповідних кримінальних процесуальних повноважень в законодавстві інших держав – підписантів Будапештської Конвенції про кіберзлочинність.

Список літератури:

1. Official site Council of Europe. The Convention on Cybercrime of the Council of Europe (CETS No. 185). URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185 (дата звернення: 30.11.2021).

2. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вересня 2005 року № 2824-IV. Дата оновлення: 14.10.2010. URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 30.11.2021).

3. Список підписань та ратифікацій Конвенції про злочинність у сфері комп'ютерної інформації (ETS № 185) станом на 28 червня 2006 року. URL: https://zakon.rada.gov.ua/laws/show/994_789 (дата звернення: 30.11.2021).

4. Єдиний звіт про кримінальні правопорушення по державі за грудень 2014 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=111480&libid=100820# (дата звернення: 30.11.2021).

5. Єдиний звіт про кримінальні правопорушення по державі за грудень 2018 року. Генеральна прокуратура України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (дата звернення: 30.11.2021).

6. Єдиний звіт про кримінальні правопорушення по державі за грудень 2020 року. Статистика Офісу Генерального прокурора. URL: https://www.gp.gov.ua/ua/stat_n_st?dir_id=114138&libid=100820&c=edit&_c=fo (дата звернення: 30.11.2021).

7. На Кипре появятся веб-констебли. *Вестник Кипра*. URL: https://www.vkcyprus.com/society/5976-na-kipre-poyavyatsya-veb-konstebli (дата звернення: 30.11.2021).

8. Спільний проект Європейського Союзу та Ради Європи CyberEast, спрямований на реалізацію положень Будапештської Конвенції про кіберзлочинність. URL: https://www.coe.int/en/web/cybercrime/cybereast (дата звернення: 30.11.2021).

9. Спільний проект Європейського Союзу та Ради Європи CyberSouth, спрямований на реалізацію положень Будапештської Конвенції про кіберзлочинність. URL: https://www.coe.int/en/web/cybercrime/cybersouth (дата звернення: 30.11.2021).

10. Орлов Ю. Ю., Чернявський С. С. Використання електронних відображень як доказів у кримінальному провадженні. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3(104). С. 13. URL: https://scientbul.naiau.kiev.ua/article/view/612/616 (дата звернення: 30.11.2021).

11. Буяджи С. А. Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект : дис. … канд. юрид. наук : 12.00.01 / Класичний приватний університет ПВНЗ Університет Короля Данила. Київ, 2018. 203 с.

12. Кримінальний процесуальний кодекс України : Закон України від 13 квітня 2012 року № 4651-VI. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (дата звернення: 30.11.2021).

13. Про електронні документи та електронний документообіг : Закон України від 22 травня 2003 року № 851-IV. Дата оновлення: 07.11.2018. URL: https://zakon.rada.gov.ua/laws/show/851-15 (дата звернення: 30.11.2021).

14. Osula, Anna-Maria. Remote search and seizure of extraterritorial data. Dissertation for the commencement of the degree of Doctor of Philosophy (PhD) in law on February 20, 2017. University of Tartu. URL: https://dspace.ut.ee/handle/10062/55683 (дата звернення: 30.11.2021).

15. Osula, Anna-Maria. Remote search and seizure in domestic criminal procedure: Estonian case study. *International Journal of Law and Information Technology*. Volume 24. Issue 4. Winter 2016. P. 343–373. URL: https://academic.oup.com/ijlit/article/24/4/343/2566974 (дата звернення: 30.11.2021).

16. Shurson, Jessica. Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law. *International Journal of Law and Information Technology.* Volume 28. Issue 2. Summer

2020. P. 167–184. URL: https://academic.oup.com/ijlit/article/28/2/167/5866176 (дата звернення: 30.11.2021).

17. Scrtic, Drazen. Search and seizure data in cyber space – mechanisms to preserve and reproduce data in a non-volatile format: Criminal justice and security – contemporary criminal justice practice and research, conference proceedings. 2013. URL: https://apps.webofknowledge.com/full_record.do?product=WOS&search_mode=GeneralSearch&qid=61&SID=D6A4txHKkBgNPFIH7Kp&page=6&doc=51&cacheurlFromRightClick=no (дата звернення: 30.11.2021).

18. Lopez-Barajas Perea, Inmaculada. New technology applied to criminal investigation: searching computers: Revista de los Estudios de Derecho y Ciencia Politica. Universitat Oberta de Catalunia. IDP № 24 (Februare, 2017). URL: https://www.researchgate.net/publication/318119092_New_technology_applied_to_criminal_investigation_searching_computers (дата звернення: 30.11.2021).

19. Klevtsov K., Vasyukov V. Obtaining electronic information on criminal cases within the framework of international cooperation: *Vestnik of Saint Petersburg University-Pravo.* 2021. T. 12. Vol. 1. P. 36–51. URL: https://click.endnote.com/viewer?doi=10.21638%2Fspbu14.2021.103&token=WzMxNDQ3NzMsIjEwLjIxNjM4L3NwYnUxNC4yMDIxLjEwMyJd.xsdqOHVyTX_6yu0UOtWtLfu7Z7A (дата звернення: 30.11.2021).

20. Про порядок денний десятої сесії Верховної Ради України восьмого скликання: постанова Верховної Ради України від 7 лютого 2019 року № 2679-VIII. URL: https://zakon.rada.gov.ua/laws/show/2679-viii (дата звернення: 30.11.2021).

21. Проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю від 19 червня 2015 року № 2133а. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2133%D0%B0&skl=9 (дата звернення: 30.11.2021).

22. Проект Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю від 30 вересня 2016 року № 2133а-1. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2133%D0%B0-1&skl=9 (дата звернення: 30.11.2021).

23. Проект Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері від 12 липня 2017 року № 6688. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236 (дата звернення: 30.11.2021).

24. Кримінально-процесуальний кодекс Естонської Республіки від 01 липня 2004 року. Дата оновлення: 15.07.2021. URL: https://www.juristaitab.ee/ru/zakonodatelstvo/ugolovno-processualnyy-kodeks (дата звернення: 30.11.2021).

25. Code of Criminal Procedure of the Republic of Lithuania in force from 14.03.2002. URL: https://wipolex.wipo.int/ru/text/202109 (дата звернення: 30.11.2021).

26. Act XIX of 1998 on Criminal Proceedings of Hungary. URL: https://sherloc.unodc.org/cld/document/hun/1998/hungarian_criminal_procedure_code.html? (дата звернення: 30.11.2021).

27. Кримінально-процесуальний кодекс Румунії від 7 лютого 2014 року. Дата оновлення: 10.09.2018. URL: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2018)043-e (дата звернення: 30.11.2021).

28. Penal Procedure Code the Republic of Bulgaria in force from 29.04.2006, amend. SG. 13/11 Feb 2011. Sharing Electronic Resources and Laws on Crime. URL: https://sherloc.unodc.org/cld/document/bgr/2006/criminal_procedure_code_of_the_republic_of_bulgaria.html (дата звернення: 30.11.2021).

29. Case of Iliya Stefanov v. Bulgaria (Application no. 65755/01) from 22 May 2008. URL: https://international.vlex.com/vid/case-of-iliya-stefanov-v-bulgaria-41720163 (дата звернення: 30.11.2021).

30. Кримінально-процесуальний кодекс Російської Федерації від 18 грудня 2001 року № 174-ФЗ. Дата оновлення: 08.12.2020. URL: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=602039487&backlink=1&&nd=102073942 (дата звернення: 30.11.2021).

31. Кримінально-процесуальний кодекс Республіки Білорусь від 16 липня 1999 року № 295-З. Дата оновлення: 06.01.2021. URL: https://etalonline.by/document/?regnum=HK9900295 (дата звернення: 30.11.2021).

32. Кримінально-процесуальний кодекс Чеської Республіки від 29 листопада 1961 року № 141/1961 Coll. Дата оновлення: 43/2012. URL: https://www.legislationline.org/download/id/6371/file/Czech%20Republic_CPC_1961_am2012_en.pdf (дата звернення: 30.11.2021).

33. Кримінально-процесуальний кодекс Республіки Польща від 6 червня 1997 року. Дата оновлення: 01.04.2021. URL: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970890555/U/D19970555Lj.pdf (дата звернення: 30.11.2021).

34. Кримінально-процесуальний кодекс Латвійської Республіки від 11 травня 2005 року. Дата оновлення: 04.03.2021. URL: https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law (дата звернення: 30.11.2021).

35. Рішення ЄСПЛ «Юдицька та інші проти Росії» (заява № 5678/06) від 12 лютого 2015 року. URL: https://protocol.ua/ua/yuditska_ta_inshi_proti_rosii_peresliduvannya_predstavnikiv_yuridichnoi_profesii/ (дата звернення: 30.11.2021).

36. Кримінально-процесуальний кодекс Республіки Молдова від 14 березня 2003 року № 122-XV. Дата оновлення: 16.12.2020. URL: http://continent-online.com/Document/?doc_id=30397729#pos=6;-142 (дата звернення: 30.11.2021).

37. Кримінально-процесуальний кодекс Республіки Словаччина No. 301/2005 Coll. URL: https://www.legislationline.org/download/id/8295/file/Slovakia_CPC_2005_excerpts_en.pdf (дата звернення: 30.11.2021).

References:

1. Official site Council of Europe. The Convention on Cybercrime of the Council of Europe (CETS No. 185). Retrieved from: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185 (accessed 30 November 2021).

2. On Ratification of the Convantion of Cybercrime: Law of Ukraine of September 7, 2005 № 2824-IV. Update data: 14.10.2010. Retrieved from: https://zakon.rada.gov.ua/laws/show/2824-15 (accessed 30 November 2021).

3. List of signatures and ratifications of the Convention on Computer Information Crime (ETS № 185) up to 28 June 2006. Retrieved from: https://zakon.rada.gov.ua/laws/show/994_789 (accessed 30 November 2021).

4. The single report on criminal offenses on the state for December, 2014. General Prosecutor of Ukraine. Retrieved from: https://www.gp.gov.ua/ua/stst2011.html?dir_id=111480&libid=100820# (accessed 30 November 2021).

5. The single report on criminal offenses on the state for December, 2018. General Prosecutor of Ukraine. Retrieved from: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113653&libid=100820&c=edit&_c=fo (accessed 30 November 2021).

6. The single report on criminal offenses on the state for December, 2020. Statistics of the Office of the Attorney General. Retrieved from: https://www.gp.gov.ua/ua/stat_n_st?dir_id=114138&libid=100820&c=edit&_c=fo (accessed 30 November 2021).

7. There will be web constables in Cyprus. *Bulletin of Cyprus*. Retrieved from: https://www.vkcyprus.com/society/5976-na-kipre-poyavyatsya-veb-konstebli (accessed 30 November 2021).

8. Joint project of the European Union and the Council of Europe CyberEast, aimed at implementing the provisions of the Budapest Convention on Cybercrime. Retrieved from: https://www.coe.int/en/web/cybercrime/cybereast (accessed 30 November 2021).

9. Joint project of the European Union and the Council of Europe CyberSouth, aimed at implementing the provisions of the Budapest Convention on Cybercrime. Retrieved from: https://www.coe.int/en/web/cybercrime/cybersouth (accessed 30 November 2021).

10. Orlov Yu. Yu., Cherniavskyi S. S. (2017). The use of electronic mappings as evidence in criminal proceedings. *Scientific Bulletin of the National Academy of Internal Affairs*, no. 3(104), p. 13. Retrieved from: https://scientbul.naiau.kiev.ua/article/view/612/616 (accessed 30 November 2021).

11. Buiadzhy S. A. (2018). Legal regulation of the fight against cybercrime: theoretical and legal aspect: dissertation. … Doctor of Law: 12.00.01 / Classic private university PHEI King Daniel University. Kyiv, 203 p.

12. Criminal Procedure Code of Ukraine: Law of Ukraine of April 13, 2012 № 4651-VI. Update data: 14.01.2021. Retrieved from: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (accessed 30 November 2021).

13. On electronic documents and electronic document circulation: the Law of Ukraine of May 22, 2003 № 851-IV. Update data: 07.11.2018. Retrieved from: https://zakon.rada.gov.ua/laws/show/851-15 (accessed 30 November 2021).

14. Osula, Anna-Maria. Remote search and seizure of extraterritorial data. Dissertation for the commencement of the degree of Doctor of Philosophy (PhD) in law on February 20, 2017. University of Tartu. Retrieved from: https://dspace.ut.ee/handle/10062/55683 (accessed 30 November 2021).

15. Osula, Anna-Maria. Remote search and seizure in domestic criminal procedure: Estonian case study. *International Journal of Law and Information*

Technology, vol. 24, issue 4, Winter 2016, pp. 343–373. Retrieved from: https://academic.oup.com/ijlit/article/24/4/343/2566974 (accessed 30 November 2021).

16. Shurson, Jessica. Data protection and law enforcement access to digital evidence: resolving the reciprocal conflicts between EU and US law. *International Journal of Law and Information Technology*, vol. 28, issue 2, Summer 2020, pp. 167–184. Retrieved from: https://academic.oup.com/ijlit/article/28/2/167/5866176 (accessed 30 November 2021).

17. Scrtic, Drazen (2013). Search and seizure data in cyber space – mechanisms to preserve and reproduce data in a non-volatile format: Criminal justice and security – contemporary criminal justice practice and research, conference proceedings. Retrieved from: https://apps.webofknowledge.com/full_record.do?product=WOS&search_mode=GeneralSearch&qid=61&SID=D6A4txHKkBgNPFIH7Kp&page=6&doc=51&cacheurlFromRightClick=no (accessed 30 November 2021).

18. Lopez-Barajas Perea, Inmaculada (Februare, 2017). New technology applied to criminal investigation: searching computers: Revista de los Estudios de Derecho y Ciencia Politica. Universitat Oberta de Catalunia. IDP № 24. Retrieved from: https://www.researchgate.net/publication/318119092_New_technology_applied_to_criminal_investigation_searching_computers (accessed 30 November 2021).

19. Klevtsov K., Vasyukov V. (2021). Obtaining electronic information on criminal cases within the framework of international cooperation. *Vestnik of Saint Petersburg University-Pravo*, t. 12, vol. 1, pp. 36–51. Retrieved from: https://click.endnote.com/viewer?doi=10.21638%2Fspbu14.2021.103&token=WzMxNDQ3NzMsIjEwLjIxNjM4L3NwYnUxNC4yMDIxLjEwMyJd.xsd-qOHVyTX_6yu0UOtWtLfu7Z7A (accessed 30 November 2021).

20. On the agenda of the tenth session of the Verkhovna Rada of Ukraine of the eighth convocation: Resolution of the Verkhovna Rada of Ukraine of February 7, 2019 № 2679-VIII. Retrieved from: https://zakon.rada.gov.ua/laws/show/2679-viii (accessed 30 November 2021).

21. . Draft Law on Amendments to Certain Laws of Ukraine on Strengthening Liability for Committed Offenses in the Sphere of Information Security and Combating Cybercrime of June 19, 2015 № 2133a. Retrieved from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2133%D0%B0&skl=9 (accessed 30 November 2021).

22. Draft Law on Amendments to Certain Laws of Ukraine on Strengthening Liability for Committed Offenses in the Sphere of Information Security and Combating Cybercrime of September 30, 2016 № 2133a-1. Retrieved from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3516=2133%D0%B0-1&skl=9 (accessed 30 November 2021).

23. Draft Law on Amendments to Certain Legislative Acts of Ukraine on Counteracting Threats to National Security in the Information Sphere of July 12, 2017 № 6688. Retrieved from: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236 (accessed 30 November 2021).

24. Code of Criminal Procedure of the Republic of Estonia of July, 1, 2004. Update data: 08.01.2021. Retrieved from: https://www.juristaitab.ee/ru/zakonodatelstvo/ugolovno-processualnyy-kodeks (accessed 30 November 2021).

25. Code of Criminal Procedure of the Republic of Lithuania in force from 14.03.2002. Retrieved from: https://wipolex.wipo.int/ru/text/202109 (accessed 30 November 2021).

26. Act XIX of 1998 on Criminal Proceedings of Hungary. Retrieved from: https://sherloc.unodc.org/cld/document/hun/1998/hungarian_criminal_procedure_code.html? (accessed 30 November 2021).

27. Code of Criminal Procedure of Romania of February, 7, 2014. Update data: 10.09.2018. Retrieved from: https://www.venice.coe.int/webforms/documents/default.aspx?pdffile=CDL-REF(2018)043-e (accessed 30 November 2021).

28. Penal Procedure Code the Republic of Bulgaria in force from 29.04.2006, amend. SG. 13/11 Feb 2011. Sharing Electronic Resources and Laws on Crime. Retrieved from: https://sherloc.unodc.org/cld/document/bgr/2006/criminal_procedure_code_of_the_republic_of_bulgaria.html (accessed 30 November 2021).

29. Case of Iliya Stefanov v. Bulgaria (Application no. 65755/01) from May, 22, 2008. Retrieved from: https://international.vlex.com/vid/case-of-iliya-stefanov-v-bulgaria-41720163 (accessed 30 November 2021).

30. Code of Criminal Procedure of the Russian Federation of December, 18, 2001 № 174-FL. Update data: 08.12.2020. Retrieved from: http://pravo.gov.ru/proxy/ips/?docbody=&prevDoc=602039487&backlink=1&&nd=102073942 (accessed 30 November 2021).

31. The Code of Criminal Procedure of the Republic of Belarus of July, 16, 1999 № 295-L. Update data: 06.01.2021. Retrieved from: https://etalonline.by/document/?regnum=HK9900295 (accessed 30 November 2021).

32. Criminal Procedure Code of the Czech Republic of November, 29, 1961 № 141/1961 Coll. Update data: 43/2012. Retrieved from: https://www.legislationline.org/download/id/6371/file/Czech%20Republic_CPC_1961_am2012_en.pdf (accessed 30 November 2021).

33. Code of Criminal Procedure of the Republic of Poland of June, 6, 1997. Update data: 01.04.2021. Retrieved from: https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU19970890555/U/D19970555Lj.pdf (accessed 30 November 2021).

34. Code of Criminal Procedure of the Republic of Latvia of May, 11, 2005. Update data: 04.03.2021. Retrieved from: https://likumi.lv/ta/en/en/id/107820-criminal-procedure-law (accessed 30 November 2021).

35. Judgment of the European Court of Human Rights "Yuditska and Others v. Russia" (application no. 5678/06) of February, 12, 2015. Retrieved from: https://protocol.ua/ua/yuditska_ta_inshi_proti_rosii_peresliduvannya_predstavnikiv_yuridichnoi_profesii/ (accessed 30 November 2021).

36. Code of Criminal Procedure of the Republic of Moldova of March, 14, 2003 № 122-XV. Update data: 16.12.2020. Retrieved from: http://continent-online.com/Document/?doc_id=30397729#pos=6;-142 (accessed 30 November 2021).

37. Code of Criminal Procedure of the Slovak Republic No. 301/2005 Coll. Retrieved from: https://www.legislationline.org/download/id/8295/file/Slovakia_CPC_2005_excerpts_en.pdf (accessed 30 November 2021).