KrYUI ODUVS [in Ukr.].

3. Ampleeva, T.Yu. (2006) Po Zakonu Russkomu. Ystoryya uholovnoho sudoproyzvodstva Drevney Rusy [According to the Law of Russian. History of criminal proceedings of Ancient Rus]: monohrafyya. Moskva: MYYT. URL: https://www.twirpx.com/file/1767938. [in Rus.].

4. Elynskyy, V.Y. (1997) Stanovlenye y razvytye uholovnoho syska v Rossyy (X – nach. XX v.) [Formation and development of criminal investigation in Russia (X - beginning of XX century)]. Moskva: MYUY. URL: https://search.rsl.ru/ru/record/01001778898 (data zvernennya: 10.04.2019). [in Rus.].

5. Bohatyrev, A.H. (2014) Ystoryya stanovlenyya y razvytyya ponyatyya operatyvnoho vnedrenyya v deyatel′nosty Rossyyskoy polytsyy (mylytsyy) [History of the formation and development of the concept of operational implementation in the activities of the Russian police (police)]. *Vestnyk Moskovskoho unyversyteta MVD Rossyy,* 8. URL: https://cyberleninka.ru/article/n/istoriya-stanovleniya-i-razvitiya-ponyatiya-operativnogo-vnedreniya-v-deyatelnosti-rossiyskoy-politsii-militsii. [in Rus.].

SUMMARY

Davidyuk V.M. Genesis of operative-search activity of the National Police in combating crime. The author makes an attempt to conduct the genesis of the formation of the use of the forces of the ORD in counteracting crime. In particular, historical literature is analyzed and analyzed from ancient times to the present, certain historical stages and their characteristic features are singled out. Thus, it is determined that the first mention of persons who made vowels on secret actions aimed at establishing the perpetrators of the crime occurred during the years of Kievan Rus, in particular mentioning those who are looking for criminals. In the middle of the sixteenth century, the second stage of the formation of the ORD forces was initiated, which were used in the course of unwilling activity, in particular, of separate subjects of investigative activity - the detectives, whose powers were given to certain representatives of the state authorities to carry out secret measures for combating crime and to involve civilian population to carry out some of them. The third stage begins in the XVIII century. the adoption of the Preobrazhensky order and other regulations, which resulted in the establishment of a police office, where execution of secret search activities is carried out by soldiers and non-commissioned officers. Briefly characterizing the XIth century, it has been determined that the existence of both the main and auxiliary forces in the course of carrying out the secret search work is actually traced. In particular, the police detachments are created, the help of military, as well as secret agents is used. The fourth period begins during the Soviet Union and lasts until 1991, that is, starting from the 20s of the 20th century, excluding military and first post-war years, special units of the police, the NKVD, the KGB and other law enforcement agencies that were exclusively the right to conduct secret search activities. The adoption of the Law of Ukraine "On Operational and Investigative Activity" and the fifth phase began, which by the way continues to this day.

Keywords*: forces, subjects, operative-search activity, genesis, historical stages.*

УДК 343.141
DOI: 10.31733/2078-3566-2019-2-134-142

Захарко А. В.©
кандидат юридичних наук, доцент
(Дніпропетровський державний університет внутрішніх справ)

АНАЛІЗ СТАНУ ЗАКОНОТВОРЧОЇ ДІЯЛЬНОСТІ ЩОДО ІМПЛЕМЕНТАЦІЇ ПРОЦЕДУРНИХ ПОЛОЖЕНЬ КОНВЕНЦІЇ ПРО КІБЕРЗЛОЧИННІСТЬ

Здійснено огляд процедурних положень Конвенції про кіберзлочинність. Проаналізовано актуальний стан кримінального процесуального законодавства на наявність норм, що кореспондують процедурним положенням Конвенції про кіберзлочинність. Висвітлено порядок денний десятої сесії Верховної Ради України восьмого скликання на предмет наявності законопроектів щодо імплементації процедурних положень Конвенції про кіберзлочинність до Кримінального процесуального кодексу України (далі – КПК України). Зазначені законопроекти досліджено на предмет охоплення ними усієї системи відповідних процедурних положень Конвенції про кіберзлочинність.

Ключові слова: *процедурні положення, Конвенція про кіберзлочинність, кримінальні процесуальні норми, обсяг імплементації.*

ORCID iD: https://orcid.org/0000-0003-1216-5323
a.zaharko@ukr.net

Постановка проблеми. 1 липня 2006 року з метою підвищення ефективності кримінальних розслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, для створення умов із надання органам досудового розслідування можливості збирання доказів, що стосуються злочину, в електронній формі, в Україні набрала чинності Конвенція про кіберзлочинність (далі – Конвенція) [1-3]. Крім цієї Конвенції, питанню ефективності діяльності органів досудового розслідування щодо збору доказів, пов'язаних із комп'ютерними даними та їх обробкою в електронних інформаційних системах, приділено увагу, зокрема, в Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності.

Згідно зі ст. 29 Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності, Україна має розробляти та вдосконалювати конкретні програми підготовки персоналу правоохоронних органів, зокрема, прокурорів і слідчих, такою мірою, щоб забезпечувати питання збору доказів, розробки методів, використовуваних у боротьбі з транснаціональними організованими злочинами, вчинюваними з використанням комп'ютерів, телекомунікаційних мереж та інших видів сучасних технологій [4]. Таким чином, питання збору доказів при розслідуванні злочинів, вчинюваних з використанням електронних форм передавання інформації, створення якісної регламентації відповідних процедурних повноважень органів досудового розслідування набули особливої актуальності.

Вивчення КПК України [5] показало недостатній рівень регламентованості в ньому процедурних повноважень органів досудового розслідування при розслідуванні злочинів, вчинюваних з використанням комп'ютерних даних[1]. Ці процедурні повноваження мали б надавати можливість органам досудового розслідування оперативно збирати докази при роботі з комп'ютерними даними, комп'ютерними носіями інформації, транспортними телекомунікаційними мережами тощо.

Згідно зі ст. 14 Конвенції [1], 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.

Аналіз публікацій, в яких започатковано розв'язання даної проблеми. У нормативних документах: проекти Закону про внесення змін до деяких законів України: № 2133а від 19 червня 2015 року [6], № 2133а-1 від 30 вересня 2016 року [7], № 6688 від 12 липня 2017 року [8], запропоновано імплементацію деяких із регламентованих у Конвенції про кіберзлочинність процедурних положень. Деякі питання, пов'язані з імплементацією відповідних положень, висвітлювалися в публікаціях С. А. Буяджи [9], Ю. Ю. Орлова, С. С. Чернявського [10].

Мета статті полягає у висвітленні активності законодавця в контексті імплементації до КПК України процедурних положень Конвенції про кіберзлочинність та обґрунтуванні пропозицій щодо подальшої оптимізації цього процесу.

Для досягнення поставленої мети планується послідовне виконання таких завдань: 1) зіставити процедурні положення Конвенції про кіберзлочинність із повноваженнями сторони обвинувачення за чинним КПК України, 2) проаналізувати відповідні законопроекти та з'ясувати стан законотворчого процесу щодо імплементації відповідних процедурних положень Конвенції до КПК України, 3) обґрунтувати пропозиції, спрямовані на розширення повноважень сторони обвинувачення у КПК України задля досягнення їх відповідності регламентованому в Конвенції обсягу й змісту процедурних положень.

[1] Згідно зі ст.1 Конвенції про кіберзлочинність, термін «комп'ютерні дані» означає будь-яке представлення фактів, інформації або концепцій у формі, яка є придатною для обробки у комп'ютерній системі, включаючи програму, яка є придатною для того, щоб спричинити виконання певної функції комп'ютерною системою.

Виклад основного матеріалу. Спершу проаналізуємо процедурні положення Конвенції про кіберзлочинність. Для ефективного збирання доказів у електронній формі у ст.ст. 16, 17 Конвенції передбачено:

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) покладання обов'язку на особу, під контролем якої знаходяться відповідні комп'ютерні дані, зберігати і підтримувати цілісність таких комп'ютерних даних протягом певного періоду, необхідного для отримання компетентним органом дозволу на розкриття таких даних;

3) покладання обов'язку на особу, яка має зберігати відповідні комп'ютерні дані за ордером компетентного органу, дотримуватися конфіденційності 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 органу обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і маршруту, яким була передана інформація [1].

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 зі 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;
- 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 в 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 [1]. 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.

У ст.ст. 29, 30, 32 Конвенції також передбачено порядок виконання тимчасових заходів у контексті міжнародного співробітництва, втім, ці тимчасові заходи не будемо досліджувати в цій статті, оскільки їх дослідження потребує окремої уваги.

Конвенція про кіберзлочинність була ратифікована Законом України від 7 вересня 2005 року. Набула чинності в Україні з 1 липня 2006 року. Проаналізувавши чинне кримінальне процесуальне законодавство України на предмет наявності відповід-

них процесуальних повноважень, можемо констатувати:

1) український кримінальний процесуальний закон наразі передбачає можливість збирати електронні документи, в тому числі комп'ютерні дані, як підвид процесуальних джерел доказів (документів) за контекстом ч. 2 ст. 84 КПК України. Це випливає зі змісту ст. 99 КПК України, яка в п. 1 ч. 2 відносить електронні носії інформації до документів. Цю тезу також підтверджено у ст. 8 Закону України «Про електронні документи та електронний документообіг», де зазначено: допустимість електронного документа як доказу не може заперечуватися виключно на підставі того, що він має електронну форму [11] і кореспондується з рішенням ЄСПЛ «Сервуло та партнери» проти Португалії від 3 вересня 2015 року, в п. 96 якого констатується, що для визнання «передбаченим законом» збирання «комп'ютерних доказів», останні не обов'язково буквально мають регламентуватися у Кримінальному процесуальному кодексі [12]. Уявляється, що чинний КПК України слід тлумачити таким чином, що ним передбачається огляд, обшук комп'ютерної системи, її частини, комп'ютерного носія інформації, комп'ютерних даних, проникнення до них (ст.ст. 233–237 КПК), тимчасовий доступ до комп'ютерної системи або її частини (ст. 164 КПК), арешт комп'ютерної системи, її частини або комп'ютерного носія інформації, копіювання і збереження копій комп'ютерних даних (ст. 170, 159 КПК). Врешті-решт, звертаємо увагу на поняття «інше володіння» особи, визначене в постанові Пленуму Верховного Суду України від 28 березня 2008 року № 2 як об'єкти природного чи штучного походження, які за своїми властивостями дають змогу туди проникнути і зберегти або приховати певні предмети, речі, цінності тощо [13]. Уявляється, під іншим володінням особи, зокрема, можна розуміти й комп'ютерні дані, комп'ютерну систему, комп'ютерний носій інформації тощо. Адже навіть самі по собі комп'ютерні дані можуть містити відомості про приватне життя особи, мати грошовий еквівалент вартості, і навіть у комп'ютерні дані, тобто всередину їх, може проникнути шкідливе вірусне програмне забезпечення;

2) на жаль, в КПК України досі не передбачено достатніх і конкретних положень, які б надавали стороні обвинувачення процесуальні повноваження[1], що кореспондували б вищезазначеним зобов'язанням України за Конвенцією та відповідним процедурним положенням, передбаченим у Конвенції. Погоджуємося з позицією Ю. Ю. Орлова, С. С. Чернявського про доцільність внесення відповідних змін до КПК України [10].

Згідно з 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 вищезазначені можливості компетентним органам не можна ототожнювати з конкретними повноваженнями органів досудового розслідування, прокурора. Тому наразі органи досудового розслідування України не можуть застосовувати ряд зазначених (не імплементованих до КПК України) положень Конвенції, бо КПК України не містить кореспондуючих їм відповідних повноважень.

Перейдемо до виконання другого завдання цієї статті: дослідимо відповідні законопроекти та з'ясуємо актуальний стан законотворчого процесу щодо імплементації відповідних процедурних положень Конвенції до КПК України. Аналіз порядку денного десятої сесії Верховної Ради України восьмого скликання [14] показав, що питання посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю в Україні не залишаються поза увагою законодавця. У вказаному порядку денному, зокрема, наявні вищезазначені нами проекти Закону про внесення змін до деяких законів України: № 2133а від 19 червня 2015 року [6], № 2133а-1 від 30 вересня 2016 року [7]. Окремої уваги заслуговує проект Закону про внесення змін до деяких законодавчих актів України № 6688 від 12 липня 2017 року [8]. В зазначеному

[1] У цій статті здійснено спробу відшукати необхідні специфічні процесуальні засоби збирання доказів стороною обвинувачення у контексті гласних слідчих (розшукових) дій та заходів забезпечення кримінального провадження. Не слід плутати схожі із переліченими положеннями про збирання комп'ютерних даних у реальному масштабі часу, зазначені в заголовку 5 Конвенції, які дійсно імплементовані в КПК України, але до глави 21 «Негласні слідчі (розшукові) дії».

порядку денному є й інші проекти Законів, спрямовані на посилення захисту інформаційних та інформаційно-телекомунікаційних систем, але через відсутність у них спрямованості на імплементацію процедурних положень Конвенції про кіберзлочинність, залишимо ці інші законопроекти поза увагою.

Перейдемо до послідовного аналізу зазначених законопроектів. У п. 3 проекту Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю № 2133а від 19 червня 2015 року [6], зокрема, запропоновано доповнити ст. 25 Закону «Про Службу безпеки України» правом безперешкодно отримувати в установленому законом порядку доступ до інформації, яка обробляється в державних електронних інформаційних ресурсах (реєстри, бази та банки даних, інші інформаційні масиви), інформаційних, інформаційно-телекомунікаційних, телекомунікаційних системах операторів і провайдерів телекомунікацій, інших суб'єктів, які обробляють інформацію в електронному вигляді, незалежно від форм власності, щодо споживача, отриманих при укладанні договору, наданні телекомунікаційних послуг, у тому числі отриманні послуг, їх тривалості та змісту, маршрутів передавання, а також тієї, що передається та отримується каналами команди реагування на комп'ютерні інциденти CERT – UA і через можливості національного контактного пункту 24/7, що функціонує в рамках Конвенції про кіберзлочинність. У разі загрози втрати інформації, яка міститься у державних реєстрах, базах даних (у тому числі приватних та комерційних структур), які використовуються у державних органах, установах та організаціях, передбачено можливість здійснювати заходи по її збереженню, в тому числі й через блокування доступу до відповідних інформаційних ресурсів. Як бачимо, тут мова йде про фрагментарне врахування положень, викладених у Конвенції про кіберзлочинність. У змісті проаналізованого законопроекту немає положень, у яких би відображалося системне впровадження в кримінальне процесуальне законодавство процедурних положень Конвенції у вигляді додаткових повноважень сторони обвинувачення, що створять умови й можливості для ефективного розслідування злочинів, пов'язаних із електронною обробкою комп'ютерних даних.

Проаналізуємо наступний законопроект. У п. 4 проекту Закону про внесення змін до деяких законів України щодо посилення відповідальності за вчинені правопорушення у сфері інформаційної безпеки та боротьби з кіберзлочинністю № 2133а-1 від 30 вересня 2016 року [7], зокрема, запропоновано доповнити ч. 2 ст. 8 Закону «Про основи національної безпеки України» (який втратив чинність 21 червня 2018 року) такими напрямками державної політики з питань національної безпеки України: «удосконалення законодавства з питань інформаційної безпеки, у тому числі кібербезпеки; запобігання проявам комп'ютерної злочинності та комп'ютерного тероризму; удосконалення засобів захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах; удосконалення форм і способів протидії інформаційним заходам, які спрямовані на послаблення обороноздатності держави; забезпечення повноправної участі України в міжнародному співробітництві у сфері боротьби з комп'ютерною злочинністю та комп'ютерним тероризмом». Аналізуючи сутність цього законопроекту, маємо підстави зазначити, що органам досудового розслідування в ньому знову таки не передбачено реального надання додаткових повноважень, які б створювали належні умови для підвищення ефективності досудових розслідувань відповідних кримінальних правопорушень. У чинному нині ЗУ «Про національну безпеку України» [15], яким замінено вищезазначений ЗУ «Про основи національної безпеки України» [16], знову ж таки, на жаль, поки що немає положень, якими можна було б аргументувати, що законодавець системно просунувся в напрямку імплементації взятих за Конвенцією зобов'язань.

Перейдемо до аналізу третього законопроекту. У проекті Закону про внесення змін до деяких законодавчих актів України щодо протидії загрозам національній безпеці в інформаційній сфері № 6688 від 12 липня 2017 року [8] приділено більш предметну увагу створенню умов для реального посилення повноважень компетентних органів і підвищення дієвості відповідних досудових розслідувань. Зокрема, в п. 3 зазначеного законопроекту передбачено доповнення ст. 25 ЗУ «Про Службу безпеки України» [17] правом блокування доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) з використанням технічних засобів, що встановлюються операторами, провайдерами телекомунікацій, а також іншими суб'єктами господарювання на виконання вимог частини 4-1 статті 39 Закону України "Про телекомунікації"» (обов'язки операторів телекомунікацій встановлювати власним коштом відповідні технічні засоби та забезпе-

чувати їх функціонування). У п. 5 зазначеного законопроекту передбачено доповнення ч. 1 ст. 1 ЗУ «Про телекомунікації» рядом дефініцій: «блокування доступу до інформаційного ресурсу (сервісу)», «веб-сайт (сайт)», «сторінка сайту в мережі Інтернет (інтернет-сторінка або веб-сторінка)», «доменне ім'я», «мережева адреса», «реєстратор домену (доменного імені)» тощо. Впровадження цих дефініцій у законодавство сприятиме належній уніфікації термінології і полегшить вирішення досліджуваних у цій статті процедурних питань.

Також у цьому законопроекті передбачено створення Єдиного реєстру виконання судових рішень і застосування санкцій у сфері телекомунікацій, зокрема, через доповнення ЗУ «Про телекомунікації» відповідною статтею: «Стаття 18-1. Єдиний реєстр виконання судових рішень і застосування санкцій у сфері телекомунікацій». У зазначеній статті, зокрема, запропоновано створення Єдиного реєстру виконання судових рішень і застосування санкцій у сфері телекомунікацій (далі – Реєстр) з метою блокування доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) в інформаційно-телекомунікаційних мережах (системах) у мережі Інтернет, що містять інформацію, поширення якої в Україні заборонено. До Реєстру будуть включені: доменні імена та (або) покажчики сторінок сайтів у мережі Інтернет, що містять інформацію, поширення якої в Україні заборонено, та (або) мережні адреси, що дають змогу ідентифікувати лінії доступу або вузли мережі Інтернет, які містять інформацію, поширення якої в Україні заборонено. Підставою для включення до Реєстру відповідних відомостей є надходження до національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, прийнятого відповідно до закону рішення слідчого судді, суду, прокурора, слідчого, погодженого з прокурором, про застосування тимчасового блокування (обмеження) доступу до інформаційних ресурсів (сервісів) чи рішення суду про блокування доступу до інформаційних ресурсів (сервісів), а також набрання чинності рішення Ради національної безпеки та оборони України щодо застосування санкцій відповідно до Закону України "Про санкції". Тимчасовим блокуванням (обмеженням) доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) пропонується вважати дії, внаслідок яких унеможливлюється доступ та/або поширення інформації з визначеного (ідентифікованого) інформаційного ресурсу (сервісу) через інформаційні, телекомунікаційні та інформаційно-телекомунікаційні мережі (системи) з метою припинення кримінального правопорушення чи запобігання вчиненню іншого. Тимчасове блокування (обмеження) доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) в інформаційно-телекомунікаційних мережах (системах) може застосовуватися: під час досудового розслідування – слідчим суддею за клопотанням слідчого, погодженим з прокурором, або за клопотанням прокурора, а під час судового провадження – судом за клопотанням прокурора.

У виняткових невідкладних випадках, пов'язаних із врятуванням життя людей та запобіганням вчиненню тяжкого або особливо тяжкого злочину, тимчасове блокування (обмеження) доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) може бути розпочато до постановлення ухвали слідчого судді, суду за постановою прокурора або постановою слідчого, погодженою прокурором, і застосовується на строк не більше 48 годин. У такому випадку прокурор, слідчий за погодженням з прокурором зобов'язаний невідкладно після початку здійснення таких дій звернутися з відповідним клопотанням до слідчого судді чи суду.

На підставі вищевикладеного аналізу чинного КПК України, інших законів та законопроектів, що наразі знаходяться на порядку денному у Верховній Раді України, можемо навести такі **висновки:**

1) повноваження сторони обвинувачення збирати докази вчинення злочинів у електронній формі за чинним КПК України є значно вужчими, у порівнянні з регламентованими в Конвенції про кіберзлочинність відповідними процедурними положеннями;

2) чинний КПК України правильно тлумачити як такий, в якому передбачено можливість для органів досудового розслідування проводити: огляд, обшук комп'ютерної системи, її частини, комп'ютерного носія інформації, комп'ютерних даних, проникнення до них, тимчасовий доступ до комп'ютерної системи або її частини, арешт комп'ютерної системи, її частини або комп'ютерного носія інформації, копіювання і збереження копій комп'ютерних даних;

3) парламентом на сьогодні проводиться законотворча діяльність щодо імплементації до кримінального процесуального законодавства таких процедурних положень

Конвенції про кіберзлочинність, як збереження комп'ютерної інформації, в тому числі шляхом блокування доступу до відповідних інформаційних ресурсів (законопроект № 2133а); тимчасове блокування (обмеження) доступу до визначеного (ідентифікованого) інформаційного ресурсу (сервісу) в інформаційно-телекомунікаційних мережах (системах) (законопроект № 6688);

4) в цілому у проаналізованих законопроектах не приділено достатньої уваги імплементації таких процедурних повноважень: термінове збереження визначених комп'ютерних даних; зобов'язання особи зберігати цілісність комп'ютерних даних; зобов'язання особи підтримувати конфіденційність даного факту; термінове розкриття обсягу даних про рух інформації; поширення обшуку або подібного доступу до комп'ютерної системи, її частини, доступних першій системі, але фізично розташованих за межами об'єкта, в якому проводиться обшук, але в межах території держави, на яку поширюється юрисдикція органу досудового розслідування; заборона доступу або вилучення комп'ютерних даних з комп'ютерної системи, до якої здійснювався доступ, тощо.

Тому парламенту в подальшому пропонується приділити більше уваги наданню органам досудового розслідування системи вищеперелічених процедурних повноважень, що неодмінно підвищить ефективність досудових розслідувань кримінальних правопорушень, визначених Конвенцією про кіберзлочинність, а також інших кримінальних правопорушень, вчинених за допомогою комп'ютерних систем.

Бібліографічні посилання

1. Конвенція про кіберзлочинність, ратифікована законом від 07 вересня 2005 року № 2824-IV. Дата оновлення: 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 27.02.2019).

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: 03.03.2019).

3. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи, ратифікований законом від 21 липня 2006 року № 23-V. URL: https://zakon.rada.gov.ua/laws/show/994_687/conv (дата звернення: 18.03.2019).

4. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності, прийнята резолюцією 55/25 Генеральної Асамблеї від 15 листопада 2000 року, ратифікована законом від 4 лютого 2004 року № 1433-IV. Дата оновлення: 4.02.2004. URL: https://zakon.rada.gov.ua/laws/show/995_789 (дата звернення: 18.03.2019).

5. 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: 30.04.2019).

6. 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: 12.03.2019).

7. 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: 12.03.2019).

8. 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: 12.03.2019).

9. 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.

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: 28.02.2019).

11. 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: 18.03.2019).

12. Рішення «Servulo **& Associados**» («Сервуло та партнери») проти Португалії від 3 вересня 2015 року. URL: https://precedent.in.ua/2016/06/16/servulo-partnery-advokatskaya-kontora-rl-y-drugye-protyv-portugalyy/ (дата звернення: 06.05.2019).

13. Про деякі питання застосування судами України законодавства при дачі дозволів на тимчасове обмеження окремих конституційних прав і свобод людини і громадянина під час здійс-

нення оперативно-розшукової діяльності, дізнання і досудового слідства: постанова Пленуму Верховного Суду України від 28 березня 2008 року № 2. Дата оновлення: 04.06.2010. URL: https://zakon.rada.gov.ua/laws/show/v0002700-08 (дата звернення: 21.05.2019).

14. 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: 12.03.2019).

15. Про національну безпеку України: Закон України від 21 червня 2018 року № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (дата звернення: 01.05.2019).

16. Про основи національної безпеки України: Закон України від 19 червня 2003 року № 964-IV. Втратив чинність 8 липня 2018 року. URL: https://zakon.rada.gov.ua/laws/show/964-15 (дата звернення: 01.05.2019).

17. Про Службу безпеки України: Закон України від 25 березня 1992 року № 2229-XII. Дата оновлення: 02.08.2018. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (дата звернення: 01.05.2019).

Надійшла до редакції 27.05.2019

References

1. Konventsiya pro kiberzlochynnist′, ratyfikovana zakonom vid 07 veresnya 2005 roku № 2824-IV [Convention on Cybercrime, ratified by Law No. 2824-IV of September 7, 2005]. Data onovlennya: 07.09.2005. URL: https://zakon.rada.gov.ua/laws/show/994_575 [in Ukr.].

2. Pro ratyfikatsiyu Konventsiyi pro kiberzlochynnist′: Zakon Ukrayiny vid 07 veresnya 2005 roku № 2824-IV [Ratification of the Convention on Cybercrime: Law of Ukraine of September 7, 2005]. Data onovlennya: 14.10.2010. URL: https://zakon.rada.gov.ua/laws/show/2824-15 [in Ukr.].

3. Dodatkovyy protokol do Konventsiyi pro kiberzlochynnist′, yakyy stosuyet′sya kryminalizatsiyi diy rasyst·s′koho ta ksenofobnoho kharakteru, vchynenykh cherez komp″yuterni systemy, ratyfikovanyy zakonom vid 21 lypnya 2006 roku № 23-V [Additional Protocol to the Convention on Cybercrime Concerning the Criminalization of Racist and Xenophobic Actions Committed through Computer Systems, ratified by Law No. 23-V of 21 July 2006]. URL: https://zakon.rada.gov.ua/laws/show/994_687/conv (data zvernennya: 18.03.2019) [in Ukr.].

4. Konventsiya Orhanizatsiyi Ob″yednanykh Natsiy proty transnatsional′noyi orhanizovanoyi zlo-chynnosti, pryynyata rezolyutsiyeyu 55/25 Heneral′noyi Asambleyi vid 15 lystopada 2000 roku, ratyfikovana zakonom vid 4 lyutoho 2004 roku № 1433-IV [United Nations Convention against Transnational Organized Crime, adopted by General Assembly resolution 55/25 of 15 November 2000, ratified by Law No. 1433-IV of 4 February 2004]. Data onovlennya: 4.02.2004. URL: https://zakon.rada.gov.ua/laws/show/995_789 (data zvernennya: 18.03.2019) [in Ukr.].

5. Kryminal′nyy protsesual′nyy kodeks Ukrayiny: Zakon Ukrayiny vid 13 kvitnya 2012 roku № 4651-VI [Criminal Procedure Code of Ukraine: Law of Ukraine of April 13, 2012 No. 4651-VI]. URL: http://zakon.rada.gov.ua/laws/show/4651-17#n384 (data zvernennya: 30.04.2019) [in Ukr.].

6. Proekt Zakonu pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo posylennya vidpovi-dal′nosti za vchyneni pravoporushennya u sferi informatsiynoyi bezpeky ta borot′by z kiberzlochynnistyu vid 19 chervnya 2015 roku № 2133a [Draft Law on Amendments to Certain Laws of Ukraine on Strengthening Responsibility for Committing Offenses in the Field of Information Security and Combating Cybercrime of June 19, 2015] URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf35l=9 (data zvernennya: 12.03.2019) [in Ukr.].

7. Proekt Zakonu pro vnesennya zmin do deyakykh zakoniv Ukrayiny shchodo posylennya vidpovidal′nosti za vchyneni pravoporushennya u sferi informatsiynoyi bezpeky ta borot′by z kiberzlochynnistyu vid 30 veresnya 2016 roku № 2133a-1 [Draft Law on Amendments to Certain Laws of Ukraine on Strengthening Accountability for Offenses in the Field of Information Security and Combating Cybercrime of September 30, 2016]. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_2?pf3510-1&skl=9 (data zvernennya: 12.03.2019) [in Ukr.].

8. Proekt Zakonu pro vnesennya zmin do deyakykh zakonodavchykh aktiv Ukrayiny shchodo protydiyi zahrozam natsional′niy bezpetsi v informatsiyniy sferi vid 12 lypnya 2017 roku № 6688 [Draft Law on Amendments to Certain Legislative Acts of Ukraine on Countering National Security Threats in the Information Sector of July 6, 2017]. URL: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=62236 (data zvernennya: 12.03.2019) [in Ukr.].

9. Buyadzhy, S.A. (2018) Pravove rehulyuvannya borot′by z kiberzlochynnistyu: teoretyko-pravovyy aspect [Legal regulation of the fight against cybercrime: theoretical and legal aspect]: dys. … kand. yuryd. nauk: 12.00.01 / Klasychnyy pryvatnyy universytet PVNZ Univers. Korolya Danyla. Kyyiv [in Ukr.].

10. Orlov, YU. YU., Chernyavs′kyy, S.S. (2017) Vykorystannya elektronnykh vidobrazhen′ yak dokaziv u kryminal′nomu provadzhenni [Use of electronic reflections as evidence in criminal proceedings]. *Naukovyy visnyk Natsional'noyi akademiyi vnutrishnikh sprav,* 3 (104), 13. URL: https://scientbul.naiau.kiev.ua/article/view/612/616 (data zvernennya: 28.02.2019) [in Ukr.].

11. Pro elektronni dokumenty ta elektronnyy dokumentoobih: Zakon Ukrayiny vid 22 travnya 2003 roku № 851-IV [On electronic documents and electronic document flow: Law of Ukraine of May 22, 2003]. Data onovlennya: 07.11.2018. URL: https://zakon.rada.gov.ua/laws/show/851-15 (data

zvernennya: 18.03.2019) [in Ukr.].

12. Rishennya «Servulo & Associados» («Servulo ta partnery») proty Portuhaliyi vid 3 veresnya 2015 roku [Judgment of Servulo & Associados (Servulo & Partners) against Portugal on 3 September 2015]. URL: https://precedent.in.ua/2016/06/16/servulo-partnery-advokatskaya-kontora-rl-y-drugye-protyv-portugalyy/ (data zvernennya: 06.05.2019) [in Ukr.].

13. Pro deyaki pytannya zastosuvannya sudamy Ukrayiny zakonodavstva pry dachi dozvoliv na tymchasove obmezhennya okremykh konstytutsiynykh prav i svobod lyudyny i hromadyanyna pid chas zdiys-nennya operatyvno-rozshukovoyi diyal′nosti, diznannya i dosudovoho slidstva [On Some Issues of Application by the Courts of Ukraine of Legislation in Issuing Permits for Temporary Restriction of Individual Constitutional Rights and Freedoms of Man and Citizen in the Pursuit of Operational Investigation, Investigation and Pre-Trial Investigation]: postanova Plenumu Ver-khovnoho Sudu Ukrayiny vid 28 bereznya 2008 roku № 2. Data onovlennya: 04.06.2010. URL: https://zakon.rada.gov.ua/laws/show/v0002700-08 (data zvernennya: 21.05.2019) [in Ukr.].

14. Pro poryadok dennyy desyatoyi sesiyi Verkhovnoyi Rady Ukrayiny vos′moho sklykannya [Agenda of the tenth session of the Verkhovna Rada of Ukraine of the Eighth Convocation]: Postanova Verkhovnoyi Rady Ukrayiny vid 7 lyutoho 2019 roku № 2679-VIII. URL: https://zakon.rada.gov.ua/laws/show/2679-viii (data zvernennya: 12.03.2019) [in Ukr.].

15. Pro natsional′nu bezpeku Ukrayiny [On National Security of Ukraine]: Zakon Ukrayiny vid 21 chervnya 2018 roku № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19 (data zvernennya: 01.05.2019) [in Ukr.].

16. Pro osnovy natsional′noyi bezpeky Ukrayiny: Zakon Ukrayiny vid 19 chervnya 2003 roku № 964-IV. Vtratyv chynnist′ 8 lypnya 2018 roku [On the basics of Ukraine's national security: Law of Ukraine of June 19, 2003]. URL: https://zakon.rada.gov.ua/laws/show/964-15 (data zvernennya: 01.05.2019) [in Ukr.].

17. Pro Sluzhbu bezpeky Ukrayiny: Zakon Ukrayiny vid 25 bereznya 1992 roku № 2229-KHII. Data onovlennya: 02.08.2018. [On the Security Service of Ukraine: Law of Ukraine of March 25, 1992]. URL: https://zakon.rada.gov.ua/laws/show/2229-12 (data zvernennya: 01.05.2019) [in Ukr.].

SUMMARY

Zakharko A.V. Analysis of the state of law-making activities on the implementation of the procedural provisions of the Cyber Crime Convention. The criminal procedural regulation of the pre-trial investigation authorities' powers in order to create the conditions for the effective activity of the pre-trial investigation bodies regarding the collection of evidence related to computer data and their processing in electronic information systems has been described. The procedural provisions of the Cybercrime Convention have been analyzed and their comparisons are made with the powers of the prosecution party under the current CPC of Ukraine.

Relevant bills on the implementation of the relevant procedural provisions of the Convention to the CPC of Ukraine have been reviewed.

The current CPC of Ukraine is interpreted as providing for inspection, search of the computer system, its parts, computer media, computer data, penetration (articles 233-237 of the CPC), temporary access to the computer. computer system, part or computer media, copy and save copies of computer data (articles 170, 159 of the CPC).

An analysis of the relevant bills has led to the conclusion that they have the following procedural provisions of the Cybercrime Convention: the preservation of computer information, including by blocking access to relevant information resources; temporary blocking (limitation) of access to a certain (identified) information resource (service) in information and telecommunication networks (systems).

The bills analyzed do not pay sufficient attention to the implementation of the following procedural powers: urgent retention of certain computer data; the obligation of the person to maintain the integrity of the computer data; the obligation of the individual to maintain the confidentiality of the fact; urgent disclosure of data flow; extending a search or similar access to a computer system, part of it, accessible to the first system but physically located outside the object being searched but within the territory of the State to which the pre-trial investigation authority is subject; prohibiting the access or removal of computer data from a computer system that was accessed.

***Keywords**: procedural provisions, Cybercrime Convention, criminal procedural rules, scope of implementation.*