УДК 342.52

МАРУЩАК А.І., *доктор юридичних наук, професор*,
директор Навчально-наукового інституту перепідготовки
та підвищення кваліфікації кадрів СБУ
Національної академії Служби безпеки України

ІНФОРМАЦІЙНО-ПРАВОВІ АСПЕКТИ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Анотація. *У статті досліджуються питання інформаційно-правових аспектів протидії кіберзлочинності в Україні. Сформульовано пропозиції щодо удосконалення інформаційного та кримінального процесуального законодавства з метою підвищення ефективності розслідування кіберзлочинів правоохоронними органами України.*

Ключові слова: *кіберзлочин, правоохоронні органи, інформаційне право, протидія кіберзлочинності.*

Summary. *The article deals with the issues of information law aspects of counteraction to cybercrime in Ukraine. The proposals on improvement of information and criminal procedural legislation are formulated in order to increase the effectiveness of the investigation of cybercrime by law enforcement agencies of Ukraine.*

Keywords: *cybercrime, law enforcement agencies, information law, counteraction to cybercrime.*

Аннотация. *В статье исследуются вопросы информационно-правовых аспектов противодействия киберпреступности в Украине. Сформулированы предложения по усовершенствованию информационного и уголовного процессуального законодательства с целью повышения эффективности расследования киберпреступлений правоохранительными органами Украины.*

Ключевые слова: *киберпреступление, правоохранительные органы, информационное право, противодействие киберпреступности.*

Постановка проблеми. Комп’ютерна або кіберзлочинність набула міжнародних масштабів, кількість злочинів у сфері інформаційних технологій постійно зростає. Серйозне занепокоєння викликає використання та розповсюдження програм-вірусів, “троянів”, фішингових програм, поширення фактів несанкціонованого доступу до державних інформаційних ресурсів, викрадення інформації з баз даних, знищення та модифікація даних у інформаційних системах, перехоплення інформації тощо.

Україна останніми роками дедалі більше відчуває на собі масштаби кібернетичних загроз і їх негативні наслідки. Так, у 2017 році підрозділами Національної поліції України розслідувалось понад 21,7 тис. кримінальних правопорушень у сфері інформаційних технологій. У 2017 році виявлено майже 14 тис. таких кримінальних правопорушень. Розслідувались наступні категорії злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж, відповідальність за які встановлена статтями 16 розділу особливої частини Кримінального кодексу України: за ст. 361 (Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку) КК України – 2606; ст. 361-1 (Створення з метою використання, розповсюдження або збуту шкідливих програм чи технічних засобів, а також їх розповсюдження або збут) КК України – 56; ст. 361-2 (Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-

обчислювальних машинах (комп’ютерах), автоматизованих системах, комп’ютерних мережах або на носіях такої інформації) КК України – 83; 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 – 863, ст. 363 (Порушення правил експлуатації електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку або порядку чи правил захисту інформації, яка в них оброблюється) КК України – 34 та ст. 363-1 (Перешкоджання роботі електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку шляхом масового розповсюдження повідомлень електрозв’язку) КК України – 4.

Крім цього, виявлено кваліфіковані види кримінальних правопорушень й інших категорій, пов’язані з використанням інформаційних технологій, відповідальність за вчинення яких, передбачено ст. 176 (Порушення авторського права і суміжних прав) КК України – 107, ст. 185 (Крадіжка) КК України – 173^1, ч. 3, 4 ст. 190 (Шахрайство) КК України – 419^2, ст. 200 (Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення) КК України – 456, ст. 229 (Незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару) КК України - 32, ст. 231 (Незаконне збирання інформації, що становить банківську таємницю) КК України – 61 та ч. 3, 4, 5 ст. 301 (Ввезення, виготовлення, збут і розповсюдження порнографічних предметів) КК України – 647.

У 10236 або 47 % кримінальних правопорушень про кіберзлочини, досудове розслідування у яких здійснювали слідчі Національної поліції, оголошено про підозру, з них у 9552 або 68 %, що вчинені у поточному році [1].

27 червня 2017 р. відбулася масована кібератака на інформаційно-телекомунікаційні системи державних органів. З метою з’ясування методів реалізації акції кібертероризму, встановлення джерел її походження, виконавців, організаторів і замовників, СБ України організовано взаємодію з партнерськими правоохоронними органами, спеціальними службами іноземних країн та міжнародними організаціями у сфері кібербезпеки. До проведення детального дослідження отриманого тіла вірусу, з’ясування обставин вірусного ураження комп’ютерних мереж об’єктів критичної інфраструктури, можливих негативних наслідків залучено можливості інопартнерів (ФБР США, Національної агенції по боротьбі зі злочинністю (NCA) Великобританії, МІТ Туреччини).

Останні кібератаки на державні органи, установи і підприємства України зумовили посилення заходів кібербезпеки на загальнодержавному рівні. Так, прийнятий Верховною Радою України Закон “Про основні засади забезпечення кібербезпеки України” визначив правові та організаційні основи забезпечення захисту життєво важливих інтересів людини і громадянина, суспільства та держави, національних інтересів України у кіберпросторі, основні цілі, напрями та принципи державної політики у сфері кібербезпеки, повноваження державних органів, підприємств, установ, організацій, осіб та громадян у цій сфері, основні засади координації їхньої діяльності із забезпечення кібербезпеки [2].

Результати аналізу наукових публікацій свідчать про те, що питання інформаційно-правових аспектів протидії кіберзлочинності частково були предметом досліджень. У вітчизняній юридичній літературі науковим розвідкам окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Брижко, В. Бутузов, В. Пилипчук, К. Тітуніна, М. Швець, О. Юрченко та інші. Автор розглядав дотичні питання у контексті розвитку інформаційного права України як науки [3].

Метою статті є розкриття інформаційно-правових аспектів протидії кіберзлочинності в Україні. Робимо акцент на проблемних питаннях виявлення, припинення і розслідування кіберзлочинів, виникнення яких (проблем) пов’язане, по-перше, із сутністю інформації, а, по-друге, із недостатнім правовим регулюванням інформаційної та правоохоронної діяльності.

Виклад основного матеріалу. Насамперед відзначимо, що протидія кіберзлочинності ускладнена недостатнім врахуванням сучасних інформаційних технологій у відповідному інформаційному і кримінальному процесуальному законодавстві. Тому на сьогодні, **“**збирання доказів в електронній формі є достатньо нелегким процесом, що зумовлено складністю об’єктів… не кожний слідчий володіє спеціальними знаннями у сфері комп’ютерних технологій у достатній мірі, щоб успішно організувати розслідування… Тому вилучення та дослідження об’єктів в електронній формі за можливості має проводити фахівець**”** [4].

Складність виявлення, припинення і розслідування кіберзлочинів значною мірою пов’язана із електронною формою інформації. Наприклад, сьогодні користувачі широко використовують хмарні технології зберігання інформації, порядок доступу до якої визначається власником інформації і власником ресурсу для збереження інформації, який може знаходитися (і часто знаходяться) у різних державах під різними юрисдикціями. Відповідно для українських правоохоронців важливо знати і правильно використовувати законодавство тієї держави, де фізично зберігається інформація про факт або сліди кіберзлочину. Знання вимог інформаційного права такої держави дозволяє правильно сформулювати запит щодо надання офіційної правової допомоги, про що йдеться нижче.

З метою виявлення, припинення і розслідування кіберзлочинів існує необхідність суттєвого удосконалення існуючої системи обміну інформацією в режимі реального часу між основними суб'єктами забезпечення кібербезпеки. Активні процеси щодо удосконалення взаємодії правоохоронних органів (насамперед, Кіберполіції та СБ України) з Держспецзв’язком України дещо покращить оперативність розслідування кіберзлочинів, однак не вирішить питань взаємодії двох правоохоронних органів.

Крім того, виявлення, припинення і розслідування кіберзлочинів потребує належної взаємодії не тільки правоохоронних органів між собою, а й з приватними суб’єктами. Наприклад, сьогодні в Україні відсутня загальнодержавна база IP-адрес, існування якої сприяло б забезпеченню негайного розкриття вчинених кіберзлочинів. Адже встановлення унікальної IP-адреси і її зв’язок зі злочинцем (потерпілим) є одним із найважливіших етапів розслідування кіберзлочинів. Проблемним також є той факт, що унаслідок обмеженої кількості IP-адрес провайдери використовують динамічні IP-адреси (Dynamic IP Address) завдяки протоколу динамічного налаштування вузла (Dynamic Host Configuration Protocol – DHCP) [4].

Таку базу IP-адрес, як видається, доцільно створити у межах державно-приватного партнерства Держспецзв’язку з операторами, провайдерами послуг Інтернет-доступу.

Припинення кіберзлочину та ліквідація його наслідків вимагає оперативності. У процесуальному законодавстві багатьох країн-учасниць Конвенції про кіберзлочинність є норми, які передбачають особливий порядок перехоплення і розкриття інформації про рух даних у комп’ютерних системах задля розслідування кіберзлочинів [5].

Однак, відповідно до чинного Кримінального процесуального кодексу України (КПК України) [6] для отримання інформації від операторів і провайдерів, необхідної для припинення злочину або встановлення винних у його вчиненні, ліквідації негативних

наслідків від кримінального правопорушення, зокрема блокування (обмеження) ресурсу з протиправним контентом, правоохоронні органи витрачають значний час для отримання відповідного рішення суду в межах кримінального провадження. Таким чином, і**снує потреба у** наданні додаткових повноважень правоохоронним органам, які здійснюють розслідування кіберзлочинів, пов’язаних із доступом до інформації, яка має значення при розслідуванні кіберзлочинів. Більшість таких повноважень передбачені Конвенцією про кіберзлочинність. Крім того, Указ Президента України від 13.02.17 р. № 32 **“**Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 **“**Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації**”** передбачає розробку законодавчих пропозицій щодо підвищення ефективності протидії злочинам у кіберпросторі [7].

У цьому контексті, зважаючи на особливості інформаційних відносин у кіберпросторі, насамперед, необхідно:

– закріпити визначення поняття цифрових (електронних) доказів;

– передбачити ефективний і оперативний механізм обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу);

– впровадити специфічні умови проведення обшуку і арешту цифрових (електронних) доказів, насамперед, передбачити процесуально значиму можливість копіювання даних.

Підвищить ефективність розслідування кіберзлочинів імплементація у вітчизняне законодавство статей 16-18 Конвенції про кіберзлочинність, а саме невідкладне фіксування і подальше зберігання даних операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сайту, веб-сторінки, тощо) із забезпеченням їх цілісності. Потребують впровадження у вітчизняне законодавство норми статті 19 (Обшук і арешт комп’ютерних даних, які зберігаються) Конвенції про кіберзлочинність шляхом закріплення можливості копіювати електронні дані, здійснювати їх пошук, а також їх блокувати/арештовувати. Відповідні процесуальні дії доцільно здійснювати на підставі ухвали слідчого судді, суду, а фактичні дані, отримані подібними способами вважати допустимими доказами у кримінальному провадженні.

Доволі чутливим для громадянського суспільства, але виправданим з огляду на характер загроз безпеці людини, суспільства і держави в кіберпросторі, є запровадження обмеження (блокування) доступу до інформаційних ресурсів (сервісів), що здійснюватиметься операторами, провайдерами телекомунікацій, постачальниками послуг хостингу, власниками ресурсу (веб-сторінки, веб-сайту тощо) стосовно інформації, що містить ознаки діяння, передбаченого законом України про кримінальну відповідальність на підставі ухвали слідчого судді, суду. Подібний процесуальний захід доцільно застосовувати у вичерпних випадках, а саме щодо ресурсів, через які розповсюджуються або з використанням яких вчиняються: пропаганда війни; публічні заклики, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади; публічні заклики, спрямовані на зміну меж території або державного кордону України на порушення порядку, встановленого Конституцією України; дитяча порнографія; шахрайства, яке вчиняється з використанням інформаційно-телекомунікаційних систем; незаконне розповсюдження зброї, бойових припасів або вибухових речовин; незаконне розповсюдження наркотичних засобів, психотропних речовин, їх аналогів чи прекурсорів або фальсифікованих лікарських засобів.

Безумовно існує потреба у законодавчій регламентації механізмів сприяння правоохоронним органам України у формі надання необхідної інформації з метою

підвищення ефективності розслідування кіберзлочинів. Частково відповідні відносини врегульовано статтею 11 Закону України “Про основні засади забезпечення кібербезпеки України”, яка містить декларативну норму про обов’язок державних і приватних суб’єктів сприяти суб’єктам забезпечення кібербезпеки, повідомляти відомі їм дані щодо загроз національній безпеці з використанням кіберпростору або будь-яких інших кіберзагроз об’єктам кібербезпеки, кібератак та/або обставин, інформація про які може сприяти запобіганню, виявленню і припиненню таких загроз, протидії кіберзлочинам, кібератакам та мінімізації їх наслідків [2, ст. 11]. Разом з тим, законодавство України (у статті 39 Закону України **“**Про телекомунікації**”** [8]) має передбачати конкретні форми такого сприяння. Наприклад, з метою забезпечення можливості ідентифікації особи користувача пропонується закріпити обов’язок операторів, провайдерів телекомунікаційних послуг мати список своїх користувачів і надавати його правоохоронним органам на письмову вимогу останніх.

Доцільно також передбачити обов’язок операторів, провайдерів зберігати електронні дані із забезпеченням їх цілісності та неспростовності, у тому числі дані про рух трафіка, а також обов’язок обмежувати доступ своїх абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, веб-сайту, веб-сторінки, через які розповсюджується злочинний контент.

Розслідування кіберзлочинів вимагає швидкого аналізу та збереження електронних даних. Відповідно до принципів міжнародного права тільки правоохоронні органи держави можуть проводити слідчі дії на її території. Оскільки, нерідко місце вчинення, знаряддя злочину, потерпілі і злочинець можуть знаходитися під різною територіальною юрисдикцією, виникає необхідність багатьох формальних погоджень, що значно уповільнює розслідування транснаціональних кіберзлочинів. Тому існує потреба у більш інтенсивному міжнародному співробітництві у порівнянні з боротьбою з будь-якими іншими проявами транснаціональної злочинності.

Новітнє законодавство України у сфері кібербезпеки передбачає можливість надання правоохоронними органами інформації з питань, пов’язаних із боротьбою з міжнародною кіберзлочинністю, іноземній державі на підставі запиту, навіть без попереднього запиту іноземної держави, якщо це не перешкоджає проведенню досудового розслідування чи судового розгляду справи і може сприяти компетентним органам іноземної держави у припиненні кібератаки, своєчасному виявленні і припиненні кримінального правопорушення з використанням кіберпростору [2, ст. 14]. Залишається сподіватися, що на принципах взаємності інші держави світу передбачатимуть подібну можливість оперативного надання інформації з метою розслідування кіберзлочинів.

На сьогодні ж, відповідно до ст. 541 КПК України, таке співробітництво здійснюється за принципами міжнародної правової допомоги – тобто проведення компетентними органами однієї держави процесуальних дій, виконання яких необхідне для досудового розслідування, судового розгляду або для виконання вироку, ухваленого судом іншої держави або міжнародною судовою установою [6, ст. 541]. Угода між Україною та Європолом про оперативне та стратегічне співробітництво надає змогу правоохоронним органам України через Департамент міжнародного співробітництва Нацполіції (яка визначена головним органом взаємодії з Європолом) здійснювати інформаційний обмін з Європолом, зокрема направляти запити на інформацію, необхідну для розслідування злочинів.

Однак, потребує удосконалення протокол офіційної правової допомоги з урахуванням норм національного законодавства для ефективного розслідування

кіберзлочинів щодо вилученої та збереженої інформації у електронному (цифровому) вигляді з метою оперативного отримання такої інформації.

Висновки.

Розуміння інформаційно-правових проблем протидії кіберзлочинності, а також можливостей їх вирішення підвищить ефективність розслідування кіберзлочинів правоохоронними органами України. Для цього існує необхідність:

деталізації законодавства, яке б відображало положення Конвенції про кіберзлочинність, щодо отримання електронних доказів, обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу), специфічних умов проведення обшуку і арешту цифрових (електронних) доказів;

закріплення механізмів сприяння правоохоронним органам України операторів, провайдерів щодо забезпечення цілісності та неспростовності електронних даних, обмеження доступу абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, веб-сайту, веб-сторінки, через які розповсюджуються злочинний контент тощо;

створення у межах державно-приватного партнерства загальнодержавної бази IP-адрес для забезпечення негайного розкриття вчинених кіберзлочинів;

удосконалення протоколу офіційної правової допомоги з урахуванням норм національного законодавства для ефективного розслідування кіберзлочинів щодо вилученої та збереженої інформації у електронному (цифровому) вигляді;

використання правоохоронними органами України механізмів, передбачених Угодою між Україною та Європолом про оперативне та стратегічне співробітництво у напрямку оперативного (через глобальну захищену міжнародну мережу електронного зв'язку) отримання інформації про кіберзлочини і кіберзлочинців.

Перспективним напрямком у зв’язку з означеними проблемами є регулярне підвищення кваліфікації слідчих та інших задіяних співробітників правоохоронних органів з метою вивчення актуальних питань тактики проведення слідчих дій для отримання електронних доказів при розслідуванні кіберзлочинів.

Використана література

1. Офіційні відомості Національної поліції України. – Режим доступу : //www.npu.gov.ua

2. Про основні засади забезпечення кібербезпеки України : Закон України. – Режим доступу : http://zakon3.rada.gov.ua

3. Марущак А.І. Пріоритети розвитку інформаційного права України // Інформація і право. – № 1(1)/2011. – С. 20-24.

4. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М.В. Гребенюк, Г.В. Попов, В.Д. Гавловський, М.В. Гуцалюк, В. Г. Хахановський та ін.] ; за заг. ред. М.В. Гребенюка. – К. : МНДЦ при РНБО України, 2017. – 76 с.

5. Конвенція про кіберзлочинність від 23.11.01 р. // Офіційний вісник України. – 2007. – № 65. – Ст. 253.

6. Кримінальний процесуальний кодекс України від 13.04.12 р. // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.

7. Про рішення Ради національної безпеки і оборони України від 29.12.16 р. **“**Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації**” :** Указ Президента України від 13.02.17 р. № 32. – Режим доступу : http://zakon3.rada.gov.ua

8. Про телекомунікації : Закону України від 18.11.03 р. // Відомості Верховної Ради України (ВВР). – 2004. – № 12. – Ст. 155.

~~~~~~~~~~~~~ * * * ~~~~~~~~~~~~~
~~~~~~~~~~~~~