МАРУЩАК
Анатолій Іванович
martol_law@ukr.net

д.ю.н., професор, директор Навчально-наукового інституту перепідготовки та підвищення кваліфікації кадрів СБУ, Національна академія Служби безпеки України

УДК 342.52

ПРОБЛЕМИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ В УКРАЇНІ

PROBLEMS OF CIBERCRIMES INVESTIGATION IN UKRAINE

У статті досліджуються проблеми правового регулювання і правозастосування, які не дозволяють ефективно розслідувати кіберзлочини в Україні. Зроблено висновок про необхідність подальшої імплементації положень Конвенції про кіберзлочинність, регламентації механізмів сприяння правоохоронним органам України операторів, провайдерів телекомунікаційних послуг, а також використання можливостей міжнародного співробітництва у розслідуванні кіберзлочинів.

В статье исследуются проблемы правового регулирования и правоприменения, которые не позволяют эффективно расследовать киберпреступления в Украине. Сделан вывод о необходимости дальнейшей имплементации положений Конвенции о киберпреступлениях, регламентации механизмов содействия правоохранительным органам Украины операторов, провайдеров телекоммуникационных услуг, а также использование возможностей международного сотрудничества в расследовании киберпреступлений.

The article deals with problems of legal regulation and enforcement, which do not allow to investigate cybercrime effectively in Ukraine. The conclusion is made on the necessity of further implementation of the provisions of the Convention on cybercrime, the regulation of mechanisms for the operators, providers of telecommunication services assistance to law enforcement agencies of Ukraine, as well as the use of opportunities for international cooperation in the investigation of cybercrime.

Ключові слова: *кіберзлочин, правоохоронні органи, розслідування, кібербезпека, Конвенція про кіберзлочинність*

Ключевые слова: *киберпреступление, правоохранительные органы, расследование, кибербезопасность, Конвенция о киберпреступности*

Keywords: *cybercrime, law enforcement agencies, investigation, cybersecurity, Cybercrime Convention*

ПОСТАНОВКА ПРОБЛЕМИ

Розвиток інформаційних технологій зумовив виникнення нових загроз національній і міжнародній безпеці. Україна відчула на собі масштаби кібернетичних загроз і їх негативні наслідки. Останні кібератаки на державні органи, установи і підприємства України зумовили посилення заходів кібербезпеки на загальнодержавному рівні.

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 [1].

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, несанкціонований доступ до державних інформаційних ресурсів, знищення та модифікація даних у інформаційних системах, викрадення інформації з баз даних, перехоплення інформації тощо. Набуває поширення шахрайство у сфері інтернет-комерції, зокрема лише у 2016 р. кількість зафіксованих в Україні злочинних сайтів зросла в 4,5 рази – з 38 до 174. Тільки за день роботи один такий підроблений сайт може виманити дані декількох тисяч платіжних карт користувачів [2].

Результати аналізу наукових публікацій свідчать про те, що питання розкриття проблем, які виникають при розслідування кіберзлочинів в Україні фрагментарно були предметом досліджень провідних науковців. У вітчизняній юридичній літературі дослі-

дженню окремих питань цієї проблематики в різні часи приділяли увагу такі фахівці, як В. Бутузов, К. Тітуніна, В. Шеломенцев, О. Юрченко та інші. Автор розглядав дотичні питання захисту інформаційних ресурсів держави [3].

МЕТОЮ СТАТТІ є науково-теоретичне обґрунтування проблем правового регулювання і правозастосування, які не дозволяють ефективно розслідувати кіберзлочини в Україні.

ВИКЛАД ОСНОВНОГО МАТЕРІАЛУ

Насамперед, звернемо увагу на питання термінології і новітні законодавчі положення щодо суб’єктів національної системи кібербезпеки в Україні.

Рада Європи у листопаді 2001 р. прийняла Конвенцію про кіберзлочинність (далі – Конвенція), у якій використано термін «cybercrime» (кіберзлочин). Відповідно до положень Конвенції кіберзлочини можливо поділити на такі групи:

– злочини проти конфіденційності, цілісності та доступності комп’ютерних даних і систем, такі як незаконний доступ, нелегальне перехоплення, втручання у дані, втручання у систему, зловживання пристроями;

– злочини підробки і шахрайства, пов’язані з комп’ютерами, а саме навмисне вчинення, без права на це, введення, зміни, знищення або приховування комп’ютерних даних, яке призводить до створення недійсних даних, або навмисне вчинення, без права на це, дій, що призводять до втрати майна іншої особи;

– злочини, пов’язані зі змістом даних, а саме з дитячою порнографією;

– злочини, пов’язані з порушенням авторських та суміжних прав [3];

– злочини з поширення расистського та ксенофобного матеріалу через комп’ютерні системи [4].

Закон України «Про основні засади забезпечення кібербезпеки України» вперше дає визначення поняттю «кіберзлочин (комп’ютерний злочин)» – суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [1, ст. 1]. Фактично, в поняття кіберзлочин включено усі види злочинів, скоєні в інформаційно-телекомунікаційній сфері, де інформація, технічні засоби можуть бути предметом злочинних посягань, або середовищем, в якому скоюється злочин, чи знаряддям його вчинення.

Відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» основними суб’єктами національної системи кібербезпеки в Україні є: Державна служба спеціального зв’язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України.

Основні завдання щодо запобігання, виявлення, припинення та розкриття кіберзлочинів виконує Національна поліція України, яка також забезпечує захист прав і свобод людини і громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; Служба безпеки України здійснює запобігання, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснює контррозвідувальні та оперативно-розшукові заходи, спрямовані на боротьбу з кібертероризмом та кібершпигунством, негласно перевіряє готовність об’єктів критичної інфраструктури до можливих кібератак та кіберінцидентів; протидіє кіберзлочинності, наслідки якої можуть створити загрозу життєво важливим інтересам держави; розслідує кіберінциденти та кібератаки щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечує реагування на кіберінциденти у сфері державної безпеки [1, ст. 8].

Особливе місце у національній системі кібербезпеки в Україні займає урядова команда реагування на комп’ютерні надзвичайні події України CERT-UA, завданнями якої окрім іншого є:

– накопичення та проведення аналізу даних про кіберінциденти, ведення державного реєстру кіберінцидентів;

– підготовка та розміщення на своєму офіційному веб-сайті рекомендацій щодо протидії сучасним видам кібератак та кіберзагроз;

– взаємодія з правоохоронними органами, забезпечення їх своєчасного інформування про кібератаки;

– взаємодія з іноземними та міжнародними організаціями з питань реагування на кіберінциденти, зокрема в рамках участі у Форумі команд реагування на інциденти безпеки FIRST із сплатою щорічних членських внесків;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об’єктів кіберзахисту [1, ст. 9].

Забезпечення функціонування CERT-UA здійснює Державна служба спеціального зв’язку та захисту інформації України. На сьогодні в Україні створюються відомчі команди реагування на комп’ютерні надзвичайні події (остання створена у Національному банку України).

Проблеми розслідування кіберзлочинів значною мірою повязані з транснаціональністю мережі Інтернет і у відсутністю механізмів контролю, необхідних для виконання правоохоронної функції. Відсутність юрисдикційних кордонів у кіберпросторі зумовила зростання злочинності та довгий час фактично унеможливлювала здійснення контролю у сфері використання кіберпростору для вчинення злочинів.

Із збільшенням числа користувачів Інтернет та засобів доступу до мережі, збільшується потенційна можливість стати жертвою використання інформаційних технологій в злочинних цілях. Електронні дані передаються з однієї держави в іншу за кілька секунд, а контролювати передачу даних, з урахуванням їх обсягу та кількості користувачів фактично не неможливо. Ризик здійснення множинних злочинів збільшується без фінансових витрат у зв’язку з автоматизацією процесів в ПЕОМ та мережах. Використання низки серверів у процесі вчинення кіберзлочинів,

вчинення їх шляхом виходу в Інтернет через точки загального доступу, з відкритих бездротових мереж Wi-Fi тощо значно ускладнює розслідування кіберзлочинів.

Останніми роками Інтернет і засоби доступу до нього розвиваються набагато швидше від правових засобів захисту приватності, власності, гідності людини, інтересів суспільства і держави. Вразливість персональної інформації в соціальних мережах, технології хмарної обробки даних, автоматизація кібератак – проблеми, які не знайшли достатнього правового регулювання на національному і міжнародному рівнях. Зважаючи на викладені обставини, правові можливості розслідування кіберзлочинів дуже обмежені, насамперед, технологічно. І хоча нагальні питання технічного оснащення зазначених вище команд реагування високотехнологічними засобами виявлення і протидії кібератакам поступово вирішуються в Україні переважно за рахунок підтримки зарубіжних партнерів, можливості з оперативного виявлення і протидії вчиненню такої категорії злочинів обмежені.

Іншою проблемою є недостатність повноважень правоохоронних органів, які здійснюють розслідування кіберзлочинів. Указ Президента України від 13.02.2017 № 32 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації» передбачає розробку законодавчих пропозицій щодо підвищення ефективності протидії злочинам у кіберпросторі [5].

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.

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. Немає чіткого змісту у поняття цифрових (електронних) доказів. Значно підвищить ефективність розслідування кіберзлочинів імплементація у вітчизняне законодавство ст. 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 ст. 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.

Тому доцільною є необхідність:

– закріплення визначення поняття цифрових (електронних) доказів;

– передбачення ефективного і оперативного механізму обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу), який використовується зі злочинною метою;

– впровадження специфічних умов проведення обшуку і арешту цифрових (електронних) доказів, насамперед, передбачення процесуально значимої можливості копіювання даних.

Існує також потреба налагодження взаємодії СБ України і Нацполіції України під час розслідування кіберзлочинів шляхом розробки і затвердження спільного наказу про взаємодію у цій сфері. Адже відпрацювання Службою безпеки України лише доручень слідчих Нацполіції України щодо здійснення аналізу та дослідження цифрових даних, здійснення відповідної експертизи недостатньо для забезпечення безпеки державних інформаційних ресурсів.

Взаємодія правоохоронних органів з Держспецзв'язком України останнім часом значно активізується, що покращить оперативність розслідування кіберзлочинів, однак не вирішить питань взаємодії СБ України і Нацполіції України.

Серед заходів покращення результативності розслідування кіберзлочинів доцільним є також закріплення в органах прокуратури та судах спеціалізації відповідних співробітників з питань кіберзлочинів. Для цього варто здійснювати регулярні зустрічі та наради з представниками прокуратури і судів задля обговорення проблемних питань у розслідуванні, насамперед, документуванні таких злочинів.

Ще однією проблемою правового регулювання, яка знижує ефективність розслідування кіберзлочинів

в Україні є недостатня регламентація механізмів сприяння правоохоронним органам України.

Частково відповідні відносини врегульовано ст. 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 [1, ст. 11].

Разом з тим, законодавство України (у ст. 39 Закону України «Про телекомунікації» [7]) 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.

Проблемним у цьому контексті залишається питання формування переліку інформаційно-телекомунікаційних систем об’єктів критичної інфраструктури держави відповідно до рішення Ради національної безпеки і оборони України від 29 грудня 2016 року «Про загрози кібербезпеці держави та невідкладні заходи з їх нейтралізації», введеного в дію Указом Президента України від 13 лютого 2017 року № 32 [5], що суттєво ускладнює попередження злочинів на таких об’єктах.

Існують також проблеми міжнародного співробітництва правоохоронних органів, адже розслідування кіберзлочинів вимагає швидкого аналізу та збереження електронних даних. Відповідно до принципів міжнародного права тільки правоохоронні органи держави можуть проводити слідчі дії на його 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.

Конвенція про кіберзлочинність не є універсальним міжнародним інструментом, незважаючи на те, що за своїм впливом вийшла далеко за межі Європейського Союзу. Відповідно, загальносвітового правового акту, який би визначив принципи співробітництва при розслідуванні кіберзлочинів, на даний час немає. Подібні питання, логічно, мають бути врегульовані на рівні Конвенції ООН.

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 [1, ст. 14]. Залишається сподіватися, що на принципах взаємності інші держави світу передбачатимуть подібну можливість оперативного надання інформації з метою розслідування кіберзлочинів в Україні.

На сьогодні ж, відповідно до ст. 541 Кримінального процесуального кодексу 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.

ВИСНОВКИ

Ефективність співробітництва правоохоронних органів України у розслідуванні кіберзлочинів безпосередньо залежить від деталізованого законодавства, яке б відображало положення Конвенції про кіберзлочинність. Звичайно мають дотримуватися права людини і громадянина при розробці такого законодавства, зокрема у частині отримання електронних доказів, обмеження (блокування) певного інформаційного ресурсу (інформаційного сервісу), специфічних умов проведення обшуку і арешту цифрових (електронних) доказів. Існує також потреба розробки і затвердження спільного наказу про взаємодію між СБ України і Нацполіцією України під час розслідування кіберзлочинів.

Законодавчої регламентації потребують механізми сприяння правоохоронним органам України операторів, провайдерів щодо забезпечення цілісності та неспростовності електронних даних, обмеження доступу абонентів до інформаційного ресурсу (інформаційного сервісу), адреси мережі Інтернет, вебсайту, веб-сторінки, через які розповсюджується злочинний контент тощо.

Міжнародне співробітництво у розслідуванні кіберзлочинів (насамперед використання механізмів, передбачених Угодою між Україною та Європолом про оперативне та стратегічне співробітництво) вважаємо основним напрямом подолання існуючого розриву між розвитком інформаційних технологій та

відповідного правового регулювання, спрямованого на захист інтересів особи, суспільства і держави.

Список використаних джерел

1. Закон України «Про основні засади забезпечення кібербезпеки України». Режим доступу: http://zakon3.rada.gov.ua.

2. Офіційні відомості Національної поліції України. Режим доступу: www.npu.gov.ua.

3. Марущак А.І. Інформаційні ресурси держави: зміст та проблема захисту // Правова інформатика. – 2009. – № 1. – С. 64-70.

3. Конвенція про кіберзлочинність від 23.11.2001 // Офіційний вісник України. – 2007. – № 65. – Ст. 253.

4. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи від 28.01.2003 // Офіційний вісник України. – 2010. – № 56. – Ст. 1920.

5. Указ Президента України від 13.02.2017 № 32 «Про рішення Ради національної безпеки і оборони України від 29 грудня 2016 р. «Про загрози кібербезпеки держави та невідкладні заходи щодо їх нейтралізації» // Офіційний вісник України. – 2017. – № 16. – Ст. 464.

6. Кримінальний процесуальний кодекс України від 13.04.2012 // Офіційний вісник України. – 2012. – № 37. – Ст. 1370.

7. Закону України «Про телекомунікації» від 18.11.2003 // Відомості Верховної Ради України. – 2004. – № 12. – Ст. 155.