УДК 343.13

КІБЕРЗЛОЧИННІСТЬ В УКРАЇНІ: АНАЛІЗ ДІЄВОСТІ СПОСОБІВ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ І НАПРЯМИ ЇХ ВДОСКОНАЛЕННЯ

CYBER CRIME IN UKRAINE: ANALYSIS OF EFFECTIVENESS OF WAYS OF INVESTIGATION OF CYBERCRIMES AND DIRECTION OF THEIR IMPROVEMENT

Яцик Т.П., к.ю.н., доцент,
доцент кафедри кримінального процесу та криміналістики
Національний університет державної фіскальної служби України

Кисла К.О., студентка
Національний університет державної фіскальної служби України

Пушкарьова Т.М., студентка
Національний університет державної фіскальної служби України

Розглянуто питання стосовно якості розслідування кіберзлочинів в Україні шляхом проведення аналізу законодавчої бази на предмет якісності врегулювання правовідносин у цій сфері, окреслено перелік способів і засобів, які застосовуються для формування доказової бази, зокрема наведено поетапне проходження комп'ютерно-технічної експертизи.
Ключові слова: кіберзлочин, кіберпростір, кіберзагроза, кіберзахист, кібербезпека, кіберполіція, Стратегія боротьби, комп'ютерно-технічна експертиза.

Рассмотрены вопросы относительно качества расследования киберпреступлений в Украине путем проведения анализа законодательной базы на предмет качественности урегулирования правоотношений в данной сфере, намечен перечень способов и средств, применяемых при формировании доказательной базы, в частности приведено поэтапное прохождение компьютерно-технической экспертизы.
Ключевые слова: киберпреступление, киберпространство, киберугроза, киберзащита, кибербезопасность, киберполиция, Стратегия борьбы, компьютерно-техническая экспертиза.

Over the past ten years, the number of Internet users has increased in Ukraine, because it is accessible and convenient for everyone. Statistics show that our country is one of the leaders in the number of cyberattacks around the world. Ukraine turned out to be fourth in the sector after Russia, Taiwan and Germany. Therefore, the issue of studying the problem of the growth of cybercrime, and especially the reasons that allow it to do so, becomes relevant. That is why the article deals with issues related to the quality of the investigation of cybercrime in Ukraine, through the analysis of the legislative framework, on the quality of the settlement of legal relations in this area. Thus, the main focus is on the Strategy of the Cybersecurity of Ukraine, as it establishes not only methods for combating cybercrime, but also the main subjects on which these duties are assigned. Therefore, based on the provisions of this normative act, the cyberpolice, the Ministry of Defense of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the Security Service of Ukraine, the National Bank of Ukraine, and intelligence agencies are the subjects of counteraction and criminality in cyberspace in Ukraine. In addition, the list of methods and means used for the formation of the evidence base is outlined, in particular, the step-by-step passing of the computer-technical expertise and its classification, depending on the tasks which are planned to be resolved as a result of the concrete examination, are outlined. As a result, positive and negative aspects are revealed in the course of the study, in particular, the latter can be attributed to the fact that the norms of domestic legislation remain only on paper and are not carried out in practice, although in their content they do not infer the norms of European legislation. And as a positive feature, the creation of a specialized Government response team on computer emergencies of Ukraine, such as CERT-UA, could be called positive.
Key words: cybercrime, cyberspace, cyber threat, cyber defense, cyber security, cyber police, Combat strategy, computer-technical expertise.

Сьогодення важко уявити без використання різноманітних інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки та новітніх засобів комунікації. Проте поряд із розвитком інформаційної сфери набуває більшого значення проблема комп'ютерної злочинності. Хакерські атаки стають буденним явищем і завдають значних збитків як особам, так і державі.

За останні десять років в Україні зросла кількість користувачів мережі Інтернет, бо це доступно і зручно для кожного. Статистика свідчить, що наша країна є одним із лідерів за кількістю кібератак у всьому світі. Україна виявилася у цій сфері на 4 місці після Росії, Тайваню і Німеччини. Так, станом на листопад 2018 р., за даними Генеральної прокуратури, було зареєстровано 2 245 правопорушень, із яких за 129 кримінальними провадженнями було винесено вирок, а всі інші були або призупинені, або рішення за ними не було прийнято [1].

З огляду на вищенаведену статистику Україна розробила стратегію кібербезпеки, головною метою якої є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Відповідно до цього нормативно-правового акта головним органом, що відповідає за інформаційну безпеку, є підрозділ Національної поліції – кіберполіція. Крім того, обов'язки щодо протидії кіберзлочинності покладаються на Міністерство оборони України, Державну службу спеціального зв'язку та захисту інформації України, Службу безпеки України, Національний банк України, розвідувальні органи [2].

Стратегія розвитку кібербезпеки України передбачає, що основними напрямами забезпечення безпеки у кіберпросторі України є:

– розвиток безпечного, стабільного і надійного кіберпростору, тобто створення єдиної нормативно-правової бази і доведення її до широких мас із метою підвищення рівня обізнаності населення.

– кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, тобто вироблення ефективної методики протидії на рівні державних і місцевих органів;

– кіберзахист критичної інфраструктури – передбачає розроблення єдиного механізму державно-приватного партнерства у запобіганні кіберзагрозам;

– розвиток потенціалу сектору безпеки й оборони у всі попередні категорії і зв'язує їх у єдиний комплекс. Послідовно визначаються апаратно-технічні засоби та програми, що керують ними. Досліджуються інформаційні дані, якими оперують користувачі. Виявляється, як зв'язуються і функціонують окремі станції в мережевому оточенні.

Визначившись із видами експертиз, необхідно простежити алгоритм їх проведення. Доцільно виділити такі етапи організації процесу комп'ютерно-технічної експертизи:

1. Отримання дозволу про призначення експертизи – ці дії вважаються законними у разі отримання ухвали слідчого судді. Судова експертиза може бути організована за особистою ініціативою учасників судочинства, наприклад, позивачем, відповідачем, обвинуваченим, потерпілим, адвокатом, або за клопотанням прокурора чи слідчого за погодженням із прокурором. Після схвалення запиту складається список питань, на які фахівець повинен дати розгорнуту відповідь у строки, відповідні ухвалі.

2. Направлення комп'ютерної техніки і програмних продуктів до вказаного в ухвалі слідчого судді експертного центру.

3. Безпосереднє проведення досліджень і надання відповідей на поставлені питання визначені у Наказі Міністерства юстиції України.

4. Отримання висновку експерта. За неможливості дати висновок експерт зобов'язаний скласти пояснювальну записку, в якій повинен надати роз'яснення причин відмови від експертизи, до найбільш поширених можна віднести непридатність матеріалів і об'єктів досліджень; недостатність кваліфікованих кадрів; відсутність сучасних технологій, що не дозволяє дати відповідь на завдання експертизи.

Незважаючи на значні недоліки у правовому регулюванні кіберпростору в Україні, можна виокремити і позитивні аспекти. Так, наприклад, правоохоронними органами України, США, Великої Британії, Японії, Філіппін, Індонезії, Малайзії було проведено такі операції:

– «секс Торшн», внаслідок якої затримано 56 осіб, ліквідовано 4 транснаціональні кримінальні угруповання;

– «Зевс», завданням якої було знешкодження міжнародної організованої злочинної групи, котра з метою викрадення фінансових реквізитів і доступу до банківських рахунків розповсюджувала шкідливе програмне забезпечення «Зевс». Під час операції знешкоджено інфраструктуру мережі, що включала понад 40 тис. інфікованих комп'ютерів і серверів, левова частка яких знаходилася на території України. Спричинені збитки понад 300 млн доларів. Члени організованого злочинного угруповання – хакери з Одеси та Харкова на чолі з громадянином Російської Федерації [4, с. 65–70].

Крім того, з 2018 р. в Україні запрацювала Урядова команда реагування на комп'ютерні надзвичайні події України CERT-UA, яка у своїй діяльності підпорядковується Державній службі спеціального зв'язку та захисту інформації України. Правова регламентація діяльності міститься у Законі України «Про основні засади забезпечення кібербезпеки України» від 21 червня 2018 р. Так, основними завданнями центру є:

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

– надання власникам об'єктів кіберзахисту практичної допомоги з питань запобігання, виявлення й усунення наслідків кіберінцидентів щодо цих об'єктів;

– організація та проведення практичних семінарів з питань кіберзахисту для суб'єктів національної системи кібербезпеки та власників об'єктів кіберзахисту;

– підготовка та розміщення на своєму офіційному вебсайті рекомендацій щодо протидії сучасним видам кібератак і 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 зі сплатою щорічних членських внесків;

– взаємодія з українськими командами реагування на комп'ютерні надзвичайні події, а також іншими підприємствами, установами й організаціями незалежно від форми власності, які провадять діяльність, пов'язану із забезпеченням безпеки кіберпростору;

– опрацювання отриманої від громадян інформації про кіберінциденти щодо об'єктів кіберзахисту;

– сприяння державним органам, органам місцевого самоврядування, військовим формуванням, утвореним відповідно до закону, підприємствам, установам та організаціям незалежно від форми власності, а також громадянам України у вирішенні питань кіберзахисту та протидії кіберзагрозам [5].

До досягнень CERT-UA можна віднести їх спільне зі Службою зовнішньої розвідки України виявлення нової модифікації шкідливого програмного забезпечення типу Pterodo на комп'ютерах державних органів України, яка, ймовірно, є підготовчим етапом для проведення кібератаки. Такий вірус збирає дані про систему, регулярно відправляє їх на командно-контрольні сервери й очікує подальших команд. Також було попереджена спроба вчинення кіберзлочину у формі фішингу за допомогою електронного листа з прикріпленим файлом – документом із розширенням «docx», який приховано завантажує інший документ легальним чином, але вже з макросами, котрі завантажують payload [6].

Проте проблемними для України залишаються багато питань, зокрема стосовно технічного оснащення слідчої групи. На нашу думку, доцільно паралельно з традиційними криміналістичними валізами запровадити спеціалізоване науково-технічне спорядження для виявлення, фіксації та відбору інформаційних слідів на місці скоєння злочину. Так, наприклад, необхідно створити спеціалізоване програмне забезпечення, яке б могло аналізувати кіберзлочини, допомагати виявляти та досліджувати докази стосовно вчинення цих злочинів.

Наступне питання – проведення експертиз стосовно слідчих негласних розшукових дій, оскільки законом не визначено, як і хто має їх проводити. Судова експертиза вважається основним видом використання спеціальних знань у розслідуванні комп'ютерних злочинів, призначається і проводиться після порушення кримінальної справи з дотриманням вимог ст. 75–77 та 196 КПК України. Перелік експертиз, що можуть проводитися у справах про комп'ютерні злочини, досить широкий. Це і традиційні експертизи – трасологічна, дактилоскопічна, техніко-криміналістична, експертиза документів, судово-економічна, і спеціалізовані – комп'ютерно-технічна та програмно-технічна, які відіграють провідну роль у розслідуванні злочинів вказаної категорії. Очевидно, що виконувати це повинен спеціаліст, однак до завдань із технічної допомоги спеціаліста, перелічених у ч. 2 ст. 71 КПК України, вказані дії не віднесено, проте можливість залучення таких спеціалістів імовірно визначена законодавством у п. 6 ст. 246 КПК України, яким передбачено участь у проведенні таких дій, крім перелічених у ньому процесуальних осіб, ще й «інших» [7].

Крім того, практика свідчить, що правоохоронні органи та суди в питаннях кримінального провадження щодо кіберзлочинів часто діють за старими, усталеними практиками, що не сприяють зібранню доказової бази чи об'єктивному вирішенню справи. Прикладом є Ухвала слідчого судді Печерського районного суду м. Києва 28 листопада 2016 р. у справі № 757/58671/16-к про накладення арешту на грошові кошти, розміщені на рахунках

(ідентифікаторах) електронної платіжної системи «Вебмані.юей», скасувати який вдалося лише завдяки грамотній позиції адвоката, котрий доніс до суду розуміння того, що рахунки «Вебмані.юей» не містять грошових коштів, оскільки ця платіжна система не передбачає обігу грошових коштів, тому фактично на вказаних рахунках розміщена інформація про облік та електронний обмін титульних знаків, які мають виражену вартість у грошовому еквіваленті та якими користувачі системи можуть здійснювати оплату за товари та послуги тощо, але аж ніяк не грошові кошти. Тому з огляду на вищенаведену інформацію необхідно звернути увагу на такий аспект, як профільне навчання кадрів відповідних органів стосовно кіберсфери. Так, у США це є першочерговою дією, оскільки від здібностей суб'єктів розслідування залежить, чи буде розкрито злочин і чи понесе винний відповідальність за вчинене протиправне діяння [8].

Отже, проаналізувавши систему заходів протидії кіберзлочинності в Україні, можна дійти висновку, що більшість норм, передбачених Законом України «Про основні засади забезпечення кібербезпеки України», Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 р. «Про Стратегію кібербезпеки України» від 15 березня 2016 р. № 96/2016», Законом України «Про Державну службу спеціального зв'язку та захисту інформації України», Законом України «Про телекомунікації» тощо, залишаються тільки на папері і не використовуються на практиці, хоча за своїм змістом вони не поступаються нормам європейського законодавства.

ЛІТЕРАТУРА

1. Статистика Генеральної прокуратури України. URL: https://www.gp.gov.ua/ua/stst2011.html?dir_id=113656&libid=100820&c=edit&_c=fo#.

2. Стратегія кібербезпеки України. URL: http://zakon.rada.gov.ua/laws/ show/96/2016#n11.

3. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень. Наказ. URL: https://zakon.rada.gov.ua/laws/ show/z0705-98.

4. Демедюк С.В., Демедюк Т.С. Міжнародний досвід протидії кіберзлочинності. Вісник ХНУВС. 2014. № 4 (67). С. 65–75.

5. Закон України «Про основні засади забезпечення кібербезпеки України». URL: http://zakon.rada.gov.ua/laws/show/2163-19.

6. Computer Emergency Response Team of Ukraine. URL: https://cert.gov.ua/news/46.

7. Кримінальний процесуальний кодекс України. URL: http://zakon.rada.gov.ua/laws/show/4651-17.

8. Кібезлочинність – правовий аспект. URL: http://ukrainepravo.com/legal_publications/essay-on-it-law/it_law_karachevska_cybercrime/.