УДК 343.98
DOI https://doi.org/10.32782/2524-0374/2021-12/99

ОСОБЛИВОСТІ ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ ПІД ЧАС РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ: МІЖНАРОДНИЙ ДОСВІД

PECULIARITIES OF THE USING SPECIAL KNOWLEDGE DURING THE INVESTIGATION OF CYBERCRIMES: INTERNATIONAL EXPERIENCE

Мамедова Л.Ш., аспірант кафедри криміналістики та судової медицини
Національна академія внутрішніх справ

Статтю присвячено висвітленню окремих особливостей використання спеціальних знань під час розслідування кіберзлочинів із урахуванням досвіду окремих зарубіжних країн. Розглянуто правову природу таких понять, як «цифрова криміналістика» та «комп'ютерна криміналістика», оскільки для розслідування кіберзлочинів використовують знання цифрової криміналістики (digital forensics), зокрема її складової частини – комп'ютерної криміналістики (computer forensics), і розвідку з відкритим кодом (Open Source INTelligence – OSINT). Окреслено основні види цифрових криміналістичних експертиз, зазначено особливості використання знань цифрової криміналістики.

Проаналізовано та досліджено проблеми цифрової криміналістики: технічні, правові й організаційні. Акцентовано увагу на підготовці спеціалістів, фахівців (експертів) для проведення розслідувань кіберзлочинів.

Розглянуто процес залучення спеціалістів та експертів до розслідування кримінальних правопорушень на прикладі Англії, Бельгії, Франції, Фінляндії, Швеції та Нідерландів. Зазначено, що потребує ретельного дослідження правовий статус і розмежування таких понять, як «спеціаліст», «фахівець» та «експерт». Запропоновано напрями вдосконалення використання спеціальних знань під час розслідування кіберзлочинів.

Зроблено висновок, що сучасні інструменти та методи боротьби з кіберзлочинністю мають на меті підвищити рівень кваліфікації не тільки судових експертів, але й насамперед співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів. Крім того, міжнародний досвід і співробітництво сучасних країн світу з Україною стосовно використання спеціальних знань у боротьбі з кіберзлочинністю сприятиме більш ефективному вирішенню складних теоретичних і практичних завдань під час розслідування кіберзлочинів.

Ключові слова: кіберзлочини, спеціальні знання, спеціаліст, експерт, цифрова криміналістика, комп'ютерна криміналістика, експертиза.

The article is devoted to highlighting some peculiarities of the using special knowledge during the investigation of cybercrime, taking into account the experience of some foreign countries. The legal nature of such concepts as "digital forensics" and "computer forensics" is considered, as knowledge of digital forensics is used to investigate cybercrime, in particular its component part – computer forensics, and open source intelligence (Open Source INTelligence – OSINT). The main types of digital forensic examinations are outlined, the peculiarities of using the knowledge of digital forensics are indicated.

Problems of digital criminology: technical, legal and organizational are analyzed and researched. Emphasis is placed on the training of specialists, technician (experts) for the investigation of cybercrime.

The process of involving specialists and experts in the investigation of criminal offenses is considered, for example, England, Belgium, France, Finland and Sweden and the Netherlands. It is noted that the legal status and delimitation of such concepts as "specialist, "technician" and "expert" need to be carefully studied. The directions of improvement of the using special knowledge during investigation of cybercrimes are offered.

It is concluded that modern tools and methods of combating cybercrime are aimed not only at improving the skills of forensic experts, but also, above all, employees of operational units, employees of pre-trial investigation bodies, prosecutors, judges. In addition, the international experience and cooperation of modern countries with Ukraine in the use of specialized knowledge in the fight against cybercrime will contribute to a more effective solution of complex theoretical and practical problems during investigation of cybercrime.

Key words: cybercrime, special knowledge, specialist, expert (examiner), digital forensics, computer forensics, expert examination.

Постановка проблеми. В Угоді про асоціацію України з Європейським Союзом визначено, що боротьба з кіберзлочинністю має сприяти поступовій конвергенції у сфері зовнішньої та безпекової політики, задля чого доцільно вжити низку законодавчих, організаційних, кадрових і навчальних заходів [1]. Актуальність вказаних питань відображена у Стратегії кібербезпеки України, у якій передбачено, що для формування потенціалу стримування (С) необхідне досягнення стратегічних цілей, зокрема цілі С.3. Ефективної протидії кіберзлочинності.

Для досягнення вищезазначеної цілі С.3 Україна посилить спроможності у протидії кіберзлочинності шляхом забезпечення підвищення рівня кваліфікації, матеріально-технічного забезпечення судових експертів за напрямами досліджень комп'ютерної техніки та програмних продуктів, комунікаційних систем і засобів; забезпечення підвищення рівня знань співробітників оперативних підрозділів, працівників органів досудового розслідування, прокуратури, суддів у сфері інформаційних технологій і кібербезпеки, насамперед за напрямами збирання та дослідження електронних доказів тощо [2].

Для вирішення зазначених проблемних питань слід проаналізувати досвід провідних країн світу стосовно використання спеціальних знань під час розслідування кіберзлочинів.

Незважаючи на те, що більшість зарубіжних країн мають сучасні інструменти та методи боротьби з кіберзлочинністю, відкритим залишається питання стосовно створення єдиних методів проведення експертиз під час розслідування зазначеної категорії злочинів і єдиної системи підготовки та підвищення кваліфікації експертів і спеціалістів.

Аналіз останніх досліджень і публікацій. Проблемні питання розслідування кіберзлочинів, у тому числі злочинів у сфері електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку окреслені у наукових працях Н.М. Ахтирської, П.Д. Біленчука, В.Б. Вєхова, В.О. Голубєва, О.І. Мотляха, Л.П. Паламарчук, О.В. Орлова, М.В. Салтевського, Т.Л. Тропіної, В.Г. Хахановського, С.С. Чернявського та ін. Водночас поза увагою науковців залишається саме аналіз зарубіжного досвіду розслідування зазначеної категорії злочинів, що зумовлює актуальність дослідження.

Мета статті – висвітлення особливостей використання спеціальних знань під час розслідування кіберзлочинів із урахуванням міжнародного досвіду.

Виклад основного матеріалу. Кіберзлочинці у більшості країн світу, використовуючи панічні настрої серед громадян у період глобальної пандемії COVID-19, здійснюють фішинг-атаки з використанням шкідливого

програмного забезпечення. Їхньою метою є отримання персональних даних користувачів мережі, а саме логінів і паролів доступу до різних інтернет-ресурсів: електронних поштових скриньок, облікових записів соціальних мереж, електронних гаманців тощо для подальшого привласнення грошей [3].

У щорічному звіті Norton™ Cyber Safety Insights Report за 2021 рік зазначено, що майже 330 мільйонів людей у 10 країнах стали жертвами кіберзлочинів і понад 55 мільйонів людей стали жертвами крадіжки особистих даних. Жертви кіберзлочинів разом витратили майже 2,7 мільярда годин, намагаючись вирішити свої проблеми [4].

Більшість сучасних країн для розслідування кіберзлочинів використовують дві загальні категорії – цифрову криміналістику (digital forensics) і розвідку з відкритим кодом (Open Source INTelligence – OSINT).

Цифрова криміналістика застосовується для ідентифікації, збереження, відновлення, аналізу та презентації електронних доказів, знайдених у комп'ютерах чи цифрових пристроях зберігання даних. Термін «цифрова криміналістика» раніше використовувався як синонім комп'ютерної криміналістики, який українська мова запозичила з англійської (forensics – від англ. forensic science), – напрям криміналістики, що вивчає комп'ютерні злочини й має назву «computer forensics», але внаслідок запозичення термін дещо звузив своє значення. Тому в нашій країні форензіка означає суто комп'ютерну криміналістику, а термін «цифрова криміналістика» має більш широке значення [5, с. 5].

На думку О.М. Яковлєва, цифрова криміналістика – новий термін, котрий не є усталеним, проте вже має синоніми («електронна криміналістика», «комп'ютерна криміналістика» тощо). Водночас це настільки серйозна та перспективна адаптація підходів традиційної криміналістики до реалій розвитку сучасного інформаційного суспільства, що правоохоронна практика вимагає якнайшвидше пройти шлях наукового становлення цього напряму та перейти до масової практичної реалізації її положень під час розслідування злочинів. Цифрова криміналістика – це ті нові знання у криміналістиці, які базуються на розумінні особливостей функціонування сучасних інформаційно-комунікаційних технологій і використовуються для розкриття та розслідування особливо складних злочинів, які раніше справедливо вважалися латентними [6, с. 357, 360].

Сесилия Хоран і Хоссейн Сайедян надають визначення цифровій криміналістиці як практиці збору й упорядкування інформації, знайденої на електронному пристрої, для слідчих цілей. У цифровій криміналістиці виокремлюють чотири види цифрових криміналістичних експертиз: хоста, мобільних пристроїв, комп'ютерну (або мережеву) та хмарну. Крім того, важливо знати не тільки технології, методи, але й основи, які фахівці використовують у цій галузі [7, с. 582].

Знання цифрової криміналістики використовуються для виявлення кримінально-релевантних закономірностей:

1) злочинної діяльності, спрямованої на перешкоджання нормальному функціонуванню інформаційних систем, їхніх компонентів або діяльності, спрямованої на використання останніх як інструменту скоєння інших злочинів;

2) створення, зміни, передачі, видалення інформації на електронних носіях, в інформаційно-телекомунікаційних мережах, віртуальному просторі, пов'язаному з підготовкою, скоєнням, приховуванням злочинів;

3) збирання цифрової інформації з виконанням технічних процедур забезпечення її юридичної значимості;

4) дослідження цифрової інформації, збереженої в окремих інформаційних об'єктах, а також інформаційному середовищі електронного носія інформації;

5) оцінки отриманих результатів, співвіднесення їх із діями суб'єкта та використання для кваліфікації злочинного діяння;

6) інтеграції цифрових доказів у систему доказів із дотриманням процесуальної форми їх отримання [6, с. 360–361].

До проблем цифрової криміналістики, окрім технічних і правових, також належить підготовка спеціалістів/фахівців, котрі мають знання фізичних принципів роботи цифрових систем та інструментарію комп'ютерної криміналістики – знання технічних і правових аспектів.

Наприклад, правоохоронці повинні бути у змозі розслідувати кіберзлочини та/або інші злочини, які так чи інакше пов'язані з використанням пристроїв інформаційно-комунікаційних технологій (наприклад, смартфонів, у яких зберігаються докази злочину), та належним чином використовувати інформаційно-комунікаційні технології під час розслідування (наприклад, виявляти, отримувати, зберігати й аналізувати цифрові докази у такий спосіб, щоб забезпечити їх допустимість у суді) [8].

Для правильного збору та збереження доказів під час розслідування кіберзлочинності потрібно мати відповідні навички та досвід як із кібербезпеки, так і з використання методів розслідування тощо. Вкрай важливою є здатність працювати у середовищі кількох юрисдикцій або між юрисдикціями, оскільки одним із головних аспектів кіберзлочинності є її нелокальний характер. Незаконна діяльність може відбуватися у юрисдикціях, розділених великими відстанями, що насамперед створює серйозні проблеми під час розслідування кіберзлочинів, оскільки ці злочини часто вимагають міжнародної співпраці [9].

Можливості правоохоронних органів розслідувати кіберзлочини залежать від країни та варіюються залежно від конкретної установи всередині країни. Наприклад, у Киргизькій Республіці правоохоронні органи мають обмежені можливості для розслідування кіберзлочинів через відсутність спеціалізованих знань, навичок, здібностей, підготовки, а також брак кадрових і фінансових ресурсів. Для порівняння, у Франції існує кілька підрозділів, співробітники яких мають спеціальну підготовку для проведення розслідувань кіберзлочинів (наприклад, Les investigateurs en Cybercriminalité (слідчі у справах про кіберзлочинність) (ICC) і N-TECH (слідчі зі спеціальною підготовкою у сфері нових технологій), які входять до складу Національної жандармерії) [8].

У багатьох розвинених країнах існує велика кількість спеціалізованих навчальних курсів із зазначеної сфери з метою отримання або вдосконалення вже наявних знань [10, с. 299]. Для боротьби з кіберзлочинами необхідно виховувати та розвивати людські ресурси як одну з найнадійніших стратегій. Крім того, університети, заклади вищої освіти й академічні заклади мають відкрити спеціальні курси, покликані дати можливість майбутнім поколінням суддів, прокурорів та адвокатів навчатися у цій складній, але дуже актуальній і важливій сфері [11, с. 60].

Так, наприклад, у Великій Британії та США поширені програми цифрової судової експертизи або програми із криміналістики та кібербезпеки, зосереджені на цифровій судовій експертизі [10, с. 300].

Окрім того, головним онлайн-ресурсом для навчання, освіти й інформації про кібербезпеку є вебсайт National Initiative for Cybersecurity Careers and Studies (NICCS). NICCS об'єднує державних службовців, студентів, викладачів і промисловість із ресурсами кібербезпеки та постачальниками тренінгів по всій країні. Усі курси узгоджені зі спеціальними галузями The Workforce Framework for Cybersecurity (NICE Framework). Наприклад, можна стати криміналістичним аналітиком кіберзахисту (IN-FOR-002), який аналізує цифрові докази та досліджує інциденти з комп'ютерною безпекою, щоб отримати корисну інформацію для пом'якшення вразливості системи/мережі; або судовим аналітиком правоохоронних органів/контррозвідки (IN-FOR-001), котрий проводить детальні розслідування комп'ютерних злочинів, встановлюючи

документальні або речові докази, включаючи цифрові носії інформації та журнали, пов'язані з інцидентами кібер-вторгнення [12].

Отже, покращити свій набір навичок, знань і здібностей можна шляхом проходження відповідних сертифікованих курсів у галузі цифрової криміналістики, зокрема кібербезпеки.

Наприклад, у 2016 році за сприяння Управління з питань запобігання зловживанням і шахрайству Європейської Комісії (OLAF) детективи-криміналісти Національного антикорупційного бюро України пройшли повний курс навчання за кордоном за спеціалізованою програмою підготовки. За результатами виконання численних практичних завдань та успішного складання спеціальних тестів криміналісти отримали сертифікацію із проведення експертизи й аналізу файлових та операційних систем сімейства Microsoft Windows.

Сертифікат експерта з комп'ютерно-технічних досліджень за критеріями Міжнародної асоціації спеціалістів із комп'ютерних розслідувань (The International Association of Computer Investigative Specialists (IACIS) у 2017 році отримали два співробітники кримінальної лабораторії Національного антикорупційного бюро України [13].

У країнах ЄС сьогодні також закріплені дві основні організаційні форми судової експертизи. Перша – орієнтація на спеціальні (зокрема й експертні) установи, друга – орієнтація на конкретних фахівців, внесених у списки судових експертів або тих, що отримали ліцензію на право проведення судової експертизи [14, с. 131].

У Бельгії та Франції експертом вважається будь-яка особа, котра має завдяки своїй освіті та досвіду поглиблені знання в одній або декількох галузях знань. Експерти у Франції та Бельгії об'єднуються у професійні одно- або багатодисциплінарні асоціації, спілки та палати (французька Національна палата експертів-фахівців, Бельгійська Асоціація експертів, до якої входять на правах членів експерти у різних галузях знань) [15, с. 636].

Експертом у Фінляндії та Швеції є особа, що проводить судову експертизу, має для цього спеціальні знання та навички, відповідну вищу освіту. Системи експертних установ Фінляндії та Швеції складаються з державних і приватних лабораторій, які здійснюють судову експертизу, освітніх установ, котрі здійснюють підготовку фахівців у галузі судової експертизи. Особливістю підготовки експертних кадрів у Фінляндії та Швеції є те, що після закінчення навчання у закладі вищої освіти експерт отримує диплом магістра та сертифікат, на підставі якого має право проводити судову експертизу як у державних органах, так і у приватній практиці [16, с. 160].

Процесуальне законодавство Фінляндії та Швеції надає судовому експертові статус свідка та не містить терміна «спеціаліст», використовуються тільки терміни «експерт» і «фахівець». Розподіл посад експерта і фахівця у Державних лабораторіях Фінляндії здійснюється за науковим ступенем: експерт має ступінь магістра, а фахівець – ступінь бакалавра, що підтверджується відповідними дипломами про вищу освіту [16, с. 161].

У Нідерландах судові експерти державних експертних установ проводять експертизи та дослідження за зверненнями поліції, а не суду. Суд запрошує експертів незалежно від їх основного місця роботи [15, с. 636]. В Англії, як і в Україні, судового експерта до процесу може залучити як сторона обвинувачення, так і сторона захисту. У Великій Британії також існує список (перелік) експертів, котрі мають право бути залучені до проведення досліджень під час процесу, такий список зберігається у Спілці юристів Англії [16, с. 161].

Слушною є думка А.М. Лазебного, який за результатами аналізу законодавства країн ЄС, іншого міжнародного законодавства та внутрішнього законодавства багатьох країн зазначає, що у світі послідовно реалізовуються принципи забезпечення незалежності експерта, виключної орієнтації не на відомчу належність експерта, а на наявність у нього спеціальних знань, необхідних для вирішення завдань правосуддя, забезпечення принципу змагальності експертів, залучених різними сторонами процесу, та інші принципи, які мають вирішальне значення для забезпечення судочинства дійсно незалежною, об'єктивною та кваліфікованою експертизою. Наявність інституту приватної експертизи не тільки є однією з гарантій забезпечення законних прав і свобод громадян та інтересів суспільства, але й дозволяє суттєво зменшити бюджетні витрати на утримання державних експертних установ [17, с. 90].

Висновки. Необхідно більше уваги приділити дослідженню так званої цифрової криміналістики (digital forensics), оскільки знання специфіки роботи цифрових криміналістичних засобів і вміння використовувати всі їхні властивості є найважливішою умовою якісного вирішення криміналістичних завдань, що стоять перед спеціалістом, фахівцем (експертом) під час розслідування кіберзлочинів.

Крім того, з метою ефективного розслідування та розкриття зазначеної категорії злочинів доцільно приділити увагу підвищенню кваліфікації експертів і спеціалістів, створити передумови для впровадження єдиної системи підготовки та підвищення кваліфікації кадрів, які залучаються до протидії кіберзлочинності.

Важливо, ураховуючи специфіку проведення судової експертизи, зокрема цифрових криміналістичних експертиз, створити умови для їхнього розвитку та розробити єдині методи проведення судових експертиз під час розслідування зазначеної категорії злочинів шляхом удосконалення науково-методичних рекомендацій відповідно до міжнародних стандартів. Для вирішення цих питань потребує ретельного дослідження визначення таких понять, як «спеціаліст», «фахівець» та «експерт», а надалі – досягнення узгодженості їхнього правового статусу у чинному законодавстві зарубіжних країн та України.

Таким чином, міжнародний досвід і співробітництво сучасних країн світу з Україною сприятиме більш ефективному вирішенню складних теоретичних і практичних завдань щодо використання спеціальних знань під час розслідування кіберзлочинів.

ЛІТЕРАТУРА

1. Угода про асоціацію між країною, з однієї сторони, та Європейським Союзом, Європейським співтовариством з атомної енергії і їхніми державами-членами, з іншої сторони : Угода, Список, Міжнародний документ від 27 червня 2014 р. *База даних «Законодавство України»*. URL: https://zakon.rada.gov.ua/laws/show/984_011#Text. (дата звернення: 26 грудня 2021 р.).

2. Про рішення Ради національної безпеки і оборони України від 14 травня 2021 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 26 серпня 2021 р. № 447/2021. *База даних «Законодавство України»*. URL: https://zakon.rada.gov.ua/laws/show/447/2021#Text (дата звернення: 26.12.2021).

3. Кіберполіція попереджає про активізацію хакерів в період карантину / Офіційний сайт кіберполіції України. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-poperedzhaye-pro-aktyvizacziyu-xakeriv-v-period-karantynu-617/ (дата звернення: 24.12.2021).

4. 2021 Norton Cyber Safety Insights Report. *NortonLifeLock*. 2021. URL: https://www.nortonlifelock.com/us/en/newsroom/press-kits/2021-norton-cyber-safety-insights-report/ (дата звернення: 24.12.2021).

5. Павлюк Н.В. Інтеграція інноваційних технологій у діяльність з розслідування злочинів – провідний напрям підвищення її ефективності. *Теорія і практика правознавства.* 2021. Вип. 2 (20). С. 1–13.

6. Яковлев А.Н. Цифровая криминалистика и ее значение для расследования преступлений в современном информационном обществе. *Совершенствование следственной деятельности в условиях информатизации* : сб. материалов междунар. науч.-практ. конф. (Минск, 12–13 апреля 2018 г.). Следственный комитет Республики Беларусь; редкол.: С.Я. Аземша. Минск : Промышленно-торговое право, 2018. 368 с.

7. Horan C. Saiedian, H. Cyber Crime Investigation: Landscape, Challenges, and Future Research Directions. *J. Cybersecur. Priv*. 2021. № 1. P.580–596. URL: https://doi.org/10.3390/jcp1040029 (дата звернення: 25.12.2021).

8. Module 5. Cybercrime Investigation. Teaching Guide for Lecturers Using the Education for Justice University Modules on Cybercrime. *UNODC. 2019.* URL: https://www.unodc.org/e4j/en/cybercrime/module-5/index.html (дата звернення: 25.12.2021).

9. Steven Bowcut. How to become a cybercrime investigator: A complete career guide. *Cybersecurity Job Guide.* Last updated: November 5, 2021. URL: https://cybersecurityguide.org/careers/cyber-crime-investigator/ (дата звернення: 25.12.2021).

10. Richard Apau, Felix N. Koranteng. An overview of the digital forensic investigation infrastructure of Ghana. *Forensic Science International: Synergy.* Vol. 2. 2020. P. 299–309. URL: https://www.sciencedirect.com/science/article/pii/S2589871X20300619#bib2 (дата звернення: 24.12.2021).

11. Mohammed, Kabiru H., Mohammed, Yusuf D., and Solanke, Abiodun A. Cybercrime and Digital Forensics: Bridging the gap in Legislation, Investigation and Prosecution of Cybercrime in Nigeria. *International Journal of Cybersecurity Intelligence & Cybercrime*. 2019. № 2 (1). P. 56–63. URL: https://www.doi.org/10.52306/02010519ZJRK2912 (дата звернення: 24.12.2021).

12. Digital Forensics. *The National Initiative for Cybersecurity Careers and Studies (NICCS) website.* URL: https://niccs.cisa.gov/workforce-development/cyber-security-workforce-framework/digital-forensics (дата звернення: 25.12.2021).

13. Детективи-криміналісти НАБУ здобули унікальні для України навички. *Офіційний сайт Національного антикорупційного бюро України*. 2017. URL: https://nabu.gov.ua/novyny/detektyvy-kryminalisty-nabu-zdobuly-unikalni-dlya-ukrayiny-navychky.

14. Гузела М., Канцір В. Зарубіжний досвід організації судово-експертної діяльності в процесі здійснення кримінального переслідування. *Вісник Національного університету «Львівська політехніка»*. 2018. Вип. 5. № 906. С. 129–135.

15. Авдєєва Г. Проблеми гармонізації законодавства України у галузі судової експертизи із законодавством країн Європейського Союзу. *Гармонізація законодавства.* 27 березня 2015. URL: http://www.ares21.vk.kharkov.ua/bitstream/123456789/7223/1.

16. Завидняк І.О. Позитивний досвід розвинених країн європейського союзу у використанні спеціальних знань під час розслідування злочинів у сфері господарської діяльності. *Теорія та практика судово-експертної діяльності.* 2019. С. 15-–162.

17. Лазебний А.М. Міжнародний досвід використання спеціальних знань під час розслідування кримінальних правопорушень проти громадського порядку. *Міжнародний юридичний вісник: збірник наукових праць Національного університету державної податкової служби України*. Вип. 1 (3). 2016. С. 85–90.