МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ

НАЦІОНАЛЬНИЙ ЮРИДИЧНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЯРОСЛАВА МУДРОГО

КАФЕДРА КРИМІНОЛОГІЇ
ТА КРИМІНАЛЬНО-ВИКОНАВЧОГО ПРАВА

МІЖНАРОДНІ СТАНДАРТИ З КІБЕРБЕЗПЕКИ ТА ЇХ ЗАСТОСУВАННЯ В УКРАЇНІ

Матеріали «круглого столу»
(м. Харків, 19 квітня 2016 р.)

За редакцією
А. П. Гетьмана, Б. М. Головкіна

Харків
«Право»
2016

УДК343.9:004.057.2
ББК 67.61я431
М58

Редакційна колегія:
д-р юрид. наук, проф. *А.П. Гетьман,*
д-р юрид. наук, проф. *Б. М. Головкін,*
канд. юрид. наук, доц. *О. В. Ткачова,*
канд. юрид. наук, асист. *О. В. Таволжанський*

Міжнародні стандарти з кібербезпеки та їх застосування в Україні (матеріали
М58 «круглого столу» м. Харків, 19 квіт. 2016 р.) / за ред. А. П. Гетьмана, Б. М. Головкіна. – Х. : Право, 2016. – 88 с.

ISBN 978-966-937-024-2

© Національний юридичний університет імені Ярослава Мудрого, 2016
© Оформлення. Видавництво «Право», 2016

ISBN 978-966-937-024-2

виявлених слідів комп'ютерних злочинів напряму залежить від обсягу використаних спеціальних знань та рівня обізнаності спеціаліста (експерта), якого залучено до огляду (дослідження) комп'ютерної інформації. Тому для підвищення ефективності використання спеціальних знань у боротьбі з кіберзлочинністю є необхідною більш чітка процесуальна регламентація судово-експертної діяльності та надання можливості співробітникам правоохоронних органів самостійно обирати найбільш кваліфікованих спеціалістів (експертів) у галузі комп'ютерної техніки, програмних продуктів та телекомунікаційних мереж для залучення їх до проведення судових експертиз. Цю проблему на сьогодні можна вирішити лише шляхом скасування в ст. 7 Закону України «Про судову експертизу» норми «Виключно державними спеціалізованими установами здійснюється судово-експертна діяльність, пов'язана з проведенням криміналістичних експертиз» [3].

Список літератури

1. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / Офіційний сайт Верховного суду України. [Текст]. – [Електронний ресурс]. – Режим доступу: http://www.scourt.gov.ua. – Заголовок з екрану.
2. Основные услуги и тарифы на рынке киберпреступности в странах СНГ. [Текст]. – [Електронний ресурс]. – Режим доступу: http://www.interface.ru. – Заголовок з екрану.
3. Про судову експертизу. Закон України. / Законодавство України. [Текст]. – [Електронний ресурс]. – Режим доступу: http://zakon5.rada.gov.ua/laws/show/4038–12. – Заголовок з екрану.

В. В. Білоус,
к.ю.н., доцент кафедри криміналістики
Національного юридичного університету
імені Ярослава Мудрого,
м. Харків

РОЛЬ ЗАСОБІВ КРИМІНАЛІСТИКИ У ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Забезпечення інформаційної безпеки України відповідно до ст. 17 Основного Закону є однією з найважливіших функцій держави, справою всього Українського народу. Забезпечення кібербезпеки і безпеки інформаційних ресурсів Стратегією національної безпеки України віднесено до основних напрямів державної політики національної безпеки нашої держави. Серед пріоритетів цього напря-

му чільне місце відведено моніторингу кіберпростору з метою своєчасного виявлення, запобігання кіберзагрозам і їх нейтралізації, а також розвитку спроможностей правоохоронних органів щодо розслідування кіберзлочинів [1].

Не викликає жодних сумнівів пріоритетність цих завдань не тільки для України але й переважної більшості інших країн світу. Адже відкритий і вільний кіберпростір не тільки розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції тощо. Практично відразу ж після свого формування, в руках асоціальних суб'єктів він став сприятливим середовищем для модернізації існуючих або створення нових способів готування, вчинення й приховання широкого кола традиційних злочинів, а також започаткування раніше не відомих видів кримінальних правопорушень, заснованих на використанні потенціалу інформаційних технологій, що зумовило виникнення нових загроз національній та міжнародній безпеці. Останнім часом кіберпростір поступово перетворюється ще й на окрему, поряд із традиційними «Земля», «Повітря», «Море» та «Космос», сферу ведення бойових дій, у якій все більш активно діють відповідні підрозділи збройних сил провідних держав світу.

У Стратегії кібербезпеки України наголошується на тому, що забезпечення кібербезпеки нашої країни як стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави в кіберпросторі, що досягається комплексним застосуванням сукупності правових, організаційних, інформаційних заходів, має базуватися, зокрема, на принципах: пріоритетності запобіжних заходів і невідворотності покарання за вчинення кіберзлочинів; міжнародного співробітництва з метою зміцнення взаємної довіри у сфері кібербезпеки та вироблення спільних підходів у протидії кіберзагрозам, консолідації зусиль у розслідуванні та запобіганні кіберзлочинам, недопущення використання кіберпростору в протиправних та воєнних цілях тощо.

Створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави потребує створення національної системи кібербезпеки, а також посилення спроможностей суб'єктів сектору безпеки та оборони для забезпечення ефективної боротьби із кіберзагрозами воєнного характеру, кібершпигунством, кібертероризмом та кіберзлочинністю, поглиблення міжнародного співробітництва у цій сфері. Основу національної системи кібербезпеки мають становити Міністерство оборони України, Державна служба спеціального зв'язку та захисту інформації України, Служба безпеки України, Національна поліція України, Національний банк України, розвідувальні органи.

При цьому, на Службу безпеки України мають бути покладені в установленому порядку такі основні завдання, як: попередження, виявлення, припинення та розкриття злочинів проти миру і безпеки людства, які вчиняються у кіберпросторі; здійснення контррозвідувальних та оперативно-розшукових заходів, спрямованих на боротьбу з кібертероризмом та кібершпигунством, а також щодо готовності об'єктів критичної інфраструктури до можливих кібератак та кіберін-

цидентів; протидія кіберзлочинності, можливі наслідки якої безпосередньо створюють загрозу життєво важливим інтересам України; розслідування кіберінцидентів та кібератак щодо державних електронних інформаційних ресурсів, інформації, вимога щодо захисту якої встановлена законом, критичної інформаційної інфраструктури; забезпечення реагування на комп'ютерні інциденти у сфері державної безпеки.

До основних завдань Національної поліції України віднесено: забезпечення захисту прав і свобод людини та громадянина, інтересів суспільства і держави від злочинних посягань у кіберпросторі; запобігання, виявлення, припинення та розкриття кіберзлочинів; підвищення поінформованості громадян про безпеку в кіберпросторі [2], що цілковито відповідає принципу пріоритетності запобіжних заходів. Адже для більшості представників «Покоління Y», які, зросли на цифрових технологіях, мобільних додатках, соціальних Інтернет-мережах і, за деякими оцінками, вже в 2020 р. становитимуть левову частку працездатного населення планети, через низький рівень інформаційної культури та усвідомлення особистої відповідальності за порушення інформаційної безпеки залишається характерним високий рівень віктимності. Відтак, будь-які державні та приватні інвестиції у розвиток та вдосконалення систем технічного і криптографічного захисту інформації можуть виявитися марними, якщо у цій царині не відбудеться кардинальних змін, і діяльність в кіберпросторі окремих громадян і цілого суспільства не відповідатиме актуальному рівню кіберзагроз.

Тому заслуговує на цілковиту підтримку віднесення Стратегією кібербезпеки України до числа пріоритетів і напрямів забезпечення кібербезпеки нашої держави розвитку безпечного, стабільного і надійного кіберпростору, який має полягати, насамперед, у підвищенні цифрової грамотності громадян та культури безпекового поводження в кіберпросторі, комплексних знань, навичок і здібностей, необхідних для підтримки цілей кібербезпеки, впровадженні державних і громадських проектів підвищення рівня обізнаності суспільства щодо кіберзагроз та кіберзахисту.

Стратегія орієнтує нас на необхідність нейтралізації так званого суб'єктивного чинника при забезпеченні кібербезпеки і в інших напрямах. Так, кіберзахист державних електронних інформаційних ресурсів та інформаційної інфраструктури, призначеної для обробки інформації, вимога щодо захисту якої встановлена законом, має полягати, насамперед, у підвищенні обізнаності працівників державних органів у сфері інформаційної безпеки та кібербезпеки, проведенні відповідних тренінгів, навчань. Кіберзахист критичної інфраструктури має полягати в установленні кваліфікаційних вимог для окремих категорій працівників об'єктів критичної інфраструктури з урахуванням сучасних тенденцій кібербезпеки та актуальних кіберзагроз, упровадженні для таких працівників обов'язкової періодичної атестації на предмет відповідності зазначеним вимогам. А розвиток потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки передбачатиме здійснення в установленому порядку таких заходів, як розвиток системи підготовки кадрів для потреб органів цього сектору у сукупності з розвитком науково-виробничого потенціалу такої системи. Створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони підносить до рівня пріоритетів забезпечен-

ня кібербезпеки та безпеки інформаційних ресурсів і Стратегія національної безпеки України.

Стрімке впровадження в різні галузі життєдіяльності суспільства новітніх досягнень науково-технічного прогресу, заміна традиційних знарядь праці й комунікації на комп'ютерну техніку, програмне забезпечення й широкий спектр інформаційних технологій, поширення електронного документообігу у виробничій сфері й побуті, розгортання масового виробництва й використання не тільки окремих «розумних» приладів, але й їх високотехнологічних систем (наприклад, «Smart House») призвели до кардинальної зміни механізму відображення діяльності людини в об'єктивно існуючій дійсності. Для створення, передавання та збереження інформації сучасна людина все рідше використовує писемну рукописну мову. Все частіше хронологія її життєдіяльності відображається як в електронних і sms-повідомленнях, статусах на сторінках в соціальних Інтернет-мережах тощо, створюваних самою особою, так і в доріжках електронних слідів, що генеруються використовуваними електронними пристроями не залежно від волі останньої.

Криміналістика – наука про закономірності злочинної діяльності та її відображення в джерелах інформації, які слугують основою для розроблення засобів, прийомів і методів збирання, дослідження, оцінки та використання доказів з метою розкриття, розслідування, судового розгляду та запобігання злочинам [3, с. 8]. Тривалий час у криміналістиці переважно вивчалися сліди *механічної* дії, як найбільш поширені об'єкти трасологічного дослідження. Однак в епоху інформаційних технологій традиційна класифікація слідів втрачає здатність повною мірою задовольняти потреби криміналістики і слугувати дієвим засобом теоретичного забезпечення виконання вирішуваних останньою завдань, зокрема, у царині протидії кіберзлочинності. Викликом сучасності, що постав перед криміналістичною теорією і практикою, є необхідність вивчення електронних (цифрових) слідів як явища об'єктивної дійсності й розроблення криміналістичних рекомендацій щодо найбільш ефективного їх виявлення, дослідження, фіксації, вилучення й використання у діяльності з розслідування й попередження злочинів. Адже потенціал використання електронних слідів у діяльності органів кримінальної юстиції з розшуку та ідентифікації осіб, запобігання правопорушенням тощо, залишається на неприпустимо низькому рівні.

Тому цілком справедливо, що за задумом Ради національної безпеки і оборони України боротьба з кіберзлочинністю передбачатиме здійснення, серед іншого, таких заходів, як: удосконалення процесуальних механізмів щодо збирання доказів в електронній формі, що стосуються злочину, удосконалення класифікації, методів, засобів і технологій ідентифікації та фіксації кіберзлочинів, проведення експертних досліджень; врегулювання питання можливості термінового здійснення процесуальних дій у режимі реального часу із застосуванням електронних документів та електронного цифрового підпису; упровадження схеми (протоколу) координації правоохоронних органів щодо боротьби з кіберзлочинністю; запровадження особливого порядку зняття інформації з каналів телекомунікацій у випадку розслідування кіберзлочинів; підвищення кваліфікації співробітників правоохоронних органів; підготовка суддів (слідчих суддів), слідчих та прокурорів для роботи з доказами, що стосуються злочину, отриманими в елек-

тронній формі, з урахуванням особливостей кіберзлочинів тощо [2].

Вирішальну роль у протидії кіберзлочинності та реалізації вище перелічених заходів може відіграти широкий спектр засобів сучасної криміналістики, спрямованих на:

1. Масштабну інтеграцію до криміналістики знань із галузі інформатики й розроблення окремої криміналістичної теорії (вчення) про електронний слід, в рамках якої необхідно розробити теоретичні основи електронного слідознавства, дослідити закономірності виникнення електронних слідів, що відображають механізм злочину, розробити рекомендації із застосування методів і засобів виявлення електронних слідів, їх фіксації, вилучення й аналізу з метою встановлення обставин, що мають істотне значення для розкриття, розслідування й попередження злочинів. Розроблення теоретичних підвалин для розбудови інших криміналістичних теорій, необхідних для якомога швидшого упровадження «електронного кримінального провадження».

2. Модернізацію навчального курсу з криміналістики у напрямку поглибленого вивчення: прийомів і методів процесуально-коректного виявлення, фіксації і вилучення різних електронних слідів, а також трансформації виявлених електронних інформаційних масивів у процесуальні форми, доступні для сприйняття всіма учасниками судочинства; техніко-криміналістичного забезпечення і тактики огляду комп'ютерної техніки, а також вилучення електронних документів; вимог до кваліфікації слідчого, понятих і спеціалістів, що залучаються до участі в названих та інших слідчих (розшукових) діях; форм взаємодії з адміністраторами мережевої безпеки і заходів з нейтралізації технічної протидії слідству, спрямованої на знищення електронних слідів; можливостей сучасної експертизи з дослідження слідів зазначеного виду й методичних рекомендацій із забезпечення експертизи репрезентативним обсягом об'єктів дослідження. Формування професійних навичок з об'єктивного, повного і всебічного встановлення обставин розслідуваного злочину потребує набуття знань щодо здійснення аналізу й синтезу даних, отриманих із галузі високих технологій, з «класичною криміналістичною слідовою картиною», виявленою за допомогою традиційних криміналістичних методик.

3. Подальший розвиток методики експертизи комп'ютерної техніки і програмних продуктів, а також експертизи телекомунікаційних систем і засобів, в межах яких шляхом дослідження електронних слідів вирішується широке коло діагностичних й ідентифікаційних завдань. Особливості механізму утворення і трансформації цифрових слідів повинні враховуватися при проведенні й широкого кола інших криміналістичних експертиз, наприклад: *технічної експертизи документів* при встановленні документа, виготовленого шляхом монтажу із застосуванням копіювально-розмножувальної та комп'ютерної техніки; ідентифікації особи, яка надрукувала текст з використанням комп'ютерної техніки, виготовила зображення відтиску печатки з використанням програмного забезпечення за особливостями навичок виконавця; установленні типу та ідентифікації комп'ютерної техніки за виготовленим за її допомогою документом; *експертизи відеозвукозапису і фототехнічної експертизи* при вирішенні завдань ідентифікації знімальної апаратури за електронними файлами фото/відеозаписів, ідентифікації осіб, предметів, приміщень та ділянок місце-

вості, відображених на записах, в т.ч. за допомогою геоінформаційних систем, відновлення первісних зображень у фото/відеофайлах тощо.

Список літератури

1. Про рішення Ради національної безпеки і оборони України від 6 травня 2015 року «Про Стратегію національної безпеки України» : Указ Президента України від 26.05.2015 р. №287/2015. [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua.
2. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : Указ Президента України від 15.03.2016 р. №96/2016. [Електронний ресурс]. – Режим доступу : http://www.president.gov.ua.
3. Криміналістика : підруч. [Текст] / В. Ю. Шепітько, В. О. Коновалова, В. А. Журавель [та ін.] : за ред. В. Ю. Шепітька. – 5-те вид. переробл. та допов. – К. : Ін Юре, 2016. – 640 с.

М. В. Валуйська,
к.ю.н., доцент кафедри кримінології
та кримінально-виконавчого права
Національного юридичного університету
імені Ярослава Мудрого,
м. Харків

ЗНАЧЕННЯ ВИВЧЕННЯ ОСОБИСТОСТІ ЗЛОЧИНЦЯ ДЛЯ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

У зв'язку із глибокими змінами, обумовленими переходом на цифрові технології, і глобалізацією комп'ютерних мереж, для захисту електронної інформації, яка може використовуватися для вчинення кримінальних правопорушень, визнаючи необхідність співробітництва між Державами і приватними підприємствами для боротьби з кіберзлочинністю і захисту законних інтересів у ході використання і розвитку інформаційних технологій, Україна 7 вересня 2005 р. ратифікувала Конвенцію про кіберзлочинність, яка набрала чинності 1липня 2006 р.

Науковці говорять про криміналізацію Інтернету, оцінюючи його як високо криміногенне середовище, чому сприяє анонімність злочинця і реальна для нього можливість залишатися на відстані багатьох тисяч кілометрів від своєї жертви [1]. Виходячи з таких властивостей віртуального середовища, відкриваються й нові способи здійснення злочинних актів, що, у свою чергу, викликає нагальну потребу у вивченні специфіки протиправних діянь у комп'ютерних мережах.

Підвищена небезпечність кіберзлочинів полягає у тому, що вони можуть не