Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні

Олександр Юхно *

* Д-р юрид. наук, професор, Харківський національний університет внутрішніх справ, м. Харків, Україна, ORCID: https://orcid.org/0000-0002-4771-0531, e-mail: u-kafedra@ukr.net

DOI: 10.32353/khrife.3.2021.04 УДК 343.98
Надійшло 08.11.2021 / Рецензовано 09.11.2021 / Прийнято до друку 15.11.2021 / Доступно онлайн 30.12.2021

Розглянуто генезис розвитку та шляхи вдосконалення теоретичних і прикладних напрямів криміналістики, судової експертології й кримінального процесу для вирішення криміналістичних, процесуальних, організаційних та інших проблемних питань запровадження й використання досягнень науки і техніки під час досудового розслідування та судового розгляду кримінальних правопорушень на різних історичних етапах розвитку цього напряму в Україні. Окремо акцентовано увагу на науковому підході до відбору, запровадження, використання електронно-обчислювальних машин, телекомунікаційних, комп'ютерних, цифрових та інших сучасних технологій і мереж, засобів зв'язку, штучного інтелекту й досягнень науки і техніки в криміналістиці, експертній діяльності й у досудовому розслідуванні. Вивчено та проаналізовано наукові позиції окремих учених і представників вітчизняних і зарубіжних наукових шкіл із названих питань (зокрема, щодо обговорення, висвітлення й законодавчого закріплення в правовому та процесуальному механізмах відбору, запровадження й використання згаданих технологій). Висловлено авторське бачення та сформовано наукову позицію щодо порушених проблемних питань і шляхів їх вирішення.

Метою є аналіз історичного розвитку й сучасного стану криміналістичних, процесуальних і організаційних проблемних питань з відбору, ліцензування, використання, адаптування сучасних інформаційних, цифрових, телекомунікаційних,

комп'ютерних та інших технологій (зокрема, штучного інтелекту) у криміналістиці, експертній діяльності та досудовому розслідуванні, а також нормативно-правової бази, що регулює окремі питання цього напряму.

Ключові слова: *криміналістика; експертна діяльність; досудове розслідування; сучасні технології; комп'ютерні мережі; інформаційний простір; цифрові технології; штучний інтелект; відбір; адаптування.*

Постановка наукової проблеми

Людина повсякчас розвивається, намагаючись пристосувати до своїх потреб навколишній світ. На початку існування вона навчилася використовувати деревину й каміння для свого виживання, а сьогодні сягнула такого наукового рівня, що здатна опанувати навіть космічний простір. Людина XXI століття вже не уявляє свого існування без новітніх засобів спілкування, які вдосконалює день у день. Не уявляють свого життя без цього й ті, хто намагається жити за рахунок оточуючих, скоюючи кримінальні правопорушення. У всьому світі правоохоронні органи протиставляють діяльності таких осіб сучасні досягнення науки й техніки, застосовуючи передові наукові підходи до відбору, ліцензування, запровадження й адаптування новацій у методиках розслідування негативних явищ. Це повною мірою стосується застосування новітніх досягнень науки й техніки у сфері інформаційних, телекомунікаційних, комп'ютерних, цифрових та інших технологій, штучного інтелекту в протидії злочинності, зокрема, у судовій експертології й досудовому слідстві.

Майбутні розвиток, формування та використання криміналістичних знань обумовлені науково-технічним прогресом. Так, ми поділяємо думку відомого криміналіста В. Ю. Шепітька про те, що створення інформаційного соціального середовища сприяло технологізації криміналістики, розробленню й упровадженню інформаційних, телекомунікаційних, цифрових та інших сучасних технологій і штучного інтелекту. У нових умовах криміналістика від традиційного вивчення матеріально фіксованих слідів переходить до дослідження звукових, електронних або геномних слідів. Змінюються також способи, прийоми й методи роботи з такими слідами, правила їх збирання, дослідження та фіксування [1]. Злочини у сфері сучасних інформаційних та інших технологій набувають міжнародного, транснаціонального характеру, до того ж потерпілі від таких злочинів і самі злочинці можуть перебувати в різних країнах світу (наприклад, злочинці — навіть у місцях позбавлення волі). Для протидії таким видам злочинів особливе значення насамперед має посилення й удосконалення міжнародного співробітництва в цій сфері,

1 Шепітько В. Ю. Роль професора М. В. Салтевського у формуванні методологічних засад криміналістики. *Актуальні питання судової експертизи та криміналістики* : зб. мат-лів міжнар. наук.-практ. конф. (Харків, 07—08.11.2017). Харків, 2017. С. 7—8.

підвищення його ефективності. Сьогодні міжнародні організації й органи влади багатьох країн активно вживають організаційних і правових заходів із запобігання та протидії злочинам у сфері сучасних інформаційних та інших технологій. Із цією метою на базі використання системи криміналістичної класифікації способів вчинення правопорушень у сфері інформаційних технологій розроблено кодифікатор Генерального Секретаріату Інтерполу, де окремо передбачено комп'ютерні злочини [2]. Для запобігання злочинам, скоєним у сфері інформаційних технологій, 23.11.2001 р. в Будапешті підписано Конвенцію Ради Європи про злочинність у сфері комп'ютерної інформації *ETS* № 185, більш відому в Україні під назвою «Конвенція про кіберзлочинність» [3] (далі — *Конвенція*). Вона відкрита для підписання як державами — членами Ради Європи, так і тими державами, які не є її членами, але брали участь у її розробленні (зокрема, її підписали США та Японія). Крім того, Європейський комітет з проблем злочинності Ради Європи (із метою підвищення ефективності протидії таким видам злочинів і правового визначення в Європі групи злочинів, пов'язаних із комп'ютерами й інформаційними технологіями) 1990 р. підготував рекомендації про включення до законодавств європейських країн кримінальних норм «мінімального списку» і «необов'язкового списку» комп'ютерних злочинів. На початку 2002 р. додатково ухвалено Протокол № 1 до Конвенції, який додав до цього переліку злочини із поширення інформації расистського, ксенофобного й іншого характеру, що підбурює до насильницьких дій, ненависті чи дискримінації окремої особи або групи осіб і/або ґрунтується на расовій, національній, релігійній або етнічній належності. Згаданий Протокол також ратифіковано Верховною Радою України. Згідно з Конвенцією злочини класифіковано за чотирма групами, а саме: 1) спрямовані проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), вплив на комп'ютерні дані (протиправне навмисне пошкодження, знищення, погіршення якості, зміна або блокування комп'ютерних даних) (ст. 4) або системи (ст. 5)), протизаконне використання спеціальних технічних пристроїв (ст. 6) і комп'ютерних програм, розроблених або адаптованих для скоєння злочинів, передбачених у ст. 25, а також комп'ютерних паролів, кодів доступу, їх аналогів, за допомогою яких можна отримати доступ до комп'ютерної системи загалом або будь-якої її частини (норми ст. 6 застосовують тільки в разі, якщо використання (поширення) спеціальних технічних пристроїв спрямовано на скоєння протиправних діянь); 2) пов'язані з використанням комп'ютерних засобів (підроблення та шахрайство з використанням комп'ютерних технологій (ст. 7, 8): зловмисні й протиправні введення, зміна, видалення або блокування комп'ютерних даних, що тягнуть за собою порушення автентичності даних із наміром, щоб їх розглядали або використовували з юридичною метою як автентичні); 3) здійснювані з метою розповсюдження за допомогою комп'ютерних систем (надання пропозицій

2 Операції з кіберзлочинності / Інтерпол : офіц. вебсайт. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations (дата звернення: 06.11.2021).

3 Конвенція про кіберзлочинність : ратифік. Законом України від 07.09.2005 р. № 2824-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 06.11.2021).

для користування, поширення та придбання різних видів дитячої порнографії, а також наявність дитячої порнографії в пам'яті комп'ютера певної особи; ст. 9); 4) пов'язані з порушенням авторського права й суміжних прав на програмне забезпечення (ст. 10; в Україні — ст. 176 Кримінального кодексу [4], далі — *КК України*) [5].

Відповідно до чинного законодавства України вже до 2021 р. рівень розвитку інформаційного суспільства в нашій державі мав гармонізувати із загальносвітовим шляхом інтеграції національного та всесвітнього інформаційних просторів. Утім, для повноправного користування благами інформаційного суспільства нашій країні слід прийняти також негативні наслідки такого розвитку — більш сучасні й інтенсивні способи (замість традиційних) учинення кримінальних правопорушень. Тож ми поділяємо позицію В. П. Бахіна про те, що криміналістика має працювати на прогнозування та запобігання тому, що може стати злочинами в найближчому майбутньому [6], а це цілком стосується й дослідження та вирішення проблем протидії скоєнню злочинам у сфері телекомунікаційних, інформаційних, комп'ютерних, цифрових технологій, штучного інтелекту й інших новітніх досягнень науки та техніки. За результатами аналізу стану криміногенної обстановки простежується тенденція усе частішого використання злочинцями інформації як предмета посягання чи інструмента злочинної діяльності в інформаційному середовищі (кіберпросторі) на різноманітні правовідносини — від сфери національної безпеки до сфери приватної власності. Механізм і динаміка таких злочинів значно ускладнюють правоохоронним органам досудові розслідування, а судам — розгляд кримінальних проваджень. За статистикою у кримінальному провадженні впродовж 2014—2018 рр. перебувало злочинів, скоєних із використанням високих інформаційних технологій: 2014 р.— 4883, 2015 р.— 6026, 2016 р.— 6219, 2017 р.— 10 872, 2018 р.— 11 131. Водночас (на тлі загального зростання рівня кіберзлочинності) показник розкриття таких злочинів має тенденцію до щорічного зниження — зокрема, слідчі склали обвинувальних актів: 2014 р.— 797, 2015 р.— 756, 2016 р.— 453, 2017 р.— 764, 2018 р.— 666 [7].

Досліджуючи кримінологічні чинники скоєння злочинів у кіберпросторі, Д. Маренич з'ясувала, що 2009 р. було засуджено 56 осіб, 2010 р.— 69, 2011 р.— 56, 2012 р.— 80, 2013 р.— 49, хоча зареєстровано таких кримінальних проваджень у рази більше. Серед засуджених більшість чоловіків — 90,82 %, жінок — 8 %, і їх кількість зменшується (так, 2009 р. їх частка складала 21,5 %, 2010 р.— 8,7 %, 2011 р.— 12,5 %, 2012 р.— 1,25 %, 2013 р.— 6,1 %). Найбільша кримінальна активність характерна для осіб віком від 30 до 50 років (44,92 %), віком від 25 до 30 років — 27,2 %, віком від 16 до 18 років — 0,33 %, а віком від 50 до 65 років — 4,91 % (отже, хакери — не обов'язково підлітки). Водночас серед засуджених осіб 44,9 % працездатні, але ніде не працювали

4 Кримінальний кодекс України від 05.04.2001 р. № 2341-III (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 06.11.2021).

5 Конвенція про кіберзлочинність … . URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 06.11.2021).

6 Бахин В. П. Криминалистика. Проблемы и мнения (1962—2002). Киев, 2002. С. 15.

7 Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А. Ф. Волобуєва. Одеса, 2020. С. 5.

й не навчалися [8]. Така сама тенденція простежується й останніми роками. Зазначене свідчить про недостатню готовність правоохоронних органів протидіяти не лише проявам кіберзлочинності, а й традиційній технічно оновленій злочинності.

Оскільки зі злочинною метою все активніше використовують інформаційні, телекомунікаційні, цифрові й інші технології, а також мережі кіберпростору, різноманітні види засобів зв'язку, штучний інтелект та інші сучасні досягнення науки й техніки, то нагальною стає необхідність відбору, застосування й адаптування всіх цих засобів до потреб криміналістики, експертології й досудового слідства, а саме розроблення відповідних методик розслідування, які б передбачали застосування єдиних методів, засобів і прийомів для вирішення типових завдань досудового розслідування на різних його етапах [9], що спонукало обрати саме таку тему цієї статті.

Аналіз основних досліджень і публікацій

Подібну проблематику розглядали: О. В. Баулін, Ф. Ю. Бердичевський, А. С. Білоусов, Л. В. Борисов, В. М. Бутузов, В. Б. Вєхов, В. О. Голубов, І. М. Гуткін, О. Ю. Довженко, А. Я. Дубинський, В. В. Журавель, Р. А. Калюжний, Л. М. Карнєєв, М. В. Карчевський, О. М. люєв, О. О. Книженко, М. О. Кравцова, В. А. Коршенко, О. М. Ларін, Д. Маренич, О. А. Самойленко, Е. Б. Сімакова-Єфремян, Д. П. Письменний, І. В. Пиріг, В. О. Приходько, М. А. Погорецький, В. М. Тертишник, В. Ю. Шепітько, В. П. Шеломцев, О. М. Юрченко, О. О. Юхно та ін. [10] Розглянемо докладніше деякі дисертації, у яких досліджено порушені питання. Так, питання

8 Маренич Д. Соціально-демографічні ознаки особи, що вчинила злочин у сфері використання ЕОМ, систем, комп'ютерних мереж, мереж електрозв'язку. *Вісник прокуратури*. 2014. № 9. С. 91—97.

9 Самойленко О. А. Зазнач. твір.

10 Клюєв О. М. Удосконалення експертного забезпечення правосуддя: теоретичні, правові та організаційні аспекти. *Теорія та практика судової експертизи і криміналістики* : зб. наук. пр. 2019. Вип. 19. С. 102—117. DOI: 10.32353/khrife.1.2019.08 (дата звернення: 06.11.2021) ; Шепітько М. В. Проблеми виявлення та розслідування злочинів проти правосуддя, що вчиняються професійними учасниками судочинства (провадження). *Там само*. С. 48—57. DOI: 10.32353/khrife.1.2019.04 (дата звернення: 06.11.2021) ; Шепітько В. Ю., Авдєєва Г. К. Проблеми застосування науково-технічних засобів та інноваційних продуктів у діяльності органів правопорядку. *Там само*. Вип. 20. С. 11—26. DOI: 10.32353/khrife.2.2019.01 (дата звернення: 06.11.2021) ; Хараберюш І. Ф. Окремі погляди щодо співвідношення спеціальної техніки правоохоронних органів та криміналістичної техніки. *Там само*. С. 88—102. DOI: 10.32353/khrife.2.2019.06 (дата звернення: 06.11.2021) ; Філіпенко Н. Є., Снігерьов О. П., Бубліков А. В. Застосування спеціальних знань під час виявлення, профілактики й розслідування злочинів у сфері комп'ютерної інформації та високих технологій (оглядова стаття). *Там само*. 2020. Вип. 22. С. 162—178. DOI: 10.32353/khrife.2.2020.12 (дата звернення: 06.11.2021) ; Пиріг І. В., Приходько В. О. Криміналістичні обліки: проблеми класифікації. *Там само*. 2021. Вип. 23. С. 45—60. DOI: 10.32353/khrife.1.2021.03 (дата звернення: 06.11.2021) ; Сімакова-Єфремян Е. Б. Впровадження новітніх методів експертних досліджень та підходів до здійснення судово-експертної діяльності — необхідний фактор експертного забезпечення правосуддя. *Інноваційні методи та цифрові технології в криміналістиці, судовій експертизі та юридичній практиці* : мат-ли міжнар. «кругл. столу» (Харків, 12.12.2019). Харків, 2019. С. 123—128 та ін.

кримінологічної характеристики кіберзлочинності та запобігання їй органами внутрішніх справ вивчала 2016 р. М. О. Кравцова; теоретичні й методичні основи судової телекомунікаційної експертизи 2017 р. розглядав В. А. Коршенко; проблемам основ методики розслідування злочинів, скоєних у кіберпросторі, 2020 р. присвятили роботи О. А. Самойленко й О. Ю. Довженко. Окремо слід акцентувати увагу на інших дослідженнях, результати яких викладено в наукових працях, зокрема: В. М. Бутузова «Протидія комп'ютерній злочинності в Україні» і «Організація боротьби зі злочинами у сфері високих технологій», Ю. М. Юрченка «Запобігання злочинам у сфері високих технологій: погляд в майбутнє», М. В. Карчевського «Злочини в сфері використання ЕОМ, систем комп'ютерних мереж та мереж електрозв'язку, що вчиняються організованими злочинними групами та злочинними організаціями: проблеми кваліфікації та попередження».

Проте, генезис вирішення криміналістичних, процесуальних і організаційних питань щодо застосування сучасних телекомунікаційних, інформаційних, комп'ютерних і цифрових технологій у криміналістиці, експертній діяльності й досудовому розслідуванні останнім часом комплексно не досліджено.

Зважаючи на стрімкий розвиток сучасних новітніх інформаційних та інших зазначених вище технологій, окремі теоретичні та правозастосовні криміналістичні, організаційні, оперативно-розшукові та процесуальні особливості використання таких технологій і мереж у криміналістиці, судовій експертології, досудовому розслідуванні потребують подальших комплексних і концептуальних досліджень. Водночас залишаються невирішеними проблемні питання протидії латентності таких видів злочинів, оскільки мінімізувати латентність можна, зокрема, і шляхом впливу на осіб, які скоюють такі злочини. Тому зростає значення досліджень криміналістичної характеристики та кримінологічного портрета злочинця й розв'язання решти нагальних питань, які зумовлять напрями подальших наукових розвідок. У межах цієї наукової статті спробуємо дослідити порушені питання та запропонувати шляхи вирішення окремих проблем (зокрема, щодо відбору, ліцензування, запровадження, адаптування й використання новітніх досягнень науки і техніки).

Недоліки теорії та практики, а також несвоєчасність відбору, ліцензування, апробації й запровадження сучасних досягнень науки та техніки в криміналістику, експертну діяльність і правозастосовну діяльність досудового слідства певною мірою знижують ефективність виявлення, розкриття й розслідування кримінальних правопорушень, скоєних із застосуванням новітньої техніки, проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій органами слідства, дізнання, прокуратури, оперативними підрозділами, що негативно впливає на своєчасність і якість досудового розслідування й судового розгляду загалом та розроблення відповідних методик розслідування кримінальних правопорушень зокрема.

Мета роботи

Метою є аналіз історичного розвитку й сучасного стану криміналістичних, процесуальних і організаційних проблемних питань з відбору, ліцензування, використання, адаптування сучасних інформаційних, цифрових, телекомунікаційних, комп'ютерних та інших технологій (зокрема, штучного

інтелекту) у криміналістиці, експертній діяльності та досудовому розслідуванні, а також нормативно-правової бази, що регулює окремі питання цього напряму.

Основне завдання — виробити пропозиції й рекомендації щодо шляхів вирішення виявлених проблемних питань на теоретичному, правозастосовному та законодавчому рівнях.

Наукова новизна дослідження. Наукове дослідження має такі елементи новизни: *уперше* його здійснено на перетині криміналістики, експертології, кримінального права та процесу; проаналізовано історичний розвиток і сучасний стан відбору, ліцензування, запровадження й використання досягнень науки та техніки (зокрема, у сфері інформаційних, телекомунікаційних, комп'ютерних, цифрових та інших технологій, засобів і мереж), а також розроблення за їх допомогою відповідних методик розслідування; удосконалено пропозиції й рекомендації щодо розв'язання наявних проблемних питань шляхом кардинальних змін наукової парадигми криміналістики, експертології та досудового розслідування із застосуванням інновацій.

Викладення основного матеріалу дослідження

Стрімкий і динамічний розвиток інформаційних, телекомунікаційних, комп'ютерних, цифрових та інших технологій, штучного інтелекту щодня все більше змінює аспекти економічного, політичного й соціального життя всіх країн світу. У середині 1950-х рр. не кожна родина мала телевізор, у середині 1970-х — персональний комп'ютер, а сьогодні нікого не здивуєш індивідуальним смартфоном. За даними *Nua Internet Surveys,* кількість користувачів глобальної мережі «Інтернет» із 80 тис. (1988) зросла до 4,5 млрд (2020) і продовжує збільшуватись. Від часу набрання Кримінальним процесуальним кодексом України (далі — *КПК України*) чинності кожен службовий персональний комп'ютер слідчого, із якого здійснюють пошук у Єдиному реєстрі досудового розслідування (далі — *ЄРДР*), має підключення до інтернету, що надає працівникам правоохоронних органів низку сучасних інформаційних інструментів для реєстрації заяв і повідомлень про кримінальні правопорушення та проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій.

Збільшення кількості персональних комп'ютерів та користувачів інтернету, мобільних телефонів і їх різновидів впливає на кількість злочинів, скоєних із використанням сучасних інформаційних технологій. Про це свідчать статистичні дані: в Україні таких злочинів 2016 р. зареєстровано 217, а 2018 р.— уже 6000, а надалі їх щорічне зростання склало понад 25 %, ураховуючи значну латентність і недосконалість чинного законодавства тощо. У зв'язку із цим у системі МВС України створено спеціальні підрозділи протидії кіберзлочинам, що напрацьовують відповідні методики та практику за цим напрямом організаційної, слідчої, оперативно-розшукової й іншої діяльності. Невипадково ООН іще 1992 р. додала до переліку транснаціональних організованих такі види злочинів, дорівнявши їх до: незаконного відмивання грошей; терористичної діяльності; організованого наркобізнесу; крадіжок витворів мистецтв, інтелектуальної власності; незаконної торгівлі зброєю, людьми й людськими органами; захоплення повітряних суден і наземного транспорту; морського піратства; шахрайства; екологічних злочинів. Якщо сьогодні різні соціальні верстви та різні вікові категорії насе-

лення використовують зазначені вище й інші новітні технології (особливо мережу «Інтернет»), і таке використання стає день у день активнішим, то в діяльності правоохоронних органів (зокрема, органів поліції) — через обмежене фінансування — відбір таких технологій, їх застосування, адаптування та вирішення питань ліцензування відбуваються доволі повільно.

На виконання рекомендацій міжнародних інституцій і міжнародних правових актів вітчизняні законодавці передбачили кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (далі — *ЕОМ*) і комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку в Україні. Родовим об'єктом злочинів, відповідальність за які обумовлено розд. XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» КК України [11], є сукупність відносин, що виникають щодо оброблення (збирання, уведення, записування, перетворення, зчитування, зберігання, знищення, реєстрування), захисту комп'ютерної інформації й експлуатації ЕОМ, комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Предметом злочинів, відповідальність за які передбачена розд. XVI КК України, можуть бути: 1) електронно-обчислювальні машини (комп'ютери); 2) автоматизовані системи; 3) комп'ютерні мережі; 4) мережі електрозв'язку; 5) інформація; 6) програмні чи технічні засоби; 7) повідомлення електрозв'язку. Маємо зауважити, що розд. XVI КК України характеризується неузгодженістю термінів (як у самому розділі, так і щодо решти нормативно-правових актів), а термін *ЕОМ* (*ЕОМ (комп'ютер)* — це будь-який пристрій або група взаємно поєднаних пристроїв, один чи більше з яких, відповідно до певної програми, автоматично обробляє інформацію й обладнаний допоміжним устаткуванням (пристосуванням), що дає змогу змінювати або перезаписувати керівні програми і/або дані, необхідні для реалізації процесором його цільових функцій) узагалі сьогодні вже є архаїчним. Уже існують оптичні, квантові й біокомп'ютери, тобто комп'ютери, що базуються на відмінних від електронної технологіях, тому термін *ЕОМ* — це дефініція, застосування якої невдовзі (у разі використання комп'ютерними злочинцями нових нейрокомп'ютерів і/або об'єктів штучного інтелекту) уже не дасть змоги криміналізувати протиправні діяння. Згідно зі ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» інформаційна (автоматизована) система — це організаційно-технічна система, у якій реалізується технологія оброблення інформації з використанням технічних і програмних засобів [12].

Як відомо, *комп'ютерна мережа* — це комплекс (сукупність) з'єднаних лініями зв'язку комп'ютерів. Залежно від швидкості обміну даними між робочими комп'ютерами й розмірів охопленої території розрізняють локальні, регіональні та глобальні комп'ютерні мережі.

11 Кримінальний кодекс України … . URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text (дата звернення: 06.11.2021).

12 Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 05.07.1994 р. № 80/94-ВР (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text (дата звернення: 06.11.2021).

Зважаючи на положення ст. 1 Закону України «Про телекомунікації» [13], можна дійти висновку, що *мережі електрозв'язку* (як синонім до телекомунікаційних мереж) — це комплекс технічних засобів телекомунікацій і споруд, призначених для маршрутизації, комутації, передавання і/або приймання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого роду по радіо, проводових, оптичних чи інших електромагнітних системах між кінцевим обладнанням.

Співпраця криміналістів, математиків, фізиків і представників інших галузей науки у розробленні кібернетичних методів дослідження сприяла запровадженню сучасних технічних досягнень у судово-експертну практику. Зокрема, комп'ютерні технології сьогодні є незамінним ефективним засобом роботи сучасного слідчого, дізнавача, експерта, прокурора, судді та ін. і основним способом удосконалити таку роботу [14]. Саме тому існує нагальна потреба дослідити генезис вирішення криміналістичних, процесуальних та організаційних проблемних питань щодо використання інформаційних, телекомунікаційних, комп'ютерних і цифрових технологій у теорії, правозастосовній та експертній діяльності, криміналістиці та кримінальному процесі, а також їх тенденції й певний науковий досвід з метою подальшого вдосконалення та розв'язання порушених у цій статті проблемних питань.

Іще 1969 р. Л. Ю. Ароцкер зазначав, що для практичного використання ЕОМ в експертній діяльності та практиці потрібно розробити алгоритми й режими їх роботи, які б дали змогу забезпечити достатню надійність відповідей для здійснення ідентифікаційних завдань і правильне вирішення як організаційних, так і процесуальних питань, без чого неможливе подальше використання ЕОМ у діяльності судових експертів [15]. Дискутуючи щодо цього, Р. М. Ланцман також зазначав, що першочергового вирішення потребують питання організаційного та процесуального характеру (зокрема, на якій стадії науково-експериментальної перевірки надійності ЕОМ їх можна застосовувати для проведення судових експертиз). За його твердженням, література 1968 р. вже містила описи застосування ЕОМ під час проведення експертиз, однак тоді правильного розпізнання досягли не за всіма випадками та напрямами [16].

Важливою умовою застосування ЕОМ в експертній практиці є відсутність грубих помилок в роботі ЕОМ за кожним із алгоритмів, які перевіряють. Якщо певні види сучасних технічних засобів, працюючи за визначеним алгоритмом, експериментальним шляхом і в достатній кількості дослідів дають правильні відповіді, то такий алгоритм можна використовувати також під час проведення судових експертиз. В іншому разі завжди існують сумніви в надійності обраного експертом алгоритму.

13 Про телекомунікації : Закон України від 18.11.2003 р. № 1280-IV (зі змін. та допов.). URL: https://zakon.rada.gov.ua/laws/show/1280-15#Text (дата звернення: 06.11.2021).

14 Іванов В. Г., Іванов С. М., Карасюк В. В. та ін. Правова інформація та комп'ютерні технології в юридичній діяльності : навч. посіб. / за заг. ред. В. Г. Іванова. 4-те вид., змін. і допов. 2014. С. 4.

15 Ароцкер Л. Е. Организационные и процессуальные вопросы использования электронно-вычислительных машин в экспертной практике. *Криминалистика и судебная экспертиза*. 1969. Вып. 6. С. 182—183.

16 Ароцкер Л. Е., Ланцман Р. М. Кибернетика и криминалистическая экспертиза почерка. Москва, 1968. С. 51, 83—85.

Свого часу, коли наукова спільнота тільки-но порушила ці питання, М. С. Строгович зазначав, що застосовувати у слідчій, експертній і судовій практиці нові прийоми й засоби, розроблені технічними та природничими науками, можна тільки у разі, коли їх усебічно перевірено, а їх засоби здатні давати достовірні результати [17].

Застосовуючи сучасні технічні досягнення й ЕОМ для дослідження речових доказів, судовий експерт повинен з'ясувати механізм дослідницької діяльності конкретного новоствореного технічного пристрою, зрозуміти, за якими ознаками й механізмами відбуваються розпізнавання, вирішення поставленого завдання та ухвалення рішення. Без цього експерт не має права послуговуватися такими новітніми науковими досягненнями, технікою тощо, а також надавати висновок слідчому, дізнавачу, прокурору, слідчому судді, суду, адже умови й характер процесуальної діяльності цих осіб не припускають застосування методів дослідження, якщо експерт не розуміє сутності цих методів.

Безумовно, віра в абсолютну об'єктивність ЕОМ та інших досягнень науки й водночас нерозуміння механізму їх діяльності, ознак, якими вони оперують, не дає експертові права використовувати ЕОМ та інші досягнення науки під час проведення судової експертизи.

Посилання на можливість застосування ЕОМ в інших галузях людської діяльності, навіть за незнання механізму їх роботи, у правозастосовній діяльності не працюють, оскільки в ній (зокрема, у судовому дослідженні), на відміну від будь-якої іншої діяльності, кожен факт має бути доказано й обґрунтовано.

На переконання Л. Г. Еджубова, різні види завдань експертного дослідження передбачають розроблення різноманітних алгоритмів, кожний із яких має розв'язувати конкретне експертне завдання. Неможливо розробити єдиний універсальний алгоритм для дослідження всіх об'єктів навіть одного виду експертизи. У зв'язку із цим виникає потреба розробити й запровадити в експертну діяльність і слідчу й судову практику системи різних алгоритмів, покликані вирішувати конкретний клас завдань [18], що є актуальним до сьогодні. Він констатував, що такий підхід у той час (1968) найчастіше застосовували до проведення судово-почеркознавчих експертиз.

Потреба в декількох алгоритмах існуватиме й надалі — для розроблення й удосконалення кібернетичних методів багатьох видів судових експертиз, що даватиме змогу вирішувати одне слідче завдання за допомогою декількох алгоритмів, оскільки однозначні результати, здобуті завдяки застосуванню різних алгоритмів, більш переконливі.

Думка тогочасних науковців щодо необхідності постійного відбору, застосування й адаптування новітніх досягнень науки та техніки в експертній діяльності за окремими напрямами є слушною до сьогодні. Наприклад, ідентифікація слідів пальців рук особи під час дактилоскопічної експертизи за допомогою ЕОМ (комп'ютерів) значно прискорює процес, на відміну від опрацювання картотечних криміналістичних обліків слідів пальців рук людини

17 Строгович М. С. Курс советского уголовного процесса. В 2 т. Т. 1. Основные положения науки советского уголовного процесса. Москва, 1968. С. 83.

18 Эджубов Л. Г. Актуальные вопросы использования электронных цифровых вычислительных машин в судебном почерковедении. *Проблемы правовой кибернетики* : мат-лы симп. Москва, 1968. С. 167—168.

вручну працівниками експертних закладів. Сучасними дронами (безпілотними летальними апаратами й наземними та підводними безпілотниками) кермують за допомогою спеціальних персональних комп'ютерів під час огляду місця події в разі, коли предмети злочину або частини тіл потерпілих знаходяться на певній відстані від основного місця події, або коли їх застосовують для затримання злочинців «на гарячому» та ін. Для протидії загрозі вибуху на місці події вибухотехнічні криміналістичні лабораторії застосовують робототехніку для ідентифікації вибухового пристрою.

Активно послуговуються комп'ютерною технікою й мережами у правозастосовній діяльності, а вільний доступ до відповідних криміналістичних та інших обліків дасть змогу слідчому, дізнавачеві, оперативному працівникові значно пришвидшити першочергові слідчі (розшукові) дії (наприклад, зі встановлення особи злочинця, геномні сліди якого виявлено на місці події). Перспективним є поповнення криміналістичних обліків такими новими видами, як: фіксування райдужної сітківки ока, відеокомп'ютерне розпізнавання особи за зображенням, рентгенограма тулуба, геномні портрети та ін.

Використання сучасних досягнень науки й техніки дає змогу розширити коло питань, які можуть вирішувати експерти. Так, у разі розслідування злочинів у сфері використання ЕОМ, комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку, проводять як традиційні криміналістичні (трасологічні, почеркознавчі, речовин і матеріалів та ін.), економічні, судово-бухгалтерські експертизи, так і спеціальні для цього складу злочинів комп'ютерно-технічні експертизи. Відповідно до завдань і специфіки об'єктів дослідження сьогодні у межах цього виду можна виокремити такі підвиди експертизи: 1) технічну комп'ютерів і периферійних пристроїв; 2) технічну обладнання захисту комп'ютерної інформації; 3) машинних даних, використовуваних у комп'ютерній мережі [19]. Методичні основи судової телекомунікаційної експертизи, яку успішно впроваджено в діяльність експертних установ України, 2017 р. заклав В. А. Коршенко. Зокрема, він визначив, що *телекомунікаційна експертиза* — це рід класу інженерно-технічних експертиз, яка передбачає дослідження експертом на основі спеціальних знань телекомунікаційних систем, засобів, мереж, їх складових та інформації, яку вони передають, приймають та обробляють, що містять відомості про обставини справи, яка перебуває у провадженні органів досудового розслідування чи суду. Він аргументував, що родовим об'єктом цієї експертизи є матеріальні об'єкти, їх сукупність або частини, що за своїми характеристиками могли або за певних умов можуть передавати, випромінювати і/або приймати знаки, сигнали, текст, зображення, звуки, повідомлення й іншу інформацію за допомогою радіо, дротових, оптичних, електромагнітних та інших систем, а також програмне забезпечення й інформація, яку містять ці об'єкти [20].

Із метою повного, швидкого та неупередженого розслідування (ст. 2 КПК України) кіберзлочинів, для обрання певної тактики й методики розслідуван-

19 Панов М. І., Шепітько В. Ю., Коновалова В. О. Настільна книга слідчого. 3-тє вид., перероб. і допов. Київ, 2011. С. 536—537.

20 Коршенко В. А. Теоретичні та методичні основи судової телекомунікаційної експертизи : автореф. дис. … канд. юрид. наук. Харків, 2017. С. 12—15.

ня слідчий, дізнавач, прокурор, суддя повинні знати криміналістичну характеристику таких тактики й методики. Щодо цього наукові дискусії тривають до сьогодні. Тому вважаємо доцільним зупинитися на криміналістичній характеристиці інформаційних і кіберзлочинів, що містить такі елементи: особи злочинця й потерпілого, предмет злочинного посягання, спосіб (способи) скоєння злочинів, слідову картину.

О. Г. Волеводз і Д. Маренич зазначають, що особа злочинця найчастіше вирізняється активною життєвою позицією, витонченістю, хитрістю, оригінальним і нестандартним мисленням та поведінкою, обережністю, уважністю, пильністю, деяким талантом до передбачення під час підготовки та скоєння злочина, а також певною післязлочинною поведінкою і маскуванням. Із психофізіологічного боку це яскрава, мисляча та творча особистість, знавець своєї справи, здатна на технічний виклик, бажаний студент і/або працівник. Однак, така особа боїться втратити свій авторитет чи соціальний захист у межах соціальної групи або побоюється глузувань. Її поведінка зовні найчастіше відповідає загальноприйнятим у суспільстві соціальним нормам. Як підтверджує слідча й судова практика, комп'ютерні злочинці здебільшого не мають кримінального минулого, а ті особи, які вже перебувають у місцях позбавлення волі, намагаються опанувати знання в цій галузі та використовують їх за наявності корумпованих зв'язків із адміністрацією виправних установ для скоєння кримінальних правопорушень, скеровуючи їх за межі місць ув'язнення. За визначенням науковців, значну частину таких злочинів вчинено індивідуально, проте останнім часом спостерігається тенденція до співучасті в групових посяганнях [21]. Установлюючи особи виконавців таких злочинів, слід зважати на їх можливі трудові відносини з потерпілою організацією, особливості поведінки на роботі, види технічних посад, які посідають злочинці на момент скоєння кримінального правопорушення, групу осіб, що підлягає перевірці, способи підготовки, скоєння та приховування слідів комп'ютерних злочинів, а також вік особи, мотив і мету злочинних дій, сферу злочинної діяльності (хакери, крекери, фрікери та ін.), фінансові й технічні можливості, своєрідність комп'ютерних знань тощо, схеми дій різних груп злочинців (хакер-одинак, об'єднана хакерська група, підприємство-конкурент, представники різних структур відомчого, міжвідомчого рівня), особливості особи злочинця залежно від виду комп'ютерного злочину та ін.

Наступним елементом криміналістичної характеристики таких видів злочинів є особа потерпілого. Відповідно до чинного КПК України і статистичних даних потерпілою стороною можуть бути як фізичні, так і юридичні особи. Здебільшого потерпілими є юридичні особи (підприємства всіх форм власності, установи, відомства, організації).

Ураховуючи право власності на комп'ютерну систему, у юридичній літературі виокремлюють три групи потерпілих від таких видів злочинів: власники комп'ютерних систем — 79 %; клієнти власників комп'ютерних систем — 13 %; треті особи — 8 %. Основні елементи криміналістичної характеристики комп'ютерних злочинів різняться розмаїттям способів підготовки,

21 Волеводз А. Г. Следы преступлений, совершенных в компьтерных сетях. *Российский следователь*. 2002. № 1. С. 4—12 ; Маренич Д. Криміналістична характеристика кіберзлочинів. *Вісник прокуратури*. 2014. № 12. С. 113—120.

скоєння та приховування кримінальних правопорушень, особливістю яких є комп'ютерні об'єкти, способи скоєння, специфічна віртуальна слідова картина, що відображається на апаратних, програмних чи інформаційних елементах комп'ютерних чи інших подібних об'єктах, а також особи злочинця й потерпілого. Скоєння таких злочинів пов'язано з використанням різноманітних носіїв комп'ютерної, телекомунікаційної чи іншої інформації різного походження, зокрема: пам'ять комп'ютера, лінії електрозв'язку, роздруківки матеріалів та ін. За визначенням А. С. Білоусова, для роботи з такими об'єктами потрібні різноманітні технічні засоби, навички та спеціальні знання [22].

Черговим важливим елементом криміналістичної характеристики таких видів злочинів є способи їх скоєння, до яких належать акти поведінки й дій правопорушника, спрямовані на підготовку, скоєння та приховування кримінального правопорушення. Підготовчий етап скоєння кіберзлочинів чи інших інформаційних злочинів визначено системою способів, серед яких: перехоплення інформації, отримання несанкціонованого доступу до засобів комп'ютерної чи іншої інформаційної, телекомунікаційної й іншої техніки; маніпулювання комп'ютерними даними та керівними командами комп'ютерної техніки; копіювання й тиражування; подолання програмних засобів захисту. Способи приховування злочинів зумовлено способами їх скоєння. У криміналістичній літературі запропоновано кілька класифікацій способів скоєння кіберзлочинів. За визначенням В. М. Бутузова, В. М. Гавловського, Л. П. Скалозуба, залежно від того, як саме здійснено доступ до комп'ютерної чи іншої інформації, виокремлюють такі способи скоєння досліджуваних злочинів: 1) безпосередній доступ, за якого інформацію блокують, модифікують, копіюють, а також знищують; 2) опосередкований (віддалений) доступ до комп'ютерної чи іншої інформації, здійснений на відстані з іншого комп'ютера через комп'ютерну мережу; 3) змішані способи, здійснені як за безпосереднього, так і за опосередкованого (віддаленого) доступу [23]. Слід зазначити, що до елементів криміналістичної характеристики належить і предмет злочинного посягання, зокрема: інформація, кошти, персональні дані, що загалом також зумовлюють різні способи скоєння таких видів кримінальних правопорушень.

Залежно від предмета злочинного посягання, виокремлюють такі групи способів скоєння досліджуваних злочинів: 1) інформаційні — незаконні способи здобуття інформації, зокрема шляхом несанкціонованого доступу до комп'ютерів і мереж, поширення неправдивої інформації; 2) фінансові — їх інколи визначають як «злам» банківських систем безпеки, отримання безкоштовних послуг телефонного зв'язку, крадіжки коштів із кредитних карток, створення електронних пірамід, шахрайство у вигляді віддалених продажів або робіт тощо; 3) такі, що завдають шкоди здоров'ю й загрожують життю людей (виведення з ладу медичного обладнання, тероризування особи та ін.).

22 Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : автореф. дис. … канд. юрид. наук. Київ, 2008. С. 19.

23 Бутузов В. М., Гавловський В. Д., Скалозуб Л. П. та ін. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : навч. посіб. / за заг. ред. Л. П. Скалозуба, І. В. Бондаренка. Київ, 2010. С. 59—62.

Останнім і суттєвим елементом криміналістичної характеристики таких злочинів є їх слідова картина. Вона демонструє, як правопорушник потрапив на місце злочину та як зник звідти, подолав перешкоди, використав своє службове становище, досягнув поставленої перед собою (і співучасниками) злочинної мети, які застосував знання й навички, чи намагався приховати сліди своїх злочинних дій. Важливими для слідства та дізнання є також сліди, що свідчать про характер зв'язку злочинця з предметом злочинного посягання та ін. Варто наголосити, що в криміналістиці слідову картину кіберзлочинів визначають як сукупність інформації про типові сліди як ознаки й умови скоєння кримінального правопорушення, що характерні для певних способів скоєння незаконного втручання в роботу ЕОМ (комп'ютерів), систем комп'ютерних мереж і перебувають у кореляційній залежності з особою злочинця та предметом посягання.

Сліди скоєння кіберзлочинів можуть бути матеріальними (зокрема, рукописні записи, роздруківки та ін.) і свідчити про підготовку до злочину та про сам злочин. Матеріальні сліди можуть залишитися на обчислювальній техніці (сліди від пальців рук, мікрочастинки на клавіатурі, дисководах, принтері та ін.), а також на магнітних носіях і оптичних дисках. Окрім цього, існують інформаційні сліди, що утворюються внаслідок впливу на комп'ютерну інформацію (шляхом знищення, перекручення). Передусім їх залишають на магнітних носіях інформації, вони пов'язані зі змінами, які відбулися в самій інформації порівняно з початковим станом. Також до інформаційних слідів належать наслідки роботи антивірусних і тестових програм, які можна виявити під час вивчення комп'ютерного обладнання, робочих записів програмістів, протоколів роботи антивірусних програм і програмного забезпечення. Із метою виявлення таких слідів доцільно залучити спеціаліста з комп'ютерної техніки та програмного забезпечення [24]. Беручи участь у дослідженні закономірностей скоєння кіберзлочинів, В. О. Мещеряков зауважує, що аналіз особливостей формування слідової картини таких злочинів потребує запровадження поняття «віртуальні сліди» (як проміжні між матеріальними й ідеальними слідами) [25]. Криміналісти не тільки підтримали його наукову позицію, а й розвинули її. Так, О. Г. Волеводз констатує, що, з огляду на особливість віртуальних слідів, їх не можна вилучити, а лише скопіювати із застосуванням різних програмно-технічних засобів [26].

Слід зазначити, що віртуальні сліди існують об'єктивно на матеріальних носіях, але не доступні для безпосереднього сприйняття. Для їх сприйняття потрібно обов'язково застосувати програмно-технічні засоби. Наявність таких слідів на матеріальному носії наближує цю групу до матеріальних слідів, але не підтверджує їх як такі. При цьому маємо наголосити, що віртуальні сліди

24 Панченко В. М. Сучасний стан та проблеми боротьби з Інтернет-злочинністю. *Боротьба з Інтернет-злочинністю* : мат-ли міжнар. наук.-практ. конф. (Донецьк, 12—13.06.2013). Донецьк, 2013. С. 8 ; Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. … канд. юрид. наук. Київ, 2005. С. 18.

25 Мещеряков В. А. Основы методики расследования преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук. Воронеж, 2001. С. 21.

26 Волеводз А. Г. Указ. соч.

(через природу свого існування), отримані з матеріального носія та сприйняті внутрішньо, не надійні, а тому їх можна неправильно прочитати. Наприклад, застосувавши програмно-технічні засоби, такі сліди легко підробити або втратити. Вони подібні до ідеальних, але їх не можна ототожнювати з ідеальними, оскільки віртуальні сліди зберігаються в ідеальному вигляді, проте, не в пам'яті людини, а в машинній пам'яті й на матеріальних носіях машинної інформації, їх виявляють із використанням технічних засобів за певними алгоритмами.

Виникнення слідів на фізичному рівні викликано природним впливом апаратних комп'ютерних об'єктів: проходженням електричного струму, намагнічуванням або розмагнічуванням певних ділянок магнітного носія в результаті дій злочинця. Такі сліди невидимі, зовнішніх проявів на апаратних елементах комп'ютерних об'єктів не мають. Виявити, зафіксувати, вилучити й дослідити їх можна тільки із застосуванням комп'ютерних апаратних пристроїв і програмних засобів [27].

Одним із досягнень науково-технічної революції XXI ст. є розроблення штучного інтелекту й робототехніки, однак у цій сфері бракує ефективних правових механізмів регулювання. До того ж спостерігається тенденція не стільки впливу права на цю галузь, скільки впливу цифрових технологій на право. Сьогодні доволі актуальним і перспективним є використання штучного інтелекту в криміналістиці й судових експертизах. Розвинені країни світу розглядають штучний інтелект як одну з найважливіших стратегій підвищення конкурентоспроможності та забезпечення національної безпеки. За визначенням О. А. Теличко зі співавторами, штучний інтелект широко використовують у сфері освіти, медичного обслуговування, пенсійного забезпечення, охорони навколишнього середовища, державного управління та правозастосовної діяльності.

Штучний інтелект стає найважливішим чинником розвитку цифрової економіки будь-якої держави, однак можливі загрози від його застосування породжують питання та вимагають правових гарантій безпечного функціювання його систем, до того ж недостатньо досліджено етичні та правові аспекти його використання, він до сьогодні навіть не має одностайного визначення. Також існує проблема формування понятійного апарату штучного інтелекту як чинника регулювання будь-якої нової сфери [28]. Для розв'язання цього проблемного питання розпорядженням Кабінету Міністрів України (далі — *КМУ*) від 02.12.2020 р. схвалено Концепцію розвитку штучного інтелекту в Україні [29], а розпорядженням КМУ від 09.09.2020 р.

27 Шепітько В. Ю. Зазнач. твір. С. 8.

28 Теличко О. А., Рекун В. А., Чабаненко Ю. С. Проблеми визначення та нормативного закріплення поняття «штучний інтелект» у законодавстві зарубіжних країн та України. *Юридичний науковий електронний журнал*. 2021. № 2. С. 310—313. DOI: 10.32782/2524-0374/2021-2/75 (дата звернення: 06.11.2021) ; Шестак В. А., Волеводз А. Г. Современные потребности правового обеспечения искусственного интеллекта : взгляд из России. *Всероссийский криминологический журнал*. 2019. Т. 13. № 2. С. 197—206. DOI 10.17150/2500-4255.2019.13(2).197-206 (дата звернення: 06.11.2021).

29 Про схвалення Концепції розвитку штучного інтелекту в Україні : розпорядження КМУ від 02.12.2020 р. № 1556-р. URL: https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text (дата звернення: 06.11.2021).

затверджено План пріоритетних дій Уряду на 2020 рік із цих питань [30].

Отже, як свідчить дослідження, відбір, використання, адаптування досягнень науки та техніки в криміналістиці, судовій експертології й досудовому слідстві на всіх історичних етапах активно підтримували і сьогодні підтримують науковці та правозастосовувачі. Ми поділяємо слушну думку Н. І. Клименко про те, що знання, які мають слідчий та експерт, цінні лише тоді, коли їх застосовують у практичній діяльності [31], і вважаємо доцільним поширити цю думку на досліджуваний тут напрям.

Висновки

Правове підґрунтя та стан криміногенної обстановки в державі й у світі спонукають до подальших наукових досліджень у сфері використання сучасних досягнень телекомунікаційних, інформаційних, комп'ютерних, цифрових технологій і штучного інтелекту в криміналістиці, судових експертизах та під час досудового розслідування, оскільки цього потребує сучасний стан розвитку науки й техніки, досягненнями яких активно послуговуються кримінально налаштовані особи для скоєння нових видів кримінальних правопорушень.

Дослідження генезису цього питання дало змогу з'ясувати, що вже у XX ст. науковці всебічно вивчали особливості використання досягнень науки й техніки (зокрема, інформаційної, телекомунікаційної, комп'ютерної, мережевої, ЕОМ, засобів зв'язку, штучного інтелекту та ін.) під час проведення досудового слідства й судових експертиз. Подальші наукові розвідки сприяли активній дискусії у цьому напрямі із безсумнівними висновками про доцільність подальшого відбору, ліцензування, апробації, запровадження, застосування й удосконалення нових видів науки та техніки в правозастосовній практиці. Хронологію генезису використання таких знань під час проведення судових експертиз можна визначити за порядком початку їх застосування (зокрема, для проведення почеркознавчих, дактилоскопічних, комп'ютерно-технічних, телекомунікаційних та інших видів експертизи). Найбільшого поширення набули дослідження із використання наукових здобутків цифрових технологій і штучного інтелекту, ДНК-аналізу в теорії криміналістики й практиці судової експертології, слідчих органів, органів дізнання, прокуратури, судів. Згідно з генезисом, уперше питання правового регулювання відносин між людиною і штучним інтелектом 2005 р. порушили південнокорейські вчені, яких підтримав їхній уряд, закріпивши доктринальні положення, зокрема, у «Корейському праві розвитку штучного інтелекту роботів» (2005), «Етичному статуті роботів» (2007), «Правовому регулюванні автономних систем в Південній Кореї» (2012) [32]. Українські законодавці також на нормативному рівні підтримали подальший розвиток, удосконалення та напрям розвитку в Україні штучного інтелекту.

30 Про затвердження плану пріоритетних дій Уряду на 2020 рік : розпорядження КМУ від 09.09.2020 р. № 1133-р. URL: https://zakon.rada.gov.ua/laws/show/1133-2020-%D1%80#Text (дата звернення: 06.11.2021).

31 Клименко Н. І. Криміналістичні знання: поняття, структура, розвиток. *Криміналістика XXI століття* : мат-ли міжнар. наук. практ. конф. (Харків, 25—26.11.2010). Харків, 2010. С. 28.

32 Теличко О. А., Рекун В. А., Чабаненко Ю. С. Зазнач. твір.

Із метою запровадження криміналістичних рекомендацій у правозастосовну діяльність окреслено сучасні завдання криміналістики, зокрема: 1) формалізацію криміналістичних знань; 2) уніфікацію криміналістичних рекомендацій щодо прагматичних цілей; 3) запровадження запропонованих наукою інноваційних розробок [33]. Зважаючи на порушені питання, варто підтримати позиції науковців щодо виокремлення в криміналістиці, зокрема: диференціювання криміналістичних знань; формування нових окремих криміналістичних теорій; комп'ютеризації криміналістичних засобів і методів; розширення слідової картини злочинів, появи нових нетрадиційних слідів; розроблення надчутливих аналітичних методів; виникнення нових слідчих дій, які складно або неможливо здійснити без науково-технічного супроводу; посилення значення науково-технічного забезпечення для проведення досудового розслідування; розроблення нових методик розслідування злочинів, скоєних із застосуванням досягнень науково-технічного прогресу [34].

Отже, дослідження генезису й сучасного стану застосування досягнень науки та техніки в криміналістиці, судовій експертології й досудовому розслідуванні підтверджують прогресивність цього напряму для правозастосовної діяльності та виконання завдань кримінального провадження (ст. 2 КПК України) із метою забезпечення й дотримання прав, свобод і законних інтересів особи в Україні.

Генезис и проблемные вопросы использования новейших технологий и искусственного интеллекта в криминалистике, экспертной деятельности и досудебном расследовании

Александр Юхно

Рассмотрен генезис развития и пути совершенствования теоретических и прикладных направлений криминалистики, судебной экспертологии и уголовного процесса для решения криминалистических, процессуальных, организационных и других проблемных вопросов внедрения и использования достижений науки и техники в досудебном расследовании и судебном разбирательстве уголовных правонарушений на различных исторических этапах развития этого направления в Украине. Отдельно акцентировано внимание на научном подходе к отбору, внедрению, использованию электронно-вычислительных машин, телекоммуникационных, компьютерных, цифровых и других современных технологий и сетей, средств связи, искусственного интеллекта и достижений науки и техники в криминалистике, экспертной деятельности и в досудебном расследовании. Изучены и проанализированы научные позиции отдельных учёных и представителей отечественных и зарубежных научных школ по названным вопросам (в частности, относительно обсуждения, освещения и законодательного закрепления в правовом и процессуальном механизмах отбора, внедрения и использования упомянутых технологий). Высказано авторское видение и сформулирована научная позиция по поднятым проблемным вопросам и путям их решения.

33 Шепитько В. Ю. Изменчивость криминалистики в XXI веке и ее задачи в современных условиях. *Там само*. С. 58—59.

34 Тонков Е. Е., Комаров И. М. Современные тенденции развития криминалистики и судебной экспертизы. *Современное право*. 2011. № 6. С. 129—134. URL: http://dspace.bsu.edu.ru/handle/123456789/17029 (дата звернення: 06.11.2021).

Целью является анализ исторического развития и современного состояния криминалистических, процессуальных и организационных проблемных вопросов по отбору, лицензированию, использованию, адаптации современных информационных, цифровых, телекоммуникационных, компьютерных и других технологий (в том числе искусственного интеллекта) в криминалистике, экспертной деятельности и досудебном расследовании, а также нормативно-правовой базы, регулирующей отдельные вопросы этого направления.

Ключевые слова: *криминалистика; экспертная деятельность; досудебное расследование; современные технологии; компьютерные сети; информационное пространство; цифровые технологии; искусственный интеллект; отбор; адаптация.*

Genesis and Issues of Using Latest Technologies and Artificial Intelligence in Criminalistics, Forensic Expert Activity and Pre-Trial Investigation

Oleksandr Ukhno

The genesis of development and ways to improve theoretical and applied areas of criminalistics, forensic expertology and criminal procedure for solving forensic, procedural, organizational and other issues of implementation and use of science and technology in pre-trial investigation and trial of criminal offenses in various historical offenses in Ukraine. Special attention is paid to the scientific approach to the selection, implementation, use of computers, telecommunications, digital and other modern technologies and networks, artificial intelligence and advances in science and technology in forensics, expertise and pre-trial investigation. The scientific positions of individual scientists and representatives of domestic and foreign scientific schools on these issues were studied and analyzed (in particular, on the discussion, coverage and legislative consolidation in the legal and procedural mechanisms of selection, implementation and use of these technologies). The author's vision is expressed and the scientific position on the raised problem questions and ways of their decision is formulated.

The aim is to analyze the historical development and current state of forensic, procedural and organizational issues of selection, licensing, use, adaptation of modern information, digital, telecommunications, computer and other technologies (including artificial intelligence) in forensics, expertise and pre-trial investigation, as well as the regulatory framework governing certain issues in this area.

Keywords: *criminalistics; forensic expert activity; pre-trial investigation; modern technologies; computer networks; informational space; digital technologies; artificial intelligence; selection; adaptation.*

Фінансування

Це дослідження не отримало жодного спеціального гранту від фінансових установ у державному, комерційному чи некомерційному секторах.

Відмова від відповідальності

Засновники не грали жодної ролі у розробленні дослідження, добиранні й аналізуванні даних, рішенні про публікацію чи підготовку рукопису.

Учасники

Автор вніс свій внесок винятково в інтелектуальну дискусію, що є основою цього документа, дослідження судової практики, написання та редагування, і бере на себе відповідальність за її зміст і тлумачення.

Декларація щодо конфлікту інтересів

Автор заявляє, що у нього відсутній конфлікт інтересів.

References

Arotsker, L. E. (1969). Organizatsionnye i protsessualnye voprosy ispolzovaniia ehlektronno-vychislitelnykh mashin v ehkspertnoi praktike [Organizational and Procedural Issues of PC Use in Forensic Expert Practice]. *Kriminalistika i sudebnaia ehkspertiza*. Vyp. 6 [in Russian].

Arotsker, L. E., Lantsman, R. M. (1968). *Kibernetika i kriminalisticheskaia ehkspertiza pocherka* [Cybernetics and Forensic Handwriting Examination]. Moskva [in Russian].

Bakhin, V. P. (2002). *Kriminalistika. Problemy i mneniia (1962—2002)* [Criminalistics. Issues and Opinions (1962—2002)]. Kiev [in Russian].

Bilousov, A. S. (2008). *Kryminalistychnyi analiz obiektiv kompiuternykh zlochyniv* [Forensic Analysis of Objects of Computer Crimes]: avtoref. dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Butuzov, V. M., Havlovskyi, V. D., Skalozub, L. P. ta in. (2010). *Dokumentuvannia zlochyniv u sferi vykorystannia elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh i merezh elektrozviazku pry provedenni doslidchoi perevirky* [Documentation of Crimes in the Field of PC Use, Systems and Computer and Telecommunication Networks while Investigation]: navch. posib. ; za zah. red. L. P. Skalozuba, I. V. Bondarenka. Kyiv [in Ukrainian].

Ehdzhubov, L. G. (1968). Aktualnye voprosy ispolzovaniia ehlektronnykh tsifrovykh vychislitelnykh mashin v sudebnom pocherkovedenii [Current issues in PC use in Forensic Handwriting]. *Problemy pravovoi kibernetiki* : mat-ly simp. Moskva [in Russian].

Filipenko, N. Ye., Sniherov, O. P., Bublikov, A. V. (2020). Zastosuvannia spetsialnykh znan pid chas vyiavlennia, profilaktyky y rozsliduvannia zlochyniv u sferi kompiuternoi informatsii ta vysokykh tekhnolohii (ohliadova stattia) [Specific Expertise Application in Detection, Prevention and Investigation of Crimes in the Field of Computer Information and High Technology (Review Article)]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 22. DOI: 10.32353/khrife.2.2020.12 [in Ukrainian].

Ivanov, V. H., Ivanov, S. M., Karasiuk, V. V. ta in. (2014). *Pravova informatsiia ta kompiuterni tekhnolohii v yurydychnii diialnosti* [Legal Information and IT in Legal Activities]: navch. posib. ; za zah. red. V. H. Ivanova. 4-te vyd., zmin. i dop. Kharkiv [in Ukrainian].

Kharaberiush, I. F. (2019). Okremi pohliady shchodo spivvidnoshennia spetsialnoi tekhniky pravookhoronnykh orhaniv ta kryminalistychnoi tekhniky [Separate Views on Correlation between Special Equipment of Law Enforcement Agencies and Forensic Equipment]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 20. DOI: 10.32353/khrife.2.2019.06 [in Ukrainian].

Kliuiev, O. M. (2019). Udoskonalennia ekspertnoho zabezpechennia pravosuddia: teoretychni, pravovi ta orhanizatsiini aspekty [Improving Forensic Expert Support of Justice: Theoretical, Legal and Organizational Aspects]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 19. DOI: 10.32353/khrife.1.2019.08 [in Ukrainian].

Klymenko, N. I. (2010). Kryminalistychni znannia: poniattia, struktura, rozvytok [Forensic Knowledge: Concept, Structure, Development]. *Kryminalistyka XXI stolittia* : mat-ly Mizhnar. nauk. prakt. konf. (Kharkiv, 25—26.11.2010). Kharkiv [in Ukrainian].

Korshenko, V. A. (2017). *Teoretychni ta metodychni osnovy sudovoi telekomunikatsiinoi ekspertyzy* [Theoretical and Methodological Bases of Forensic Telecommunication Examination]: avtoref. dys. ... kand. yuryd. nauk. Kharkiv [in Ukrainian].

Marenych, D. (2014). Kryminalistychna kharakterystyka kiberzlochyniv [Forensic Characteristics of Cybercrime]. *Visnyk prokuratury.* № 12 [in Ukrainian].

Marenych, D. (2014). Sotsialno-demohrafichni oznaky osoby, shcho vchynyla zlochyn u sferi vykorystannia EOM, system, kompiuternykh merezh, merezh elektrozviazku [Socio-demographic Characteristics of Person who Has Committed a Crime in the Field of Use of Computers, Systems, Computer Networks, Telecommunications Networks]. *Visnyk prokuratury.* № 9 [in Ukrainian].

Meshcheriakov, V. A. (2001). *Osnovy metodiki rassledovaniia prestuplenii v sfere kompiuternoi informatsii* [Fundamentals of Methods of Investigating Crimes in the Field of Computer Information]: avtoref. dis. ... kand. iurid. nauk. Voronezh [in Russian].

Operatsii z kiberzlochynnosti [Cybercrime operations]/ Ofitsiinyi sait Interpolu. URL: https://www.interpol.int/en/Crimes/Cybercrime/Cybercrime-operations [in Ukrainian].

Palamarchuk, L. P. (2005). *Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh* [Forensic Investigation of Illegal Interference In the Work of Computers, Systems and Computer Networks]: avtoref. dys. ... kand. yuryd. nauk. Kyiv [in Ukrainian].

Panchenko, V. M. (2013). Suchasnyi stan ta problemy borotby z Internet-zlochynnistiu [Current State and Issues of Combating Cybercrime]. *Borotba z Internet-zlochynnistiu* : mat-ly Mizhnar. nauk.-prakt. konf. (Donetsk, 12—13.06.2013). Donetsk [in Ukrainian].

Panov, M. I., Shepitko, V. Yu., Konovalova, V. O. (2011). *Nastilna knyha slidchoho* [Investigator's handbook]. 3-tie vyd., pererob. i dopov. Kyiv [in Ukrainian].

Pyrih, I. V., Prykhodko, V. O. (2021). Kryminalistychni obliky: problemy klasyfikatsii [Forensic Accounting: Classification Issues]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 23. DOI: 10.32353/khrife.1.2021.03 [in Ukrainian].

Samoilenko, O. A. (2020). *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* [Fundamentals of Methods of Investigating Crimes Committed in Cyberspace]: monohrafiia ; za zah. red. A. F. Volobuieva. Odesa [in Ukrainian].

Shepitko, M. V. (2019). Problemy vyiavlennia ta rozsliduvannia zlochyniv proty pravosuddia, shcho vchyniaiutsia profesiinymy uchasnykamy sudochynstva (provadzhennia) [Issues of Detection and Investigation of Crimes against Justice Committed by Professional Participants in the Legal Proceedings]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 19. DOI: 10.32353/khrife.1.2019.04 [in Ukrainian].

Shepitko, V. Iu. (2010). Izmenchivost kriminalistiki v XXI veke i ee zadachi v sovremennykh usloviiakh [Variability of Criminalistics in the XXI Century and its Tasks in Modern Conditions]. *Kryminalistyka XXI stolittia* : mat-ly Mizhnar. nauk. prakt. konf. (Kharkiv, 25—26.11.2010). Kharkiv [in Russian].

Shepitko, V. Yu. (2017). Rol profesora M. V. Saltevskoho u formuvanni metodolohichnykh zasad kryminalistyky [Role of M. V. Saltevskyi, Professor in Formation of Methodological Foundations of Criminalistics]. *Aktualni pytannia sudovoi ekspertyzy ta kryminalistyky* : zb. mat-liv Mizhnar. nauk.-prakt. konf. (Kharkiv, 07—08.11.2017). Kharkiv [in Ukrainian].

Shepitko, V. Yu., Avdieieva, H. K. (2019). Problemy zastosuvannia naukovo-tekhnichnykh zasobiv ta innovatsiinykh produktiv u diialnosti orhaniv pravoporiadku [Issues of Application of Scientific and Technical Means and Innovative Products in Activity of Law Enforcement Agencies]. *Teoriia ta praktyka sudovoi ekspertyzy i kryminalistyky.* Vyp. 20. DOI: 10.32353/khrife.2.2019.01 [in Ukrainian].

Shestak, V. A., Volevodz, A. G. (2019). Sovremennye potrebnosti pravovogo obespecheniia iskusstvennogo intellekta : vzgliad iz Rossii [Modern Needs of Legal Support of Artificial Intelligence: View from Russia.]. *Vserossiiskii kriminologicheskii zhurnal.* T. 13. № 2. DOI 10.17150/2500-4255.2019.13(2).197-206 [in Russian].

Simakova-Yefremian, E. B. (2019). Vprovadzhennia novitnikh metodiv ekspertnykh doslidzhen ta pidkhodiv do zdiisnennia sudovo-ekspertnoi diialnosti — neobkhidnyi faktor ekspertnoho zabezpechennia pravosuddia [Introduction of Latest Methods of Forensic Expert Research and Approaches to Implementation of Forensic Activities is Necessary Factor in Forensic Expert Support of Justice]. *Innovatsiini metody ta tsyfrovi tekhnolohii v kryminalistytsi, sudovii ekspertyzi ta yurydychnii praktytsi* : mat-ly mizhnar. «kruhl. stolu» (Kharkiv, 12.12.2019). Kharkiv [in Ukrainian].

Strogovich, M. S. (1968). *Kurs sovetskogo ugolovnogo protsessa* [Course of Soviet Criminal Procedure]. V 2 t. T. 1. Osnovnye polozheniia nauki sovetskogo ugolovnogo protsessa. Moskva [in Russian].

Telychko, O. A., Rekun, V. A., Chabanenko, Yu. S. (2021). Problemy vyznachennia ta normatyvnoho zakriplennia poniattia «shtuchnyi intelekt» u zakonodavstvi zarubizhnykh krain ta Ukrainy [Issues of Definition and Normative Consolidation of the Artificial Intelligence Concept in Legislation of Foreign Countries and Ukraine]. *Yurydychnyi naukovyi elektronnyi zhurnal.* № 2. DOI: 10.32782/2524-0374/2021-2/75 [in Ukrainian].

Tonkov, E. E., Komarov, I. M. (2011). Sovremennye tendentsii razvitiia kriminalistiki i sudebnoi ehkspertizy [Current Trends in Development of Criminalistics and Forensic Science]. *Sovremennoe pravo.* № 6. URL: http://dspace.bsu.edu.ru/handle/123456789/17029 [in Russian].

Volevodz, A. G. (2002). Sledy prestuplenii, sovershennykh v kompternykh setiakh [Traces of Crimes Committed on Computer Networks]. *Rossiiskii sledovatel.* № 1 [in Russian].

Юхно, О. (2021). Генезис і проблемні питання використання новітніх технологій та штучного інтелекту в криміналістиці, експертній діяльності й досудовому розслідуванні. *Теорія та практика судової експертизи і криміналістики.* Вип. 3 (25). С. 40—59. DOI: 10.32353/khrife.3.2021.04.