

Гора І. В.,

*доктор юридичних наук, професор,
провідний науковий співробітник науково-організаційного центру
Національної академії Служби безпеки України*

Колесник В. А.,

*доктор юридичних наук, професор,
головний науковий співробітник науково-організаційного центру
Національної академії Служби безпеки України*

Попович І. І.,

*кандидат юридичних наук, доцент,
доцент кафедри кримінального права та процесу
ДВНЗ «Ужгородський національний університет»*

ДО ПИТАННЯ ПРО ЦИФРОВУ КРИМІНАЛІСТИКУ В СИСТЕМІ КРИМІНАЛІСТИЧНИХ ЗНАТЬ

Анотація. Стаття присвячена розгляду питань впливу новітніх цифрових технологій на злочинну діяльність, модифікацію знарядь та способів вчинення злочинів, появу їх нового виду – комп’ютерних кримінальних правопорушень і формування окремої категорії об’єктів криміналістичного дослідження – цифрових доказів та іншої доказової інформації в цифровій формі. Робота з пошуку, дослідження та використання таких доказів вимагає від слідчого, прокурора й залучених ними спеціалістів використання відповідних новітніх науково-технічних засобів, розроблення комп’ютерних програм та дослідження віртуального середовища глобальної мережі зв’язку. Зазначене також викликає потребу врахування органами досудового розслідування й судом цифрової форми отриманої інформації та її носіїв. Разом з тим виникла потреба розроблення нових або модифікації існуючих тактичних прийомів проведення окремих слідчих дій, нових видів судово-експертних досліджень, формування основ новітніх методик розслідування кримінальних правопорушень, при вчиненні та для вивчення наслідків яких використовують засоби комп’ютерної техніки й цифрові програмні продукти. Все це дає підстави для появи в науковому й практичному обігу поняття «цифрова або комп’ютерна криміналістика», природа й місце якої в системі наукових знань залишаються не до кінця з’ясованими, а часто – дискусійними.

Результатом даного наукового пошуку є висновок про те, що впровадження цифрових технологій в суспільну й виробничу практику, використання комп’ютерних засобів та їхнього програмного забезпечення має безпосередній вплив на формування обсягу завдань, які ставляться перед криміналістикою як наукою і криміналістами як користувачами її досягнень. Цифрова форма інформації, що збирається й вивчається під час досудового розслідування, цифрові знаряддя й засоби вчинення кримінальних правопорушень, цифрові сліди й інші докази протиправної діяльності дають підстави вести мову про формування нового напрямку науки – цифрової криміналістики. Проте поглиблене вивчення цієї проблеми вказує на те, що варто вести мову не про виникнення й розвиток нової окремої науки, а саме про важливий і навіть стратегічний цифро-

вий напрям розвитку традиційної криміналістики. Цифрова складова криміналістики має бути присутньою в усіх її сформованих на сьогодні розділах – в загальній теорії, в криміналістичній техніці, тактиці та методиці розслідування певних видів злочинів.

Ключові слова: кримінальне правопорушення; комп’ютерні злочини; досудове розслідування; криміналістика; система криміналістики; цифрова криміналістика; доказування; інформаційно-цифрові технології; цифрові докази.

Постановка проблеми. Сьогодні питання цифрових технологій, комп’ютеризації, діджиталізації, цифрової інформації та використання результатів їх застосування і отримуваних наслідків цікавлять не лише розробників, а й багатьох користувачів – від пересічних громадян до представників державних структур та правоохоронних органів. З початку нинішнього тисячоліття цифрові технології активно впроваджують в різні, а можна навіть стверджувати, що буквально у всі сфери людського життя. Разом з обговоренням ціннісних характеристик цього загалом позитивного для розвитку людства процесу представники різних галузей права й правоохоронної діяльності все частіше почали залучати до дослідження цих явищ фахівців з комп’ютерної й мережевої безпеки, кібертехнологій, Інтернет технологій, інформаційних технологій тощо, намагаючись розв’язати питання протидії використанню таких технологій з протиправною метою. Не секрет, що кожний новий виток технічного прогресу і впровадження його результатів у суспільну практику несе з собою і нові можливості використання новітніх досягнень зі злочинною метою, створює нові злочинні засоби, породжує нові способи вчинення раніше відомих злочинів, а часто – навіть призводить до появи нових видів кримінальних правопорушень. Серед них можемо назвати кібертероризм, кібершпигунство, комп’ютерне піратство, посягання на приватне життя й інтелектуальну власність з використанням мережі Інтернет, викрадення конфіденційної інформації й таємних даних, зокрема, й таких, що становлять державну таємницю та ін. Не дарма вітчизняні й зарубіжні фахівці ведуть

сьогодні мову про проблеми національної кібербезпеки, пов'язуючи ці питання з існуванням Інтернету, цифровими інформаційними технологіями та потенційними витратами на електронну оборону більшості країн [1, с. 1].

Разом з тим національне законодавство часто не встигає за науково-технічним прогресом з його новими технологіями і це стає на шкоду боротьбі із злочинністю та дає злочинцям нові можливості вчиняти й приховувати факт та сліди злочинів, уникати заслуженої відповідальності. Корисність і невідворотність повсякденного й широкого використання цифрових технологій несе в собі й окрему небезпеку, якою вважаємо можливість їх використання із злочинною метою. Ще у 1995 р. відомий американський вчений, фахівець в галузі інформатики, засновник і очільник Цифрової лабораторії Масачусетського технологічного інституту Н. Негропonte (N. Negroponte) у одній зі своїх ґрунтовних праць під назвою "Being Digital" вказав на те, що у кожній технології або дару науки є темний бік і цифровізація – не виключення [2, с. 227]. Ось чому правоохоронна практика та науки кримінально-правового циклу, що обслуговують таку діяльність, повинні враховувати й сучасні реалії та пов'язані з ними наслідки цифровізації економіки, соціально-політичної сфери, державного управління, освіти, культури, побуту.

Не обходять своєю увагою ці питання і криміналісти. Адже криміналістика як ніяка інша галузь науки, розробки якої мають неабияке значення для практики протидії злочинності, повинна враховувати і використовувати в теоретичних напрацюваннях та практичних рекомендаціях все те нове, що пов'язується із впровадженням новітніх досягнень науково-технічного прогресу в життя суспільства. Ось чому вважаємо, що зазначені питання є актуальними, варті на їх поглиблене й цілеспрямоване вивчення та обговорення науковцями й практиками.

Стан дослідження. Суттєвий внесок у висвітлення загальних питань використання сучасних інформаційних зокрема й комп'ютерних технологій в діяльності правоохоронних органів з протидії злочинам внесли вітчизняні криміналісти, серед яких: В. Гавловський, М. Думчиков, І. Заяць, А. Колодіна, В. Коновалова, К. Латиш, Ю. Орлов, Д. Пашнев, С. Перлін, А. Ратнова, Р. Степанюк, В. Теплицький, В. Хахановський, В. Шевчук, В. Шепітько, М. Шепітько та ін. В наукових працях останнього десятиліття розглядалися питання виявлення й дослідження комп'ютерних засобів, цифрових слідів, цифрових джерел доказів та особливостей використання спеціальних знань в досудовому розслідуванні злочинів, які вчиняються з використанням комп'ютерних засобів, в сфері обігу комп'ютерної інформації. Водночас одним з гострих залишається питання встановлення ролі й значення цифрових технологій для розвитку й визначення завдань науки криміналістики, встановлення місця «цифрової криміналістики» в системі криміналістичних знань. Актуальність дослідження таких питань має не лише теоретичне, а й суто прикладне значення для діяльності осіб та органів, що здійснюють боротьбу зі злочинністю.

Мета статті – надати інформацію щодо впливу процесу цифровізації на злочинну діяльність та боротьбу з нею і сучасних підходів вітчизняних й зарубіжних науковців та практиків до розуміння ними поняття «цифрова криміналістика», визначення її ролі й місця в системі загальнонаукових та криміналістичних знань.

Виклад основного матеріалу. Криміналістика сьогодення відрізняється від криміналістики початку її створення й роз-

робки основ та перших кроків становлення криміналістичної техніки, тактики, методики. І справа не в здійснених на той час та здійснюваних на тепер дослідженнях і опублікованих наукових працях, не у трансформації знань та способів злочинних посягань, не у принципово інакших практичних можливостях суб'єктів виявлення й розслідування злочинів, не у зміні структури криміналістики як науки. Хоча за великим рахунком це, безумовно, накладає свій відбиток. Основна відмінність зумовлена тим середовищем, в якому здійснені наукові пошуки й отримані теоретичні напрацювання, а розроблені наукою рекомендації знаходять своє практичне втілення. Вже саме середовище визначає те, які з розроблених криміналістикою наукових положень можна визнавати корисними й сучасними, а які – застарілими, такими, що втратили свою актуальність або вимагають істотного вдосконалення. Реалії сьогоденного дня не можуть не братися до уваги при аналізі теоретичних положень сучасної криміналістики й тим більше, при визначенні перспективних векторів її розвитку у майбутньому. Серед основних факторів, що глобально впливають на життєдіяльність суспільства в цілому, на структуру злочинності й на діяльність правоохоронних органів з протидії злочинним проявам, сьогодні необхідно назвати широке розповсюдження інформаційно-технічних, комп'ютерних, цифрових технологій. Ними пронизані усі найбільш значущі сфери існування сучасного суспільства і держави, вони стали невід'ємною частиною життєдіяльності кожної людини.

На теперішній час масштабний перехід суспільства на «цифру» зупинити вже не можна, адже це є цінним для користувача, вигідним для бізнесу, значущим для регулятора. Як слушно зазначає М. Думчиков, цифровізація – процес впровадження цифрових технологій населенням, бізнесом, суспільством, який є незворотнім і невід'ємним, корисним, допоміжним елементом загального процесу цивілізованого еволюціонування суспільства. Інформаційно-комунікативним технологіям властивий революційний характер, але не можна не помітити поступового переходу від етапу корисного доповнення до етапу їх розвитку як ключових елементів, без яких буде неможливою сучасна індустрія суспільства, всіх його секторів, всіх видів діяльності людини. Перетворення інформації у визначальний фактор суспільного розвитку, діджиталізація, медіатизація і віртуалізація набули статусу ключових глобальних трендів сучасності. Прогрес в галузі інфокомунікативних технологій звів до мінімуму, практично нівелював традиційний розрив між обробкою даних і комунікацією, зробивши інформаційне поле дійсно єдиним і глобальним [3, с. 101]. По суті, цифровізація – це ніщо інше ніж перетворення доступної для сприйняття інформації у цифрову форму, коли має місце заміна аналогових (фізичних) систем збирання й обробки даних технологічними системами з використанням їх цифрового програмного забезпечення.

Активна цифровізація усіх сфер людської діяльності, а разом з тим і така, що швидко посилюється технічна оснащеність кримінальних структур призводять до необхідності розробок окремих теорій і вчень, спрямованих на забезпечення використання цифрової техніки в ході виявлення й розслідування злочинів, а також на виявлення, фіксацію, дослідження та використання з метою доказування цифрових слідів й іншої цифрової інформації, її носіїв та інформаційно-технологічних пристроїв. Особливо перспективними для наукової розвідки

є актуальні проблеми криміналістики, пов'язані із кіберпростором. Адже сьогодні персональний чи виробничий комп'ютер або смартфон чи айфон з виходом до глобальної мережі можуть стати потужним інструментом як засобом вчинення протиправного діяння, бути об'єктом злочинного посягання або використовуватися з протиправною метою для збереження важливих електронних доказів злочину.

У зв'язку із цим ми виокремлюємо низку актуальних питань сучасної криміналістики, які потребують своєї наукової розробки, теоретичного обґрунтування й впровадження у практику протидії злочинності. Це, зокрема, такі напрями, що пов'язані: з розслідуванням багатьох видів злочинів проти національної безпеки України та злочинів проти миру, безпеки людства, вчинених з використанням сучасних інформаційних технологій; з дослідженням новітніх кримінальних цифрових технологій, особливостей протікання кримінальних ситуацій у кіберпросторі; з розробкою механізму використання теоретичного криміналістичного знання в оперативній, слідчій та експертній практиці; з ефективним криміналістичним запобіганням злочинів, що вчиняються з використанням комп'ютерних та інформаційно-технічних технологій і пристроїв та ін.

Як зазначають вітчизняні науковці і що підтверджує практика боротьби із злочинністю, стрімкий розвиток цифрових технологій в Україні супроводжується значною динамікою кримінальних правопорушень у даній сфері. Так звані «кіберзлочини» є найбільш динамічнішою групою суспільно небезпечних діянь. Адже з кожним роком вони стають усе більш масовими й небезпечними, а способи їх вчинення більш вигадливими й витонченими. Щороку вчиняються десятки тисяч злочинів з використанням інформаційно-телекомунікаційних систем, програмних, програмно-апаратних засобів, інших технічних і технологічних засобів та обладнання. Останніми роками найбільше поширилися такі види злочинів, що посягають на інформаційну безпеку, а саме: корисливі кіберзлочини, викрадення персональних даних, кібершпигунство, кібербулінг, розповсюдження дитячої порнографії, порушення авторських й суміжних прав та ін. Також необхідно враховувати й те, що в сучасних умовах до легального економічного обігу активно надходять нетрадиційні види майна та майнових цінностей, у тому числі інтернет-сайти, електронні гроші, цифрові технології мобільного зв'язку тощо. Оскільки вони дають змогу приносити значні і швидкі доходи, на них відповідно реагує кримінальне середовище, намагаючись отримати свою вигоду. В результаті виникають усе нові види злочинних посягань, що передбачають використання сучасних цифрових інформаційних технологій на умовах раптовості й анонімності [4, с. 99]. У протиправній діяльності зловмисниками широко використовуються сучасні цифрові засоби й технології зв'язку, електронні платіжні системи, можливості Інтернет-сервісів, що забезпечують анонімізацію особи у цифровому просторі, залишаючи при цьому складні для виявлення й дослідження слідчим та спеціалістами й експертами цифрові сліди. До того ж, здебільшого цифрова трансформація зачіпає такі сфери кримінального бізнесу як незаконний обіг наркотиків, зброї, нелегальний гральний бізнес, викрадення грошей з використанням систем дистанційного банківського обслуговування, легалізації (відмивання) доходів, отриманих протиправним шляхом, ухилення від сплати податків, злочини корупційної спрямованості та ін.

У плані розгляду можливостей щодо забезпечення виконання завдань правоохоронної діяльності необхідно констатувати, що певною мірою значна кількість людей, а особливо – у великих містах, на автотранспортних магістралях перебувають у ситуації постійного контролю за їх пересуванням та діями з боку різноманітних електронних пристроїв зовнішнього спостереження. Такі пристрої можуть бути розташовані на вулицях, в під'їздах та ліфтах будинків чи біля домоволодінь за програмою «Безпечне місто», встановлені на постійній або тимчасовій основі вздовж доріг із жвавим рухом для стеження за дорожньою обстановкою, використані працівниками дорожньої патрульної служби для контролю за дотриманням правил дорожнього руху, швидкості пересування транспортних засобів (наприклад, камери TRUCAM), відеореєстратори встановлюють на автомобілі багато хто із власників та користувачів тощо. Отримані й збережені за їх допомогою записи перетворюються у накопичену цифрову інформацію, яка може мати доказове значення в разі проведення досудового розслідування. До того ж сьогодні держава з метою боротьби зі злочинами полегшує шляхи й можливості збирання, накопичення й отримання такої цифрової інформації для потреб правоохоронних органів.

Проте захоплюватися інформацією, що створена і залишена цифровими пристроями і отримана слідчим з використанням цифрових технологій, не треба, оскільки для подальшої перевірки таких доказів вкрай необхідним може бути проведення «класичних» слідчих та негласних слідчих (розшукових) дій, зокрема таких як допит, впізнання, слідчий експеримент, а для вивчення цифрових даних буде потрібним залучення експерта та ін. Наприклад, сьогодні активно впроваджуються технології з розпізнавання обличчя людей відеопошуковими системами. Проте результати такого узнавання не рівнозначні впізнанню як процесуальній дії або фізичному ототожненню особи під час проведення оперативно-розшукових заходів і тим більше, не може вважатися результатом експертної ідентифікації особи. Це робота машини і отримані дані можуть бути помилковими. Недопущення таких помилок – одне із завдань криміналістики.

Із початком ХХІ століття істотно оновився, став більш досконалим арсенал криміналістичних засобів, тактичних прийомів і методів розслідування. Вітчизняні науковці й практики почали розробляти й накопичувати досвід використання цифрових технічних засобів, інформаційних криміналістичних технологій в роботі не лише з кримінально-процесуальною та іншою криміналістично значущою інформацією, а й з їх практичним використанням в інших галузях правозастосування. Все більше вчених-криміналістів висловлюють думки щодо сучасних тенденцій розвитку криміналістики, пов'язуючи їх з процесами цифровізації (діджиталізації). Це має призвести до таких результатів: прискорення темпів розвитку криміналістичної науки в цілому, особливо в точках взаємодії наук; матеріалізація та формалізація знань; проникнення досягнень математики, фізики, кібернетики у все нові галузі криміналістичних знань; тенденція переходу від аналізу до синтезу, системного аналізу, структурно-функціонального методу та ін.

Оскільки сучасна злочинність навчилася використовувати комп'ютерні засоби, електронні пристрої, інформаційні технології з їх програмним забезпеченням, цифрову інформацію у своїх злочинних цілях, предметом криміналістичних досліджень доволі часто стають цифрові об'єкти. Все частіше виникає необхідність в об'єктивній оцінці електронної інфор-

мації й проведенні низки комплексних досліджень таких специфічних цифрових об'єктів, котрі допоможуть виявити злочинця. Важливим є також розуміння специфіки тієї інформації, котра на сьогодні отримала визначення – «цифрова». Усе це в сукупності дає змогу забезпечити однаковий підхід до збирання й вивчення, зниження ймовірної кількості помилок, що припускаються правоохоронцями при оцінці зібраних доказів. Також важливим є й вміння оперативних працівників і слідчих правильно поводитися з електронними пристроями, створеною й збереженою в них цифровою інформацією, вилучати й зберігати їх, досліджувати та правильно оцінювати й використовувати в доказуванні інформацію, носіями котрої вони є. На оволодіння такими знаннями спрямовані розробки криміналістів, а досвід їх використання має підвищити майстерність виконавців.

Криміналістичне забезпечення діяльності оперативних підрозділів, органів досудового розслідування й суду, а разом з ними і адвокатури, представники якої беруть участь в кримінальному провадженні й причетні до здійснення правосуддя, зазнає фундаментальних змін та впроваджує інноваційні підходи. Власне, сьогодні стало можливим виділити окремий напрям у розвитку криміналістики як науки – поява «цифрової криміналістики». У окремих джерелах для позначення цього напрямку використовують й інші терміни – «комп'ютерна криміналістика» або «комп'ютерна системна криміналістика», «кіберкриміналістика» тощо. У той же час деякі вчені навіть розглядають комп'ютерну криміналістику як самостійну прикладну науку для розслідування злочинів (інцидентів), пов'язаних з комп'ютерною інформацією, розроблення методів пошуку і фіксації комп'ютерних об'єктів та цифрових доказів, їх дослідження. Поряд з нею активно розвивається і судова експертиза в контексті розширення знань про цифровізацію та діджиталізацію [5].

Проте сьогодні криміналістика як самостійна наука кримінально-правового циклу становить собою не конгломерат розрізнених даних з біології, хімії, фізики, електроніки, кібернетики, інформаційної технології, комп'ютерної інженерії, кібербезпеки чи інших галузей знань, а якісно нове знання. Рівень її розвитку дозволяє встановлювати, інтерпретувати, пояснювати досліджувані явища, використовуючи для цього досягнення інших наук. Криміналістика – наука поліморфна. Її не можна зводити до будь-якого окремо взятого наукового напрямку чи конкретного дослідження: прийому, способу, методу, науково-технічного засобу або знаряддя й отриманим в кінцевому рахунку результатам. Як і будь-яка інша наука, вона являє собою своєрідну об'єктивну матрицю уявлень, знань про явища й події: діяння, злочини, правопорушення та закономірності формування, збереження й виявлення та дослідження залишених ними слідів, які вказують на причетних осіб, а в разі протиправності діянь – на винуватців. Загалом наука криміналістика – сфера специфічних наукових знань про злочинну діяльність та про її антипод – діяльність щодо виявлення, розкриття та розслідування кримінальних правопорушень, а також встановлення істини у процесі розв'язання завдань судочинства. До того ж багато які з її теоретичних положень та наукових розробок і практичних рекомендацій сьогодні мають значення не лише для сфери кримінального, але й цивільного, адміністративного та й навіть конституційного судочинства.

Сьогодні все більше вчених не без підстав вказують на необхідність перегляду уявлень про криміналістику та її предмет, на появу нового явища в криміналістичній науці – цифрової складової криміналістики та її нового наукового предмета. Цифрову криміналістику, про яку йде мова у даному дослідженні, в її узагальненому розумінні у світовій практиці зазвичай розуміють не як окрему наукову галузь чи новий вид діяльності певної особи – слідчого, прокурора, криміналіста, експерта, а як роботу, що здійснюється комп'ютеризованими апаратними комплексами з використанням їх програмного забезпечення, де все відбувається й відтворюється за мінімальної участі людини, а результат такої діяльності відображається у цифровій формі.

Дослідники цієї проблеми вказують на те, що перші згадування про цифрову криміналістику (*англ.* – digital forensics) з'явилися в наукових джерелах ще в середині 1970-х років як про один із напрямів комп'ютерної криміналістики і увага криміналістів тривалий час була сфокусована переважно на кібератаках, витоках комп'ютерних даних та інших подібних випадках. На думку окремих науковців, перший етап розвитку цифрової криміналістики як такої охоплює 1985–1995 роки. Вважають, що цей етап включав використання програмних кодів для перегляду даних у внутрішніх операційних системах та апаратних засобах комп'ютерів. Другий етап розвитку цифрової криміналістики, на думку дослідників, припадає на 1995–2005 роки. Він ознаменувався появою кіберзлочинності й необхідністю боротьби з нею. Третій етап охоплює 2005–2010 роки. У цей період виникли складні цифрові моделі розслідування злочинів. Однією з таких моделей, яка широко використовується у світі, стала «загальна модель комп'ютерних криміналістичних розслідувань». Початок сучасного етапу розвитку цифрової криміналістики відносять приблизно до 2010 року і вважають, що він продовжується на цей час [6, с. 379].

Не зважаючи на чималий час існування «цифрової криміналістики», ще й досі серед вчених і практиків немає одностайності думок не лише щодо її назви, а й місця в системі галузей наукових знань або в структурі окремої науки – криміналістики. Вважаємо за необхідне проаналізувати деякі думки з приводу розуміння назви, мети створення, предмету вивчення, задач і функцій «цифрової криміналістики», які висловлюються окремими зарубіжними й вітчизняними науковцями. Тут варто звернути увагу на те, що в англійській мові слово та словосполучення «forensics» та «forensics science» мають однакове значення й перекладаються на українську мову як «криміналістика», а терміну «цифрова криміналістика» відповідає його англійський варіант «digital forensics».

Так, зарубіжна дослідниця М.-Х. Марас (М.-Н. Maras) в назві однієї із своїх праць вживає термін «комп'ютерна криміналістика» і зазначає разом з тим, що цифрова криміналістика є однією з галузей криміналістики, яка зосереджена на кримінально-процесуальному праві і пошуку та дослідженні доказів стосовно комп'ютерів і пов'язаних з ними пристроїв, таких як мобільні телефони, смартфони тощо, ігрові приставки та інші пристрої, що функціонують через Інтернет. У виданому нею посібнику з комп'ютерної криміналістики робиться спроба врівноважити технічні аспекти та юридичний аналіз кіберзлочинів. На її думку, це входить до світу кіберзлочинності й, відповідно, потребує окремого підходу до розслідування таких специфічних злочинів. Значну увагу вчена приділяє питанням використання цифрових технологій у судових роз-

слідують, труднощам, пов'язаним із пошуком, вилученням, обслуговуванням та збереженням електронних доказів [7]. Отже, ні комп'ютерну, ні цифрову криміналістику ця вчена не вважає окремою наукою, а веде про них мову як про напрями в криміналістиці, в межах яких науковці досліджують роботу з цифровими доказами та порядок поліцейського розслідування комп'ютерних злочинів.

Дослідники питань кіберзлочинності У.Дж. Круз (Kruse Warren G II) та Дж.Г. Хайзер (Heiser Jay G.) ведуть мову про «комп'ютерну криміналістику», до якої відносять: збереження, ідентифікацію, вилучення, документування та інтерпретацію комп'ютерних даних [8, с. 2]. Про комп'ютерну криміналістику також веде мову і американський вчений та галузевий експерт М. Шітц (M. Sheetz), вказуючи на те, що на цьому напрямі криміналістичної науки розглядаються питання розслідування комп'ютерних злочинів, протидії їх вчиненню, а також те, як комп'ютери можна використовувати для розслідування, судового переслідування та запобігання цим злочинам [9].

Науковці В. Амбхир (V. Ambhire) і Б. Мешрам (B. Meshram) визначають цифрову криміналістику (digital forensics) як використання науково обґрунтованих й перевірених методів для ідентифікації, збирання, збереження, перевірки, аналізу, інтерпретації й надання електронно-цифрових доказів, отриманих із цифрових джерел, для сприяння реконструкції подій, визнаних злочинними [10]. Інший зарубіжний вчений – Г. Палмер (G. Palmer) вважає це окремими напрямками криміналістики, зокрема такими як комп'ютерно-технічна криміналістика, мережева та відеокриміналістика й підкреслює, що метою використання науково обґрунтованих й доказаних методів цих напрямів є збереження, збирання, перевірка, ідентифікація, аналіз, інтерпретація, документування й надання цифрових доказів, отриманих із цифрових джерел. Ним виокремлено задачі цих напрямів – для полегшення або сприяння реконструкції подій, визнаних злочинними, або надання допомоги у передбаченні несанкціонованих дій, котрі, як уявляється, порушують заплановані операції [11, с. 16].

Немає однак думок щодо назви й місця «цифрової криміналістики» в системі наукових знань і серед вітчизняних вчених. Аналізуючи публікації, присвячені питанням розвитку цифрової криміналістики, необхідно відмітити, що здебільшого її розуміють як сукупність способів дослідження комп'ютерів та аналогічної техніки для пошуку цифрових слідів злочину.

Так, відомі вітчизняні криміналісти В. Коновалова й В. Шевчук ведуть мову про цифрову криміналістику як стратегічний напрям у формуванні криміналістичних знань, підкреслюючи, що цифрова інформація, як невід'ємний атрибут діяльності злочинця й органів юстиції, визначає тенденції розвитку юридичної науки, в т. ч. криміналістики, яка стоїть на передньому краї боротьби зі злочинністю і одне із завдань якої полягає в забезпеченні правоохоронних органів і судів криміналістичними методами і засобами боротьби, що відповідають сучасним викликам злочинності [12, с. 74]. Такої ж думки дотримуються й В. Шепітько та М. Шепітько, вказуючи, що цифрова криміналістика має відношення до процесу збирання, отримання, збереження, аналізу та подання електронних (цифрових) доказів у досудовому та судовому провадженні. Тому цифрова криміналістика, за їхнім переконанням, може скласти стратегічний напрям у розвитку криміналістичної науки [13, с. 192].

Про цифрову криміналістику веде мову К. Латиш, зазначаючи, що сьогодні не лише в Україні, а й в багатьох країнах світу спостерігається тенденція формування та застосування нового наукового напрямку – цифрової криміналістики (Digital Forensics, Digital Forensic Science or Digital Criminalistics) [14, с. 31–37]. Щоправда, в цій її публікації не вказано на те, йдеться тут про окремий і самостійний науковий напрям чи новий напрям в межах розвитку всіх розділів традиційної для нас науки криміналістики. Адже питання розслідування комп'ютерних злочинів, збирання й використання в доказуванні цифрових доказів, експертного дослідження цифрових технічних засобів та інших комп'ютерних об'єктів стосуються у повній мірі і теоретичних основ криміналістики як науки, і криміналістичної техніки, і тактики, і методики розслідування окремих видів злочинів. Вітчизняними дослідниками зазначених питань використовуються й інші терміни: «комп'ютерна криміналістика» [15, с. 29–30], «електронна криміналістика» [16, с. 79] та ін.

Інші вітчизняні науковці, зокрема, Р. Степанюк та С. Перлін вважають, що цифрова криміналістика – це окрема галузь судових наук, яка являє собою систему наукових методів дослідження цифрових доказів з метою сприяння виявленню та розслідуванню кримінальних правопорушень [17, с. 290]. Проте навряд чи новітні методи дослідження об'єктів окремого виду, якими можуть виступати цифрові докази, можна вважати окремою галуззю науки.

На нашу думку, зважаючи лише на стрімкий розвиток науково-технічного прогресу та впровадження цифровізації в суспільну практику, не варто відразу вести мову про виникнення якоїсь нової й відмінної від існуючої науки – «цифрової криміналістики». Адже винайдення електрики й початок ери електрифікації виробництва, соціальної практики та життя населення не призвели до виникнення «електричної криміналістики», а польоти людини в космос не ставлять питання про потребу створення «криміналістики космічної». І хоча знаряддями вчинення злочинів сьогодні можуть бути електричні прилади, а їхнє застосування залишає специфічні сліди та утворює відмінні від інших способів і знарядь вчинення злочину докази, а вчинення злочинних дій в умовах космосу вимагає окремих підходів до збирання доказів і порядку організації розслідування, криміналістичне забезпечення досудового розслідування таких кримінальних правопорушень спирається на розробки традиційної науки – криміналістики. Тому за нашим глибоким переконанням варто дослухатись до думок тих вітчизняних і зарубіжних вчених та практиків, які вважають цифрову криміналістику окремим напрямом у розвитку криміналістики традиційної. З огляду на важливість, актуальність, перспективність розвитку й впровадження у всі сфери життєдіяльності людини інноваційних технологій, збільшення потоку цифрових об'єктів, що потрапляють до сфери уваги криміналістів і не тільки як цифрових джерел доказів, слушними вважаємо пропозиції вважати такий цифровий напрям розвитку криміналістики стратегічним.

Висновки. Сьогодні однією із задач, що стоять перед наукою криміналістикою, постає питання розроблення ефективних засобів і методів протидії злочинності, які відповідають не лише її зростанню, а й вдосконаленню злочинцями їхніх можливостей вчиняти та приховувати сліди протиправних діянь. Невпинний розвиток науково-технічного технічного

прогресу, комп'ютеризація практично всієї сфери виробництва й життєдіяльності людини призвели до використання із злочинною метою новітніх досягнень в галузі використання цифрових технологій. Поява нових для сучасної правоохоронної практики об'єктів, якими є комп'ютерні засоби, мережеві канали зв'язку, цифрові способи створення й використання інформації висунули перед криміналістами нові завдання: опанування знаннями у сфері цифрових технологій та їх використання в розробленні новітніх криміналістичних засобів, прийомів, методів розслідування. Часто такі питання розглядають в межах проблеми, що отримала загальну назву «цифрова криміналістика». Автори даної статті переконані, що цифрову криміналістику слід розглядати як сучасний і важливий для розвитку як загальних положень криміналістичної науки, так і для її усталених розділів – криміналістичної техніки, тактики й методики напрям, а не як окрему науку кримінально-правового циклу або ж окремий і самостійний розділ традиційної криміналістики. Перспективними для подальших досліджень вважаємо питання встановлення ролі цифрових аспектів криміналістичного забезпечення виконання завдань судочинства у кожному із зазначених розділів.

Література:

1. National cyber security framework manual / ed. by A. Klimburg. Tallinn: NATO Cooperative Cyber Defense Center of Excellence. 2012. xvii, 235 p.
2. Negroponte Nicholas. Being Digital. New York: Alfred A. Knopf. 1995. 243 p.
3. Думчиков М.О. Процеси діджиталізації і криміналістика: ретро-спективний аналіз. *Криміналістика і судова експертиза: міжвідом. наук.-метод. зб.* / Київський НДІ судових експертиз; редкол.: Д.В. Журавльов та ін. Київ, 2020. Вип. 65. С. 100–108.
4. Злочини проти інформаційної безпеки держави: поняття, виявлення, досудове розслідування: монографія / І.В.Гора, В.А.Колесник, В.В.Малюк, В.О.Ходанович та ін. Київ: 7БЦ, 2023. 512 с.
5. Діджиталізація кримінального процесу: в Україні планують перевести провадження в електронний формат. URL: <https://uazmi.org/news/post/bReTcc20Q04a1jCN6zj9y2> (заголовок з екрану).
6. Колодіна А.С., Федорова Т.С. Цифрова криміналістика: проблеми теорії і практики. *Юридичний науковий електронний журнал*. 2022. № 4. С. 378–380.
7. Maras M.-H. Computer Forensics: Cybercriminals, Laws and Evidence. 2nd Edition. Burlington, MA: Jones & Bartlett, 2014. 408 p.
8. Kruse Warren G.II, Heiser Jay. G. Computer Forensics: Incident Response Essentials. Addison-Wesley, 2002. 392 p.
9. Sheetz Michael. Computer Forensics. An Essential Guide for Accountants, Lawyers, and Managers. Wiley: John Wiley & Sons, LTD. 2007. 176 p.
10. Vishal R. Ambhire1, Dr. B.B. Meshram. Digital Forensic Tools. Mar. 2012, Vol. 2(3) pp: 392–398. URL: https://iosrjen.org/Papers/vol2_issue3/D023392398.pdf.
11. Palmer G. A road map for digital forensic research. Report from the First Digital Forensic Research Workshop (DFRWS). 2001. 42 p.
12. Konovalova V.O., Shevchuk V.M. Digital Criminalistics as a strategic direction of formation of criminalistics knowledge. *Advanced discoveries of modern science: experience, approaches and innovations (January 20, Amsterdam 2023)*. Amsterdam, The Netherlands, 2023. P. 73–77.
13. Shepitko V., Shepitko M. The Formation of Digital Criminalistics as a Strategic Direction for the Development of Science. *XVII Criminalistics and Forensic Expertology: Science, Studies, Practice. Abstracts of the XVII International Congress* (September 16–17, 2021). Bratislava, Slovak Republic, 2021. P. 187–198.

14. Латиш К. Цифрова криміналістика у період війни в Україні: можливість використання спеціальних знань у сфері інформаційних технологій. *Kriminalistika ir teismo ekspertologija : mokslas, studijos, praktika*: XVIII, 2022. T. 18. С. 31–37.
15. Полотай О.І. Комп'ютерна криміналістика: основні завдання та проблеми. *Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення: матеріали міжн. наук. конф.* Тернопіль. Вип. 68. 2022. С. 29–30.
16. Заєць І.С. Перспективи криміналістики в умовах інформатизації суспільства. *Актуальні питання виявлення та розкриття злочинів Національною поліцією: вітчизняний та зарубіжний досвід : матеріали Міжнар. наук.-практ. круглого столу (Київ, 19 лют. 2020 р.)*. Київ : НАВС, 2020. С. 77–81.
17. Степанок Р.Л., Перлін С.І. Цифрова криміналістика й удосконалення системи криміналістичної техніки в Україні. *Вісник Луганського держ. ун-ту внутр. справ ім. Е.О. Дідоренка*. 2022. № 3 (99). С. 283–294.

Hora I., Kolesnyk V., Popovych I. To the issue of digital forensics in the system of forensic knowledge

Summary. The article is devoted to consideration of the impact of the introduction of the latest digital technologies on criminal activity, the modification of tools and methods of committing crimes caused by their influence, the emergence of a new type of them – computer criminal offenses and the formation of a separate category of forensic research objects – digital evidence and other evidentiary information in digital form. The work of finding, researching and using such evidence requires the investigator, the prosecutor and the specialists engaged by them to use the latest scientific and technical means, develop computer programs and study the virtual environment of the global communication network. This causes the need for pre-trial investigation bodies and the court to take into account the digital form of received information and its carriers. At the same time, there was a need to develop tactical techniques for carrying out individual investigative actions, new types of forensic research, forming the foundations of the latest methods of investigating criminal offenses, in the commission of which and for studying the consequences of which computer equipment and digital software products are used. This gives grounds for the emergence of the concept of «digital or computer forensics» in scientific and practical circulation, the nature and place of which in the system of scientific knowledge remain not fully clarified, and are often debatable.

The result of scientific research is the conclusion that the introduction of digital technologies into practice, the use of computer tools and their software has a direct impact on the formation of the scope of tasks that are faced by criminology as a science and criminologists as users of its achievements. The digital form of information collected and studied during the pre-trial investigation, digital tools and means of committing criminal offenses, digital traces and other evidence give reason to talk about the formation of a new direction of science – digital forensics. However, the study of this problem indicates that it is worth talking not about the emergence and development of a new separate science, but about the important and even strategic digital direction of the development of traditional criminology. The digital component of criminology should be present in all its sections formed today – in the general theory, in forensic techniques, tactics and methods of investigation of certain types of crimes.

Key words: criminal offense; computer crimes; pre-trial investigation; criminalistics; system of forensics; digital forensics; proving; information and digital technologies; digital evidence.