ПЕРСПЕКТИВИ РОЗВИТКУ КРИМІНАЛІСТИКИ У СВІТЛІ НОВИХ КРИМІНАЛЬНИХ ЗАГРОЗ, ЗОКРЕМА КІБЕРЗЛОЧИННОСТІ

ОСМОЛЯН Віталій Анатолійович - кандидат юридичних наук, старший викладач кафедри права Хмельницького кооперативного торгово-економічного інституту

УДК 343.985.3
DOI 10.32782/LAW.2020.2.13

Приведены правовые основы и перспективы развития криминалистики в свете новых криминальных угроз – стремительного развития киберпреступности и кибератак. Предложено введение новой отрасли знаний по криминалистическому киберпространству, раскрыты ее значение и место в системе криминалистики в целом. Рассмотрены процессуально-правовые и экспертно-криминалистические вопросы возможности выявления, фиксации и собирания следовой картины и формирования доказательной базы при расследовании киберпреступлений, а также обоснована необходимость эффективного сотрудничества работников следственных органов, прокуратуры, суда и экспертно-криминалистических учреждений для качественного и объективного выполнения заданий уголовного производства и улучшения инновационной политики Украины. Приведены конкретные примеры вопросов, которые нужно рассмотреть экспертам при проведении экспертиз (исследований). Сделаны выводы и предоставлены рекомендации по согласованному использованию норм действующего законодательства в практической деятельности эксперта-криминалиста и следователя. Обращено внимание на необходимость дальнейшего научного сотрудничества ученых и специалистов в сфере материального и процессуального права.

Ключевые слова: криминалистика, компьютер, киберпреступление, кибербезопасность, информация, правоохранительные органы, досудебное расследование, уголовное производство, экспертиза, эксперт, специалист.

Постановка проблеми

Кіберзлочинність є досить новим і специфічним явищем злочинної діяльності, яка постійно розвивається через поширення та удосконалення мережі Інтернет. Саме новизна, специфічність, неухильний і постійний розвиток вказаного виду злочинів вимагають від судових та правоохоронних органів, криміналістів розроблення та застосування нових криміналістичних засобів і методів для їх виявлення та фіксації з метою подальшого використання під час проведення ефективного розслідування, встановлення та притягнення винних осіб до відповідальності.

Це покладає особливу відповідальність на правоохоронні органи щодо проведення якісного та легітимного досудового розслідування у кримінальних провадженнях зазначеної категорії, повного і неупередженого збору доказової бази, що не уявляється можливим без суворого дотримання процедури законності. У цьому і полягає **актуальність** проблеми.

Аналіз останніх досліджень та публікацій

Проведений аналіз наукової літератури [1–10] показав, що вчені неодноразово досліджували діяльність правоохоронних органів із збирання доказової бази, проведення криміналістичних дій у цілому та їх окремих аспектів. Однак розгляд процесуально-правових та експертно-криміналістичних питань щодо можливості виявлен-

ня, фіксації та збирання слідової картини і формування в подальшому доказової бази під час розслідування вчинених кіберзлочинів вимагає детальнішого дослідження й аналізу.

Метою статті є на підставі проведеного теоретичного аналізу та власного практичного досвіду розглянути процесуально-правові й експертно-криміналістичні питання виявлення, фіксації та збирання слідової картини і формування доказової бази під час розслідування кіберзлочинів, а також обґрунтувати необхідність ефективної співпраці працівників слідчих органів, прокуратури, суду та експертно-криміналістичних установ для якісного й об'єктивного виконання завдань кримінального провадження та покращення інноваційної політики України.

Виклад основного матеріалу

Розбудова України як правової держави з європейським демократичним суспільством передбачає зменшення випадків порушень правопорядку, рівня злочинності, а також причин, що її породжують. У боротьбі з правопорушеннями необхідно повною мірою використовувати досягнення в галузі науки і техніки, думку суспільства, засоби масової інформації та друку, засоби переконання, силу закону, тобто всі законні засоби, які наявні в розпорядженні сучасного суспільства. У вирішенні вказаного завдання важливу роль відіграють юридичні науки, зокрема криміналістика, яка перебуває на передовій боротьби зі злочинністю.

Термін «криміналістика» походить від латинського слова *criminalis* – злочинний (той, що має відношення до злочину) [1, с. 3]. У минулому термін використовувався для позначення всієї сукупності кримінально-правових наук. До виниклої в останній чверті XIX століття науки, яка вивчає техніку, тактику і методику розслідування злочинів, вперше його застосував австрійський криміналіст Ганс Гросс. Уважаючи криміналістику допоміжною наукою кримінального права, він назвав її «вченням про реальності кримінального права» [2]. Положення науки кримінального права, як стверджував Г. Гросс, позбавлені всякого значення, якщо вони не можуть бути застосовані «до реальностей повсякденного життя» [2]. Вони здаються позбавленими життя, якщо слідчий (суддя) не розуміє чи неправильно оцінює показання свідків, якщо його вводять в оману прийоми злочинців, якщо він не вміє використовувати сліди злочину чи взагалі незнайомий з безліччю положень, сукупність яких складає криміналістику [1, с. 4].

У різних країнах світу криміналістику називали по-різному: наукова поліція, технічна поліція, кримінальна техніка тощо. Неоднозначно використовується цей термін і в наші часи. У деяких європейських країнах він часто застосовується лише для позначення криміналістичної техніки.

Криміналістика виникла на основі вивчення й узагальнення слідчої практики та активного використання природничих і технічних знань з метою розкриття, розслідування та попередження злочинів. Так, після винайдення фотографії на базі загальних наукових і практичних її положень виникла судова фотографія, яка є складовою частиною криміналістичної техніки. Успіхи хімії та фізики були покладені в основу засобів і методів техніко-криміналістичних досліджень документів, наукові закони фізіології відкрили шлях для розвитку судового почеркознавства. У наш час стрімкий розвиток комп'ютерної техніки та швидкі темпи поширення всесвітньої мережі Інтернет виступають задатками для заснування судової комп'ютеротехнології (ЕВМ-технології) або галузі знань з криміналістичного кіберпростору.

Зазначені нововведення, на наш погляд, не будуть суперечити змісту поняття криміналістики як «науки про закономірності виникнення, збирання, дослідження, оцінку та використання доказів і заснованих на пізнанні них закономірностей засобів та методів судового дослідження і попередження злочинів» [3, с. 42]. І. Ф. Крилов наголошує, що «криміналістика – це наука про технічні засоби, тактичні прийоми і методи, які використовуються з дотриманням норм процесуального закону для ви-

явлення, збирання, збереження, фіксації та дослідження доказів, з метою ефективного розкриття, розслідування і попередження злочинів» [1, с. 5].

Подія злочину, встановлення якої є основною метою процесуальних дій слідчого та криміналіста, – це один із матеріальних процесів дійсності, взаємообумовлений іншими процесами, подіями та явищами, відображений у них і є відображенням яких-небудь процесів та явищ. Будь-яка подія зумовлює зміни в навколишньому середовищі, які є результатом взаємодії між подією, явищем та самим середовищем. За такими змінами ми можемо робити висновки про зміст події.

Щодо процесу доказування зміни в середовищі як результат відображення в ньому події і є доказом цієї події, тими фактичними даними, за допомогою яких можливо робити висновки про подію злочину. Оскільки будь-яка подія злочину невід'ємно (як будь-який процес) відображається в навколишньому середовищі, то і процес виникнення доказів має необхідний, повторювальний, стійкий і загальний характер, тобто характер закономірності.

Робити висновки за відображенням того, що відображається, за доказами про злочин можливо лише в тому випадку, якщо зв'язок змін із подією можна помітити, виявити, зрозуміти за змістом цих змін. Зміни містять у собі відомості про те, чим вони є, тобто інформацію про весь процес відображення, результатом якого вони стали. Зміни – це докази, які є матеріальним носієм, «сховищем» інформації про подію.

Інформація як вираз зв'язку між подією та викликаними нею змінами в середовищі не може існувати без матеріальної основи чи, як прийнято говорити, поза межами інформаційного сигналу, під яким розуміють єдність матеріального носія та засобу передачі інформації. Таким чином, доказ – це інформаційний сигнал, який має зміст (інформацію) та форму виразу (інформаційний код) [4, с. 4].

Перед тим, як з'ясувати характер закономірності виникнення слідової картини та сукупності доказової бази за кіберзлочинами, необхідно визначити суть кібербезпеки та кіберзлочинності, що допоможе визначити, яку саме слідову картину можливо виявити під час збирання доказової бази про вчинення зазначеного виду правопорушень.

Так, законодавець у нормі Закону України «Про основні засади забезпечення кібербезпеки України» визначив, що кібербезпека – це захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [5]. Також у Законі зазначено, що кіберзлочин (комп'ютерний злочин) – це суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [5].

Характерними рисами зазначеного виду злочинної діяльності є такі:

– їх інтелектуальний характер (їх здійснення вимагає застосування спеціальних знань);

– кіберзлочини, на відміну від інших інтелектуальних злочинів, доступні для вчинення особам низьких соціальних і вікових можливостей, потрібно лише мати доступ до мережі Інтернет та електронно-обчислювальної машини;

– відсутність персоніфікації та анонімність (механізми та вимоги до ідентифікації користувача у глобальній мережі Інтернет дозволяють правопорушнику здійснювати злочинні операції анонімно або видавати себе за іншу особу, змінювати власні біографічні дані, соціальний статус або взагалі надавати неправдиві відомості щодо останніх);

– стрімке зростання кіберзлочинності, що пов'язано з поширенням інтернету, впровадженням його в різні сфери суспіль-

ного життя, а також здешевленням послуг користування глобальною мережею;

– географічна, територіальна та «особистісна» віддаленість правопорушника і потерпілої від злочину особи (при вчинені злочину за допомогою мережі Інтернет майже відсутні відмінності у протиправних діях щодо комп'ютерних систем, які розташовані в одному будинку, від злочинної атаки на системи в інших місті або країні);

– висока латентність кіберзлочинності.

Серед основних причин латентності кіберзлочинів та утруднення фактів їх виявлення можна виокремити такі:

– завдана шкода від вчиненого кіберзлочину здається потерпілій стороні незначною порівняно з громіздкістю та довготривалістю процесу розслідування, що, у свою чергу, не гарантує в подальшому притягнення винної особи до кримінальної відповідальності та відшкодування завданої шкоди;

– некомпетентність працівників правоохоронних органів держави в питаннях встановлення факту вчинення кіберзлочину, з'ясування всіх обставин події, виявлення та фіксація слідової картини правопорушення (Європейський суд з прав людини, оцінюючи криміналістичні методики розслідування деяких категорій злочинів правоохоронними органами України, серед основних негативних рис виділив явне та свідоме непроведення особами, які здійснюють розслідування, необхідних мінімальних дій із витребування й оцінювання доказів щодо відповідних подій [6, с. 7]);

– побоювання потерпілої сторони нашкодити власній репутації і втратити значну кількість клієнтів або партнерів по бізнесу внаслідок звернення до правоохоронної системи за допомогою (ця обставина притаманна холдингам, фінансово-промисловим корпораціям і банкам, які в результаті стрімкого розвитку широко запроваджують автоматизацію виробничих процесів);

– неминуче розкриття під час проведення розслідування діючої системи безпеки потерпілої юридичної особи;

– існування ризику, що під час розслідування кіберзлочину будуть виявлені та встановлені незаконні механізми вчинення окремих фінансово-економічних операцій, проведення протиправних фінансово-технічних дій, а також виникнуть сумніви у придатності та компетентності окремих посадових осіб у складі персоналу та керівництва потерпілої від кіберзлочину юридичної особи, що може призвести до виникнення негативних для них наслідків.

Основні види кіберзлочинів законодавець закріпив у ч. 3 ст. 190 і статтях 200, 231, 361–363[1] Кримінального кодексу України [7].

Залежно від мотиву вчинення кіберзлочини можна класифікувати на: направлені на заволодіння інформацією (зокрема, для власного користування або подальшого продажу); направлені на заволодіння коштами, втручання в роботу інформаційних систем з метою отримання доступу до автоматизованих систем управління (для навмисного пошкодження за винагороду або нанесення шкоди конкурентам); направлені на вчинення за допомогою кіберзлочинів інших злочинів.

Виходячи з характеристик злочинної діяльності, способів посягання на індивідуальну власність особи (інформацію), а також специфіки об'єкта і предмета злочинного посягання, встановити та виокремити слідову картину такого виду злочинів неможливо без участі спеціаліста в галузі кібербезпеки та проведення відповідної експертизи.

Сучасна наука постійно збагачується новими методами дослідження, з'являються нові наукові підходи. Це притаманно і судовій експертизі, в якій широко використовуються нові досягнення медицини, фізики, хімії, біології, електротехніки, програмування й інших наук. Значно розширюють можливості та скорочують строки виконання експертиз пошуково-діагностичні комп'ютерні програми, які постійно розробляються і запроваджуються в експертну практику. Все це свідчить про необхідність наявності певного специфічного багажу знань як у правоохо-

ронців, суддів і криміналістів, так і в експертів у галузі юриспруденції.

Існують поняття суб'єктів й об'єктів правовідносин. Суб'єктами правовідносин виступають посадові особи, які наділені правом призначення експертиз, експерти, спеціалісти, підозрюваний (обвинувачений), потерпілий та деякі інші учасники провадження – сторони кримінального провадження, що зазначено у статтях 69, 71, 101 Кримінального процесуального кодексу України [8]. Одним з об'єктів експертно-процесуальних відносин є експертиза, яка виникла з потреби права у вирішенні спеціальних питань правової практики.

Система судових експертиз в Україні покликана надавати допомогу органам правосуддя під час захисту прав і законних інтересів осіб та організацій, які потерпіли від злочинів, а також осіб, які потерпіли від незаконного та необґрунтованого обвинувачення, осуду, обмеження прав і свобод. Законом визначені правові, організаційні та фінансові основи судово-експертної діяльності з метою забезпечення правосуддя України незалежною, кваліфікованою і об'єктивною експертизою, орієнтованою на максимальне використання досягнень науки і техніки [9]. Експертно-криміналістична діяльність не може здійснюватися без врахування цих вимог.

На етапі досудового розслідування кримінальних проваджень судовій експертизі належить важлива (а в деяких випадках вирішальна) роль. Більшість правових питань без проведення експертизи просто не може бути вирішена.

Крім того, перед слідчим постає завдання оцінки експертного дослідження, що можливо лише шляхом детального вивчення й об'єктивної упевненості в науковому обґрунтуванні висновків. Усе це передбачає наявність серйозних знань основних питань судової експертизи, а також досягнень сучасних науки і техніки.

У практиці правоохоронних органів сьогодні найбільш застосовуваними є криміналістичні, судово-медичні, судово-хімічні, судово-психіатричні, психолого-психіатричні експертизи, а також судові експертизи об'єктів, виконані із застосуванням комп'ютерних технологій [10, с. 6], інакше кажучи, комп'ютерно-технічні експертизи. Об'єктами останніх є комп'ютери в зібраному вигляді та їх системні блоки, периферійні пристрої (дисплеї, принтери, дисководи тощо), магнітні носії інформації, роздруківки програмних і текстових файлів, словники знакових систем, класифікатори, технічна документація, електронні записні книжки, ноутбуки, планшети, мобільні пристрої та устаткування до них, інші носії текстової або цифрової інформації.

Завдання, які вирішуються під час проведення комп'ютерно-технічних експертиз, поділяють на діагностичні й ідентифікаційні [10, с. 200].

Наведемо приблизний перелік питань, які з'ясовуються за допомогою проведення експертизи об'єктів, виконаних із застосуванням комп'ютерних технологій.

1. Під час технічної експертизи комп'ютерів та їх комплектуючих:

а) діагностичні питання:

– модель наданого на дослідження комп'ютера;

– технічні характеристики системного блоку та периферійних пристроїв комп'ютера;

– технічні характеристики конкретної обчислювальної мережі;

– місце і час зібрання комп'ютера та його комплектуючих;

– у яких умовах (на заводі чи кустарно) здійснено збирання комп'ютера;

– відповідність внутрішніх налаштувань комп'ютера та його периферії технічній документації, що додається;

– чи були внесені до конструкції комп'ютера які-небудь зміни;

– перевірка справності зазначеного комп'ютера та його комплектуючих;

– ступінь спрацьованості комп'ютера та його комплектуючих;

– причина несправності комп'ютера та периферійних пристроїв;

– чи мають магнітні носії інформації які-небудь фізичні дефекти;

– чи проводилася переробка (адаптація) комп'ютера для роботи на ньому спе-

цифічним користувачем (людиною зі слабким зором, лівшою та ін.);

– технічні характеристики інших електронних пристроїв приймання, накопичення та передавання інформації;

б) ідентифікаційні завдання:

– чи мають комплектуючі комп'ютера єдине джерело походження.

2. Під час експертизи програмного забезпечення та комп'ютерної інформації:

а) діагностичні питання:

– операційна система комп'ютера;

– зміст інформації, що зберігається на внутрішніх і зовнішніх магнітних носіях;

– призначення програмних продуктів;

– алгоритм функціонування програмних продуктів, спосіб введення та виведення інформації;

– чи є програмний продукт ліцензійним;

– чи були внесені у програмний продукт які-небудь корективи, що змінюють виконання деяких операцій;

– відповідність отриманого програмного продукту технічному завданню;

– чи використовувалися паролі, програми захисту прихованих файлів для ускладнення доступу до інформації;

– зміст прихованої інформації;

– чи здійснювалися спроби підбору паролів, зламу засобів захисту чи інших засобів або інші спроби несанкціонованого доступу до інформації з обмеженим доступом;

– можливість відновлення знищених файлів, дефектних магнітних носіїв інформації, зміст інформації на них;

– механізм витоку інформації з локальних мереж, глобальних мереж і розподілених баз даних;

– наявність збоїв у функціонуванні комп'ютера, роботі окремих програм, їх причини;

– чи є причиною збоїв у роботі комп'ютера наявність вірусу;

– можливість відновлення пошкодженої вірусом інформації;

– зміст інформації, що зберігається на мобільному пристрої, планшеті, в електронній записній книжці;

– час проведення останнього коригування файлу (інсталяції конкретного програмного продукту);

– рівень професійної підготовки в галузі програмування та роботи з комп'ютерною технікою особи, яка здійснювала зазначені дії з комп'ютером і програмним забезпеченням;

– чи міститься на носіях інформації, наданих на експертизу, інформація щодо логінів і паролів до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів інтернет-банкінгу та інших ресурсів, якщо так, то в якому вигляді;

– атрибути (час створення, редагування, видалення тощо) виявлених файлів, що містять інформацію щодо логінів і паролів до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів інтернет-банкінгу та інших ресурсів;

– чи містять носії інформації наданих на експертизу об'єктів дослідження сліди доступу до веб-ресурсів хостинг-провайдерів (необхідно зазначити приклади останніх);

– чи містять носії інформації наданих на експертизу об'єктів дослідження сліди доступу до серверу з IP-адресою (необхідно зазначити останню), яка належить до діапазону IP-адрес хостинг-провайдера (зазначити провайдера) та до веб-ресурсів (зазначити ресурси) і ресурсів платіжної системи (зазначити назву останньої);

– чи містять носії інформації наданих на експертизу об'єктів дослідження програмне забезпечення, яке визначається антивірусним програмним забезпеченням експерта як шкідливе, якщо так, то чи є сліди його використання або розповсюдження;

– чи містять носії інформації наданих на експертизу об'єктів дослідження збережені у веб-браузерах логіни та паролі;

– чи містять носії інформації наданих на експертизу об'єктів дослідження відомості про графічні файли, що містять напис *valid*, *invalid*;

– чи містять носії інформації наданих на експертизу об'єктів дослідження програмне забезпечення для створення

(написання) веб-ресурсів та збережені шаблони веб-сайтів;

– чи містять носії інформації наданих на експертизу об'єктів дослідження історію браузера (якщо так, то потрібно її зберегти);

– чи містять носії інформації наданих на експертизу об'єктів дослідження програмне забезпечення типу (необхідно зазначити тип), яке за своїм функціоналом призначене для перевірки валідності (дієвості) логінів і паролів входу до облікових записів соціальних мереж, електронних поштових скриньок, кабінетів інтернет-банкінгу та інших ресурсів (якщо так, то чи наявні сліди використання вказаного програмного забезпечення);

б) ідентифікаційні питання:

– особа, якою була створена комп'ютерна програма;

– чи могла комп'ютерна програма бути створена конкретним спеціалістом.

Як **висновок** зазначимо, що, на нашу думку, кіберзлочинність є досить новим і специфічним явищем злочинної діяльності, яка постійно розвивається через поширення й удосконалення глобальної мережі Інтернет. Саме новизна, специфічність, неухильний і постійний розвиток вказаного виду злочинів вимагають від судових та правоохоронних органів, криміналістів розроблення та застосування нових криміналістичних засобів і методів для їх виявлення та фіксації з метою подальшого використання під час проведення ефективного розслідування, встановлення та притягнення винних осіб до відповідальності.

Зважаючи на наявність недоліків у цій сфері процесуально-правової та експертно-криміналістичної діяльності, вважаємо актуальними подальші дослідження відповідної спрямованості, адже вони створюватимуть перспективи теоретичних і практичних напрацювань та сприятимуть вирішенню проблемних питань у цьому напрямку.

Література

1. Крылов И. Ф. Криминалистика. Л. : Изд-во Ленинград. ун-та, 1976. 591 с.

2. Гросс Г. Руководство для следователей как система криминалистики. СПб., 1908. Предисл., с. XI.

3. Белкин Р. С. Теория отражения и методологические проблемы криминалистики. М., 1970. 623 с.

4. Жогин Н. В. Руководство для следователей. М. : Юрид. лит., 1971. 752 с.

5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 05.07.2020).

6. Севастьянова Н. І. Практика Європейського суду з прав людини. Рішення. Коментарі. Київ : ІНПРЕС, 2015. 240 с.

7. Кримінальний кодекс України : Закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 05.07.2020).

8. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 № 4651-VI // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4651-17 (дата звернення: 05.07.2020).

9. Про судову експертизу : Закон України від 25.02.1994 № 4038-XII // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/4038-12 (дата звернення: 05.07.2020).

10. Колкутин В. В. Судебные экспертизы. Изд. 2-е, доп. М. : Юрлитинформ, 2006. 287 с.

Osmolian V. A.

PROSPECTS FOR THE DEVELOPMENT OF CRIMINALISTICS IN THE LIGHT OF NEW CRIMINAL THREATS, NAMELY: CYBERCRIME

The article contains the legal basis and prospects of development of criminalistics (criminology) in the light of new criminal threats at fast distribution of the phenomena of cybercrime and cyber-attacks are stated. The author introductions of a new field of knowledge in «forensic cyberspace». Article

АНОТАЦІЯ

Наведено правові основи та перспективи розвитку криміналістики у світлі нових кримінальних загроз – стрімкого поширення кіберзлочинності та кібератак. Запропоновано введення нової галузі знань з криміналістичного кіберпростору, розкрито її значення та місце в системі криміналістики в цілому. Розглянуто процесуально-правові й експертно-криміналістичні питання щодо можливості виявлення, фіксації та збирання слідової картини і формування доказової бази під час розслідування кіберзлочинів, а також обґрунтовано необхідність ефективної співпраці працівників слідчих органів, прокуратури, суду та експертно-криміналістичних установ для якісного й об'єктивного виконання завдань кримінального провадження і покращення інноваційної політики України. Наведено конкретні приклади завдань, які потрібно вирішити експертам під час проведення експертиз (досліджень). Зроблено висновки та надано рекомендації щодо узгодженого застосування норм чинного законодавства у практичній діяльності експерта-криміналіста та слідчого. Звернено увагу на необхідність подальшої наукової співпраці вчених і спеціалістів у галузі матеріального та процесуального права.

Ключові слова: криміналістика, комп'ютер, кіберзлочин, кібербезпека, інформація, правоохоронні органи, досудове розслідування, кримінальне провадження, експертиза, експерт, спеціаліст.

describes and reveals the importance and place of this industry in the forensic system as a whole. Procedural-legal and forensic issues concerning the possibility of detecting, fixing and collecting a trace and the formation of the evidence base in the commission of cybercrime are considered. To direct one's attention to need for effective cooperation of employees of investigate bodies, prosecutor's office, court and forensic institutions for high-quality and objective implementation of the tasks of criminal proceedings and improvement of innovation policy of Ukraine is also substantiated. Specific examples of tasks that were set for the solution of experts in conducting examinations (research), which took place in practice. Conclusions are made and recommendations on the coordinated application of current legislation in the practice of forensic science and investigator. Attention is drawn to the need for further scientific cooperation of scientists, specialists in the field of substantive and procedural law.

Keywords: *criminalistics (criminology), computer, cybercrime, cyber security, information, police, pre-trial investigation, criminal, proceedings, expertise, expert, specialist.*