

**МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ**

ТЕПЛИЦЬКИЙ БРОНІСЛАВ БРОНІСЛАВОВИЧ



УДК 343.983:[343.34:004]

**ТЕХНІКО-КРИМІНАЛІСТИЧНЕ ЗАБЕЗПЕЧЕННЯ
РОЗСЛІДУВАННЯ ЗЛОЧИНІВ У СФЕРІ ВИКОРИСТАННЯ
ЕЛЕКТРОННО-ОБЧИСЛЮВАЛЬНИХ МАШИН (КОМП'ЮТЕРІВ),
СИСТЕМ ТА КОМП'ЮТЕРНИХ МЕРЕЖ І МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ**

12.00.09 – кримінальний процес та криміналістика;
судова експертиза; оперативно-розшукова діяльність

**Автореферат дисертації на здобуття наукового ступеня кандидата
юридичних наук**

Київ–2021

Дисертацією є рукопис

Робота виконана в Національній академії внутрішніх справ,
Міністерство внутрішніх справ України

Науковий керівник доктор юридичних наук,
старший науковий співробітник
Арешонков Віталій Володимирович,
Національна академія внутрішніх справ,
провідний науковий співробітник науково-дослідної лабораторії
з проблем криміналістичного забезпечення та судової експертології

Офіційні опоненти:

доктор юридичних наук, доцент, старший науковий співробітник,
заслужений юрист України

Рогатюк Ігор Володимирович,
Національна академія Служби безпеки України,
професор кафедри кримінального процесу та криміналістики
навчально-наукового гуманітарного інституту

кандидат юридичних наук, доцент

Давиденко Валерій Степанович,
Міжрегіональна академія управління персоналом,
професор кафедри управління безпекою,
правоохоронної та антикорупційної діяльності

Захист відбудеться «20» грудня 2021 року о 12.00 годині на засіданні спеціалізованої вченої ради Д 26.007.05 у Національній академії внутрішніх справ за адресою: 03035, м. Київ, пл. Солом'янська, 1

З дисертацією можна ознайомитись у бібліотеці Національної академії внутрішніх справ за адресою: 03035, м. Київ, пл. Солом'янська, 1

Автореферат розісланий «19» листопада 2021 року

Учений секретар
спеціалізованої вченої ради



Д. О. Савицький

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Аналіз криміногенної ситуації в Україні та практики органів досудового розслідування підтверджує тенденцію до збільшення кількості випадків кримінальних правопорушень, пов'язаних з обігом комп'ютерної інформації, а також діянь, у яких комп'ютерні інформаційні системи є засобами та знаряддями їх учинення або ж використовуються для приховування факту і слідів злочинної діяльності, а також спрямування зусиль правоохоронців на хибні об'єкти. Процеси глобальної інформатизації безпосередньо впливають на криміногенну ситуацію, обумовлюють нові способи і технології злочинних посягань в інформаційному просторі й середовищі комп'ютерних мереж.

Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, а також мереж електрозв'язку здебільшого високолатентні. Поряд з відсутністю очевидної слідової картини й традиційного «місця події» доволі ускладненим є збирання доказів, що зумовлено як застосуванням засобів віддаленого доступу, так і специфічним, нематеріальним, елементом обстановки – кібернетичним простором.

Злочинній діяльності відповідного спрямування притаманні переважно системний, професійний і груповий характер, наявність у правопорушників спеціальних знань, умінь і навичок у різних галузях науки і техніки (електроніка, електротехніка, програмування, телекомунікації, зв'язок тощо).

Згідно з офіційною статистикою, динаміка цієї категорії кримінальних правопорушень в Україні має тенденцію до щорічного зростання: якщо у 2013 р. їх зареєстровано 595, то тільки за 10 місяців 2021 р. – 2,8 тис. Йдеться про «класичні» кіберзлочини (ст. 361–363-1 КК України): несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (1,4 тис. або 50 %); несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації (1,2 тис. або 44 %) тощо¹.

Отже, забезпечення швидкого, повного та неупередженого розслідування і судового розгляду відповідних кримінальних проваджень неможливе без комплексного криміналістичного забезпечення. Відтак особливої актуальності набуває переосмислення теоретичних, правових і практичних основ використання слідчим (дознавачем), спеціалістом та експертом сучасних техніко-криміналістичних засобів з метою отримання орієнтувальної та доказової інформації, зокрема під час проведення слідчих (розшукових) та інших процесуальних дій.

Теоретичним підґрунтям дослідження стали праці вітчизняних й іноземних учених різних часів, зокрема: Ю. П. Аленіна, В. В. Арешонкова, І. В. Басистої, В. П. Бахіна, В. Д. Берназа, Р. С. Белкіна, Т. В. Варфоломеевої, В. І. Василичука,

¹ Про зареєстровані кримінальні правопорушення та результати їх досудового розслідування (2012–2021 рр.): статистична інформація Генеральної прокуратури України. URL: <http://www.gp.gov.ua/ua/stat.html>.

Г. П. Власової, А. Ф. Волобуєва, В. І. Галагана, В. Г. Гончаренка, В. Я. Горбачевського, І. В. Гори, В. А. Журавля, А. П. Запотоцького, А. В. Іщенко, Н. І. Клименко, І. І. Когутича, В. А. Колесника, О. Н. Колесніченка, В. П. Колмакова, В. О. Коновалової, В. С. Кузьмічова, В. В. Лисенка, В. К. Лисиченка, В. Г. Лукашевича, Є. Д. Лук'янчикова, Д. М. Мірковця, А. В. Мовчана, Д. Й. Никифорчука, В. Т. Нора, О. В. Одерія, Ю. Ю. Орлова, В. Л. Ортинського, І. В. Пирога, М. А. Погорецького, І. В. Рогатюка, М. В. Салтевського, М. Я. Сегая, Д. Б. Сергєєвої, О. С. Старенького, Р. Л. Степанюка, О. В. Таран, О. Ю. Татарова, В. В. Тіщенко, В. В. Топчія, Л. Д. Удалової, В. І. Фаринника, В. Г. Хахановського, П. В. Цимбала, К. О. Чаплинського, С. С. Чернявського, Ю. М. Черноус, В. М. Шевчука, В. Ю. Шепітька, М. Г. Щербаковського та ін.

На монографічному рівні питання протидії комп'ютерній злочинності та забезпечення цієї діяльності в кримінально-правовому, кримінальному процесуальному, кримінологічному та криміналістичному аспектах вивчали Л. А. Безуглий, Л. В. Борисова, В. О. Голубєв, А. І. Журба, Н. В. Карчевський, Т. В. Коршикова, О. І. Мотлях, Л. П. Паламарчук, Д. В. Пашнєв, О. Д. Ричка, Н. А. Розенфельд, С. В. Шапочка, І. Р. Шинкаренко та інші науковці. Водночас засади техніко-криміналістичного забезпечення розслідування комп'ютерних злочинів на рівні дисертаційних робіт окремо не розглядалися. З урахуванням стрімких змін у законодавстві, злочинній діяльності та правоохоронній практиці зазначена проблематика потребує цільового комплексного дослідження.

Зв'язок роботи з науковими програмами, планами, темами. Дисертацію виконано відповідно до положень Стратегії сталого розвитку «Україна – 2020» (Указ Президента України № 5/2015), Стратегії національної безпеки України (Указ Президента України № 392/2020), Стратегії розвитку системи Міністерства внутрішніх справ України до 2020 року (розпорядження Кабінету Міністрів України № 1023-р/2017), Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років (наказ МВС України № 275/2015), Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України № 454/2020), Основних напрямів наукових досліджень Національної академії внутрішніх справ на 2018–2020 роки (рішення Вченої ради НАВС від 26 грудня 2017 р., протокол № 28/1).

Тему дисертації затверджено рішенням Вченої ради Національної академії внутрішніх справ 22 грудня 2015 р. (протокол № 23).

Мета і задачі дослідження. *Метою* дисертації є розроблення теоретичних положень та науково обґрунтованих рекомендацій щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Реалізація поставленої мети зумовила необхідність вирішення таких *задач*:

– з'ясувати стан наукового розроблення проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-

обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– визначити поняття, зміст і суб'єктів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– висвітлити найкращий зарубіжний досвід техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– запропонувати поняття та здійснити розподіл техніко-криміналістичних засобів, що застосовуються під час досудового розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– розкрити особливості техніко-криміналістичного забезпечення проведення окремих слідчих (розшукових) дій у досліджуваній категорії кримінальних проваджень, надати пропозиції з удосконалення такого забезпечення;

– визначити специфіку та запропонувати рекомендації з удосконалення техніко-криміналістичного забезпечення проведення окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– розкрити особливості призначення найбільш типових видів судових експертиз при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– виявити типові помилки при призначенні експертизи комп'ютерної техніки і програмних продуктів як найбільш поширеного різновиду судових експертиз за злочинами даної категорії, запропонувати шляхи їх попередження;

– визначити особливості оцінки результатів судових експертиз та напрями їх використання під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Об'єкт дослідження – правовідносини, що виникають під час досудового розслідування і судового розгляду кримінальних правопорушень у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Предмет дослідження – техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Методи дослідження обрано з огляду на специфіку об'єкта, предмета, мети й задач дослідження, а саме: *загальнонаукові методи (спостереження, порівняння, опису, класифікації)* – для визначення та систематизації правових категорій, що характеризують злочинну діяльність і слідчу практику, а також спеціальні методи:

історико-правовий – для висвітлення етапів розвитку кримінального, кримінального процесуального законодавства, практики забезпечення органів досудового розслідування техніко-криміналістичними засобами і методами (підрозділ 1.1); *системно-структурний* – для розгляду видів і загальних вимог до техніко-криміналістичного забезпечення проведення слідчих (розшукових) дій, у тому числі негласних (підрозділи 1.2, 1.3, 2.2, 2.3); *догматичний* – з метою тлумачення понять і категорій кримінального процесу, криміналістики, оперативно-розшукової діяльності, що сприяло уточненню понятійно-категоріального апарату дослідження (розділи 1–3); *формально-логічний* – під час розгляду сутності техніко-криміналістичного забезпечення огляду, обшуку, допиту, проведення експертиз у процесі розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (підрозділ 2.2, розділ 3); *моделювання* – для розроблення й упровадження в практику алгоритмів дій під час призначення експертиз у досліджуваній категорії кримінальних проваджень (підрозділи 3.1, 3.2); *соціологічні* – для з'ясування думок працівників правоохоронних органів щодо перспектив удосконалення техніко-криміналістичного забезпечення розслідування кримінальних правопорушень цієї категорії (розділи 1–3); *статистичний* – для узагальнення результатів соціологічних досліджень, вивчення матеріалів кримінальних проваджень (розділи 1–3).

Емпіричну базу дослідження становлять результати вивчення та узагальнення 285 кримінальних проваджень щодо злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку упродовж 2016–2021 років; зведені дані опитування 180 слідчих, 350 судових експертів з Вінницької, Дніпропетровської, Житомирської, Закарпатської, Запорізької, Івано-Франківської, Київської, Львівської, Одеської, Рівненської, Чернівецької областей та м. Києва; статистичні й аналітичні матеріали Департаменту інформаційно-аналітичної підтримки Національної поліції України, Державного науково-дослідного експертно-криміналістичного центру МВС України, Офісу Генерального прокурора, Державної судової адміністрації України за 2016–2021 роки, а також результати багаторічного вивчення слідчої та судово-експертної практики з урахуванням значного досвіду роботи автора в експертних підрозділах МВС України.

Наукова новизна одержаних результатів полягає в тому, що дисертація є одним з перших в Україні комплексних монографічних досліджень засад техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. У роботі сформульовано й обґрунтовано низку положень і висновків теоретичного та практичного спрямування, а саме:

вперше:

– запропоновано визначення техніко-криміналістичних засобів розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку як системи

спеціально виготовлених або пристосованих приладів, пристроїв, засобів вимірювальної техніки, допоміжного обладнання, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, а також криміналістичних технологій їх ефективного застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів;

– запропоновано нормативне закріплення діяльності комп'ютерно-технічної лабораторії у складі спеціалізованої пересувної лабораторії Експертної служби МВС та необхідність її залучення під час розслідування злочинів у даній сфері;

– надано пропозиції до кримінально процесуального законодавства щодо посилення захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій та зберігання технічних засобів і первинних носіїв інформації, які використовувались під час проведення негласних слідчих (розшукових) дій;

– узагальнено типові помилки під час призначення експертизи комп'ютерної техніки та програмних продуктів, з поділом їх щодо якості і кількості поданих на дослідження об'єктів, процесуальних питань винесення постанов (ухвал) про призначення експертизи тощо, розроблено комплекс заходів з їх попередження;

– обґрунтовано необхідність, з метою підвищення ефективності розслідування злочинів даної категорії, запровадження відповідної спеціалізації слідчих Національної поліції України, а також регламентації у вимогах до цих посад крім юридичної наявності професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом;

удосконалено:

– поняття техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку шляхом включення до нього в якості складових елементів сукупності техніко-криміналістичних засобів та прийомів їх застосування, діяльності уповноважених суб'єктів щодо створення належних умов для використання зазначених засобів, а також системи наукових положень, спрямованих на реалізацію практичних завдань із застосування криміналістичної техніки;

– поняття та класифікацію суб'єктів техніко-криміналістичного забезпечення розслідування злочинів даної категорії як осіб, які реалізують свої повноваження на підставі чинного законодавства, використовуючи техніко-криміналістичні засоби для здійснення ефективного розслідування злочинів; поділ їх на індивідуальних та колективних суб'єктів;

– положення щодо організації і тактики застосування техніко-криміналістичних засобів під час проведення огляду, обшуку, допиту у кримінальних провадженнях при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– критерії оцінки висновків експертів з урахуванням кількісно-якісних характеристик наданих на дослідження об'єктів і порівняльних зразків,

застосованих експертом методик, повноти досліджень, правильності опису та наукової обґрунтованості проміжних і підсумкових висновків;

дістало подальший розвиток:

– визначення напрямів наукових досліджень різних аспектів техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– рекомендації на основі аналізу зарубіжного досвіду з удосконалення правового регулювання протидії кіберзлочинам, залучення вітчизняних фахівців у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку до вирішення завдань техніко-криміналістичного забезпечення розслідування кіберзлочинів, а також міжнародної технічної допомоги, пов'язаної з техніко-криміналістичним забезпеченням протидії кіберзлочинам в Україні тощо;

– наукові погляди щодо видів техніко-криміналістичних засобів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку з їх розподілом на апаратні та програмні засоби мобільної криміналістики; апаратні блокіратори запису; програмні засоби копіювання даних; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите спеціалізоване програмне забезпечення; дистрибутиви на основі Linux;

– рекомендації з техніко-криміналістичного забезпечення проведення окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку;

– бачення можливостей судових експертиз для встановлення обставин учинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку та рекомендацій з підготовки до їх призначення.

Практичне значення одержаних результатів полягає в тому, що результати дисертації впроваджено та може бути використано в:

законотворчій діяльності – при підготовці змін та доповнень до нормативно-правових актів, якими регламентуються призначення і проведення судових експертиз та експертних досліджень (довідка Інституту законодавства Верховної Ради України від 16 травня 2019 р. № 22/696-1-15);

правозастосовній діяльності – у системі службової підготовки та в оперативно-службовій діяльності органів досудового розслідування й експертних підрозділів МВС України (акт Головного слідчого управління Національної поліції України від 16 серпня 2021 р.; акт Державного науково-дослідного експертно-криміналістичного центру МВС України від 15 квітня 2021 р.);

освітньому процесі – під час викладання блоку навчальних дисциплін з криміналістики, розслідування окремих категорій кримінальних правопорушень, судової експертизи, підготовки навчальних та методичних посібників,

підручників, курсів лекцій і проведення наукових досліджень відповідного спрямування (акт Національної академії внутрішніх справ від 04 жовтня 2021 р.).

Особистий внесок здобувача. Дисертація є самостійною, завершеною науковою працею. Сформульовані в ній узагальнення, висновки, рекомендації та пропозиції обґрунтовано на підставі самостійно здійснених досліджень. В опублікованому у співавторстві науково-практичному посібнику «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз» власні теоретичні розробки дисертанта становлять не менше 25 %. Наукові ідеї та висновки, що належать співавторам, у дисертації не використано.

Апробація результатів дисертації. Основні положення та висновки дисертації оприлюднено на трьох міжнародних і всеукраїнських науково-практичних конференціях та засіданнях круглих столів, серед яких: «Судова експертиза: сучасність та майбутнє» (Львів, 25 січня 2018 року); «Актуальні проблеми криміналістики та судової експертології» (Київ, 22 листопада 2018 року); «Використання досягнень сучасної науки й техніки в розкритті злочинів» (Київ, 25 лютого 2021 р.); «Кримінальне судочинство: сучасний стан та перспективи розвитку» (Київ, 28 травня 2021 р.); «Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності» (Кропивницький, 24 вересня 2021 року).

Публікації. Результати дослідження, що сформульовані в дисертації, відображено в 12 наукових публікаціях, серед яких п'ять статей – у збірниках, включених МОН України до переліку наукових фахових видань з юридичних наук, одна – в іноземному науковому періодичному виданні, п'ять тез – у збірниках матеріалів міжнародних і всеукраїнських науково-практичних конференцій, засідань круглих столів, а також одна праця, яка додатково відображає наукові результати дисертації.

Структура та обсяг дисертації. Робота складається з анотації, переліку умовних позначень, вступу, трьох розділів, що містять дев'ять підрозділів, висновків, списку використаних джерел (202 найменування на 22 сторінках) і шести додатків (на 31 сторінці). Повний обсяг дисертації становить 268 сторінок, з них основного тексту – 197 сторінок.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність обраної теми дослідження, ступінь наукової розробленості проблеми; визначено зв'язок роботи з науковими програмами, планами й темами, окреслено мету, завдання дослідження, його об'єкт, предмет і використані методи; висвітлено наукову новизну одержаних результатів, їх теоретичне та практичне значення в законотворчій, правозастосовній діяльності й освітньому процесі; наведено дані щодо особистого

внеску здобувача, апробації результатів дослідження, структури та обсягу дисертації.

Розділ 1 «Теоретичні основи техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить три підрозділи.

У підрозділі 1.1 *«Стан наукових досліджень проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»* визначено, що сучасна інформатизація супроводжується побічними негативними явищами криміногенного характеру, у тому числі збільшенням кількості злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

За результатами огляду стану наукового вивчення та законодавчої регламентації проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку встановлено незначний спектр проведених досліджень з цієї тематики за різними галузевими спеціальностями. Наукові праці, в яких розглядалися питання протидії комп'ютерній злочинності, систематизовано в хронологічному порядку (з виокремленням періодизації) та за галузевою ознакою (кримінально-правова кваліфікація, процесуальний порядок розслідування, адміністративно-правова відповідальність, криміналістичне забезпечення). В опублікованих виданнях з проблематики комп'ютерних злочинів переважає комплексне висвітлення питань кримінально-правової кваліфікації та методики розслідування.

Виокремлено низку невирішених завдань криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, зокрема техніко-криміналістичного забезпечення методики розслідування певних категорій кримінальних правопорушень. Так, 87 % опитаних респондентів (слідчі Національної поліції, експерти Експертної служби МВС України) наголосили на невідповідності існуючої методики розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку наявному рівню злочинності в даній сфері. Відповідно, серед положень методики розслідування злочинів даної категорії, які потребують доопрацювання та подальшого розроблення, 62 % опитаних респондентів зазначили необхідність розроблення саме техніко-криміналістичного забезпечення розслідування.

У підрозділі 1.2 *«Поняття, зміст і суб'єкти техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»* розглянуто складові техніко-криміналістичного забезпечення як комплексної організаційно-функціональної системи збирання і дослідження

криміналістично значущої інформації шляхом застосування уповноваженими суб'єктами техніко-криміналістичних методів і засобів.

Зміст техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку утворюють мета й окремі завдання, реалізація яких спрямована на підвищення ефективності проведення досудового розслідування у відповідній категорії кримінальних проваджень.

Встановлено, що мета техніко-криміналістичного забезпечення полягає у виявленні, отриманні, фіксації, вилученні та зберіганні носіїв криміналістично значущої інформації; діагностиці (розпізнавання і встановлення певних характеристик осіб та матеріальних об'єктів); ідентифікації (встановлення тотожності особи або матеріального об'єкта за проявами загальної родової та групової належності порівнюваних матеріальних об'єктів); визначенні ситуації (явища, події або дії осіб) за залишеними матеріальними відображеннями; відтворенні матеріальних об'єктів у їх первісному стані шляхом реконструкції (уявного образу) або реставрації (фізичного відтворення); профілактиці; криміналістичній класифікації (систематизація даних про осіб та матеріальні об'єкти у відповідних криміналістичних інформаційних системах).

Під суб'єктами техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку запропоновано визначити осіб, які мають спеціальні знання (уміння, навички) використання техніко-криміналістичних засобів (індивідуально або у складі професійних колективів), забезпечені необхідними технічними засобами та реалізують свої повноваження, використовуючи техніко-криміналістичні засоби задля здійснення ефективного розслідування. До колективних суб'єктів належать органи досудового розслідування, оперативні підрозділи (Департамент кіберполіції Національної поліції України, його структурні підрозділи, які діють за міжрегіональним принципом), спеціалізовані слідчо-оперативні групи, судово-експертні установи; до індивідуальних – слідчі, які спеціалізуються на розслідуванні кримінальних правопорушень у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку (кіберзлочинів), спеціалісти й судові експерти.

У підрозділі 1.3 «Зарубіжний досвід техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» проаналізовано процесуальне законодавство низки західноєвропейських країн та США щодо регулювання питань протидії кіберзлочинності, технічного забезпечення виявлення та розслідування відповідних категорій кримінальних правопорушень. На основі використання відповідного зарубіжного досвіду запропоновано напрями удосконалення кримінального процесуального законодавства України та практики його застосування в частині регламентації техніко-криміналістичного забезпечення.

Визначено пріоритети міжнародної політики Європейського Союзу в кіберпросторі, що ґрунтується на гармонізації відповідного національного

законодавства країн-учасниць та розвитку потенціалу кібербезпеки через співробітництво з міжнародними партнерами, правоохоронними інституціями, приватним сектором та громадянським суспільством. Досліджено практику забезпечення кібербезпеки у Франції, яка покладається не лише на органи поліції (жандармерії), а й Міністерство оборони та інші спеціальні органи, а також практику Великої Британії, де існує інститут консультантів, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення.

Розділ 2 «Техніко-криміналістичне забезпечення проведення окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить три підрозділи.

У підрозділі 2.1 «Поняття та види техніко-криміналістичних засобів, що застосовуються у досудовому розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» визначено відповідні техніко-криміналістичні засоби як систему спеціально виготовлених або пристосованих приладів, пристроїв, засобів вимірювальної техніки, допоміжного обладнання, інструментів, матеріалів, інформаційних пошукових та ідентифікаційних, а також криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів.

З огляду на матеріали практики, визначено характеристики відповідних техніко-криміналістичних засобів, до яких належать: апаратні засоби мобільної криміналістики (фірмовий планшет Cellebrite UFED Touch 2; MSABXR; апаратні засоби «chip-off» для зняття інформації з чипів пам'яті мобільних пристроїв); програмні засоби мобільної криміналістики («Мобільний криміналіст»; Magnet AXIOM; Belkasoft Evidence Center); апаратні блокувальники запису (Tableau T35U; Wiebitech Forensic Ultra Dockv 5); програмні засоби копіювання даних (Mediaimager GM5); програмні засоби комп'ютерної експертизи (Magnet Axion; Belkasoft Evidence Center; X-Ways Forensics); апаратні засоби відновлення даних (комплекси PC-3000 Express/ Portable/ UDMA/ SAS та інші технічні засоби компанії ACELab; R-Studio; UFS Explorer); відкрите спеціалізоване програмне забезпечення (Autopsy; Photorec; Eric Zimmerman Tools); дистрибутиви на основі Linux (SIFT– Linux-дистрибутив; KaliLinux).

На основі вивчення характеристик зазначених приладів і програмних засобів, а також їх можливостей зроблено висновок, що на сьогодні вони дозволяють з більшою точністю та надійністю віднайти (відновити), зберегти та дослідити інформаційні сліди злочину та носії цифрової інформації, що є важливим для розслідування злочинів даної категорії.

У підрозділі 2.2 «Особливості застосування техніко-криміналістичних засобів при проведенні окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів),

систем та комп'ютерних мереж і мереж електрозв'язку» встановлено, що повнота збирання доказів з матеріальних джерел і від окремих осіб та їх належне процесуальне оформлення залежить від правильної організації роботи спеціалістів у сфері обчислювальної техніки та застосування техніко-криміналістичних засобів з метою ефективного пошуку інформації в комп'ютері (комп'ютерних мережах і мережах електрозв'язку), її вилучення та подальшого дослідження.

Надано криміналістичні рекомендації щодо використання техніко-криміналістичних засобів при огляді комп'ютера, що забезпечують виявлення і фіксацію точних часових характеристик його роботи, факт та зміст користування поштовими програмами, визначення кола кореспондентів тощо. Наведено правила огляду різних носіїв інформації, способи їх пакування, транспортування і зберігання.

З урахуванням практики застосування техніко-криміналістичних засобів конкретизовано тактичні прийоми проведення огляду та обшуку в місцях: збереження й обробки комп'ютерної інформації, яка зазнала злочинного впливу (наприклад, у разі незаконного втручання в роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж); виявлення комп'ютерного обладнання, яке використовувалося при вчиненні злочину (при розповсюдженні комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу); зберігання інформації, отриманої злочинним шляхом (при заволодінні комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем); порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі; настання шкідливих наслідків.

У результаті дослідження проблем допиту під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку встановлено, що при підготовці та проведенні цієї слідчої дії головні труднощі слідчих пов'язані із спеціальною термінологією (71 % респондентів), вибором тактичних прийомів допиту (19 %), встановленням психологічного контакту з особою, яка підозрюється у вчиненні злочину даної категорії (10 %). Запропоновано типовий перелік питань, що підлягають з'ясуванню під час допиту підозрюваних та свідків з числа операторів (адміністраторів) комп'ютерних систем (мереж), програмістів, відповідальних за інформаційну безпеку, співробітників, які здійснюють технічне обслуговування обчислювальної техніки.

У підрозділі 2.3 *«Особливості застосування техніко-криміналістичних засобів при проведенні окремих негласних слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»* досліджено особливості використання техніко-криміналістичних засобів з метою виявлення та фіксації слідів учинення злочину, збереження доказів, які можуть бути знищені до їх вилучення процесуальним шляхом – у 67 % випадків (зняття інформації з транспортних телекомунікаційних мереж); фіксації факту перебування в певному місці та в певний час особи, яка користується радіоелектронним засобом чи іншим пристроєм, що випромінює радіохвилі й

активованій у мережі оператора мобільного зв'язку – у 53 % (спостереження за особою, річчю або місцем, обстеження публічно недоступних місць, житла чи іншого володіння особи, установлення місцезнаходження радіоелектронного засобу, аудіо-, відеоконтроль особи); фіксації поведінки, розмов і місця перебування осіб, яких підозрюють у вчиненні злочину, отримання інформації, розміщеної особою у соціальних мережах, тематичних форумах – у 31 % (зняття інформації з електронних інформаційних систем).

Наголошено на важливості завчасного з'ясування характеру інформації, яка повинна бути досліджена в результаті проведення негласної слідчої (розшукової) дії, оскільки вона може становити державну таємницю або бути конфіденційною, що потрібно враховувати при залученні відповідного спеціаліста. Також з метою підвищення захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій та врегулювання проблемних питань зберігання технічних засобів і первинних носіїв інформації, які використовувались при проведенні таких дій, запропоновано доповнення до ст. 254 та 266 КПК України

Розділ 3 «Судові експертизи під час розслідування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить три підрозділи.

У підрозділі 3.1 *«Види та можливості судових експертиз під час розслідування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку»* констатовано, що ефективність техніко-криміналістичного забезпечення злочинів у досліджуваній категорії проваджень залежить від своєчасного проведення необхідних експертиз, як традиційних (дактилоскопічні, трасологічні, фоноскопичні, економічні, технічні експертизи документів), так і спеціальних, які вирішують низку пошукових діагностичних та ідентифікаційних завдань, що стосуються дослідження електронно-обчислювальної техніки, відповідної інформації та програмного забезпечення.

Типовими видами судових експертиз, які проводяться під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, є: експертиза комп'ютерної техніки і програмних продуктів (98 % кримінальних проваджень); експертиза телекомунікаційних систем і засобів (5 %); традиційні криміналістичні (трасологічна, дактилоскопічна, технічна експертиза документів тощо) (18 %); судово-економічні (4 %); біологічні (2 %); а також комплексні (комп'ютерно-технічна та судово-бухгалтерська експертиза, комп'ютерно-технічна та судово-товарознавча експертиза, комп'ютерно-технічна й експертиза об'єктів інтелектуальної власності тощо) (1 %) та комісійні експертизи (1 %). Встановлено, що для дослідження комп'ютерної інформації найбільше значення мають експертизи комп'ютерної техніки і програмних продуктів та експертизи телекомунікаційних систем і засобів.

У підрозділі 3.2 *«Експертизи комп'ютерної техніки і програмних продуктів та телекомунікаційних систем і засобів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та*

комп'ютерних мереж і мереж електрозв'язку» досліджено підстави призначення, об'єкти і предмет, особливості проведення відповідних судових експертиз.

Визначено місце експертизи комп'ютерної техніки та програмних продуктів у системі судових експертиз, виділено три її підвиди, залежно від груп об'єктів, які розподілено на три види: апаратні (персональні комп'ютери, периферійні пристрої до персональних комп'ютерів, мережеві апаратні засоби, інтегровані системи, будь-які комплектувальні зазначених об'єктів); програмні (системне і прикладне програмне забезпечення); інформаційні (текстові й графічні файли, аудіовізуальні (мультимедійні) дані та ін.).

На підставі вивчення слідчої й експертної практики виокремлено типові помилки, що допускають ініціатори проведення експертиз комп'ютерної техніки та програмних продуктів, зокрема: 1) під час проведення слідчої дії оглядаються та вилучаються не всі об'єкти, які містять інформаційні сліди злочину (23 % опитаних респондентів); 2) об'єкти вилучаються, зберігаються чи транспортуються без дотримання відповідних правил (10 %); 3) на експертизу надаються об'єкти, які апріорі не можуть містити інформації, що має значення для розслідування, або які з об'єктивних причин неможливо належно дослідити (7 %); 4) на вирішення експертизи ставляться питання, що не стосуються обставин справи або ж є некоректними (35 %); 5) однією постановою (ухвалою) призначають експертизи за різними видами об'єктів або ж за їх надмірною кількістю (17 %).

Виокремлено типові питання, що вирішує експертиза телекомунікаційних систем та засобів, які систематизовано відповідно до призначення, працездатності, тактико-технічних характеристик і походження телекомунікаційного засобу (системи), а також можливостей взаємодії телекомунікаційного засобу з іншими приладами (програмним забезпеченням).

У підрозділі 3.3 «Оцінка та використання результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» проаналізовано відповідні елементи процесу доказування з урахуванням специфіки висновків експертиз у досліджуваній категорії кримінальних проваджень.

Оцінку висновку експерта розглянуто через перевірку слідчим, прокурором, судом його допустимості, достовірності, належності, застосування науково обґрунтованої методики, повноти і логічної обґрунтованості дослідження та загалом його доказового значення.

За необхідності при оцінці висновку експерта рекомендовано отримувати консультаційно-довідкову допомогу експерта, який проводив експертизу, або залучати спеціаліста у сфері електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, який не зацікавлений у результатах справи.

Наголошено на меті використання слідчим, прокурором, судом результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних

мереж і мереж електрозв'язку, запропоновано рекомендації щодо вивчення та використання висновку експерта в досліджуваній категорії кримінальних проваджень.

ВИСНОВКИ

У **висновках** дисертації сформульовано наукові положення та отримано результати, що в сукупності розв'язують важливе наукове завдання, яке полягає в розробленні теоретичних положень та науково обґрунтованих рекомендацій щодо техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Найсуттєвішими з них є такі:

1. На сучасному етапі питання розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку досить детально розроблені у кримінально-правовій, кримінально процесуальній та адміністративно-правовій науці. Водночас у криміналістиці більшість наукових праць присвячено загальному дослідженню використанню спеціальних знань при розслідуванні злочинів, учинених із застосуванням комп'ютерних технологій, особливостям встановлення обставин, які підлягають доказуванню у справах про комп'ютерні злочини; окремого комплексного дослідження техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку не проводилось.

2. Зміст техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку становлять мета, на досягнення якої спрямовується така діяльність, а також завдання як окремі напрями досягнення такої мети, які полягають у виявленні, збиранні, фіксації доказової інформації; подальшому аналізі такої інформації; залученні до слідчих (розшукових), негласних слідчих (розшукових) дій компетентних осіб; техніко-криміналістичному супроводі, який здійснюється в організаційних і процесуальних формах під час досудового розслідування; оснащенні уповноважених суб'єктів сучасними техніко-криміналістичними засобами; формуванні в таких суб'єктів умінь і навичок практичного застосування криміналістичної техніки. Суб'єктів техніко-криміналістичного забезпечення за статусом розподілено на індивідуальні (слідчі, дізнавачі, слідчі-криміналісти, спеціалісти, працівники кіберполіції, оперативних та оперативно-технічних підрозділів, експерти) і колективні (слідчо-оперативна група, слідча група, судово-експертні установи, група експертів).

3. Перспективними напрямками використання зарубіжного досвіду боротьби з кіберзлочинами у вітчизняній науці та практиці розслідування злочинів є: удосконалення правового регулювання протидії кіберзлочинам; залучення цивільних фахівців у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку до

вирішення завдань техніко-криміналістичного забезпечення розслідування кіберзлочинів (досвід Німеччини); запровадження інституту консультантів, які вивчають обставини конкретного кримінального провадження, аналізують наявну доказову базу і надають рекомендації слідчим щодо доцільності дослідження конкретних речових доказів, визначення виду експертиз та послідовності їх призначення (досвід Великої Британії); налагодження взаємодії правоохоронних та інших державних інституцій у сфері протидії кіберзлочинності (досвід Франції); залучення міжнародної технічної допомоги (зокрема, для проведення транскордонного обшуку в комп'ютерних мережах), пов'язаної з техніко-криміналістичним забезпеченням протидії кіберзлочинам в Україні. Також перспективним і доцільним є запровадження в діяльність судово-експертних установ України «Глобальних керівних принципів лабораторій цифрової криміналістики», підготовлених й опублікованих Інтерполом (INTERPOL Global guidelines for digital forensics laboratories), які схвалені та рекомендовані до впровадження Європейською мережею криміналістичних установ (European Network of Forensic Science Institutes).

4. Техніко-криміналістичні засоби розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку – це система спеціально виготовлених або пристосованих приладів, пристроїв, засобів вимірювальної техніки, допоміжного обладнання, інструментів, матеріалів, інформаційних пошукових, ідентифікаційних та інших систем, криміналістичних технологій їх застосування з метою виявлення, фіксації, вилучення, дослідження, обліку, аналізу та оцінки електронних/віртуальних слідів злочину та інших речових доказів, а також здійснення інших дій з виявлення, розслідування та попередження злочинів. Видами цих техніко-криміналістичних засобів є апаратні та програмні засоби мобільної криміналістики; апаратні блокіратори запису; програмні засоби копіювання даних; програмні засоби комп'ютерної експертизи; апаратні засоби відновлення даних; відкрите спеціалізоване програмне забезпечення; дистрибутиви на основі Linux.

5. Оскільки відображенням об'єктивної сторони складу злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є поряд з «традиційними» й інформаційні сліди, важливим аспектом проведення слідчих (розшукових) дій є те, що інформація або доступ до неї можуть бути втрачені після відключення електронного пристрою (енергозалежні дані, спеціальні програми для знищення даних тощо) або ж зберігатися на серверах чи пристроях, що розташовані в іншому місці, у тому числі поза межами проведення слідчої (розшукової) дії та навіть поза межами України (використання зовнішніх пристроїв збереження даних, хмарних сховищ тощо). У зв'язку з цим, існує потреба в проведенні кваліфікованого виявлення, фіксації та вилучення такої інформації або ж її носіїв, ужитті заходів щодо недопущення стороннього (зовнішнього) впливу на електронні сліди злочину (наприклад, відключення електроенергії, віддаленого доступу до файлів та керування системою тощо), готовності органів розслідування оперативно

проводити слідчі (розшукові) дії в інших місцях, де може зберігатися цифрова інформація.

Особливістю розслідування злочинів даної категорії є обов'язкове залучення як спеціаліста фахівця (фахівців) у галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку й використання ним, за необхідності, спеціальних техніко-криміналістичних засобів, що загалом обумовлено специфікою виявлення, фіксації та вилучення електронних слідів злочину (опис у протоколі процесуальної дії, фото-, відеофіксація, копіювання на зовнішній носій інформації), а також у деяких випадках прямим згадуванням на це у КПК України (ч. 2 ст. 168). Залежно від конкретної ситуації, це може бути як судовий експерт за напрямом комп'ютерно-технічної та (або) телекомунікаційної експертизи, так й інші особи, які володіють відповідними спеціальними знаннями та навичками використання техніко-криміналістичних засобів, наприклад, фахівець з експлуатації або створення конкретних програмних засобів або ж з технічної експлуатації і ремонту певного обладнання. Така участь працівників Експертної служби МВС України має бути нормативно врегульована на відомчому рівні (наказ МВС України від 03 листопада 2015 р. № 1339) з обов'язковим залученням комп'ютерно-технічної лабораторії у складі спеціалізованої пересувної лабораторії та спеціалістів відповідного профілю до участі у проведенні оглядів місць подій. За необхідності залучення фахівців недержавних підприємств, установ та організацій таке залучення має бути заздалегідь узгоджено та організовано. У зв'язку із зазначеним, важливим елементом у проведенні слідчих (розшукових) дій є їх підготовчий етап, який дозволяє забезпечити участь потрібного фахівця та наявність необхідних технічних засобів.

6. Важливою передумовою залучення спеціаліста до проведення негласних слідчих (розшукових) дій під час розслідування злочинів даної категорії правопорушень у випадку, якщо інформація, яка буде досліджуватись, належить до державної таємниці, є наявність у нього допуску до державної таємниці відповідної форми. До того ж, з метою захисту інформації, отриманої в результаті проведення негласних слідчих (розшукових) дій, запропоновано доповнити ст. 254 КПК України положенням такого змісту: «У випадку залучення спеціаліста у протоколі негласної слідчої (розшукової) дії зазначається, що йому роз'яснено його зобов'язання, передбачені ч. 5 ст. 77 КПК України, зокрема щодо нерозголошення відомостей, які стали відомі спеціалісту у зв'язку з виконанням його обов'язків».

Щодо техніко-криміналістичних засобів, які застосовуються при проведенні негласної слідчої (розшукової) дії, потребує уточнення ч. 2 ст. 266 КПК України, у якій має бути передбачено: «Первинні носії інформації (за можливості від'єднання такого носія від технічного пристрою) долучаються до протоколу негласної слідчої (розшукової) дії. У всіх інших випадках з отриманої інформації знімається копія, яка долучається до протоколу, з фіксуванням у ньому хеш-суми скопійованих файлів. Відповідно, первинні носії інформації й технічні засоби її отримання повинні зберігатися до набрання законної сили вироком суду з

позначенням місця зберігання, відповідальної особи та її попередженням про це в протоколі негласної слідчої (розшукової) дії».

7. У зв'язку з тим, що залежно від конкретної ситуації розслідування може існувати потреба в значній кількості експертних досліджень за різними експертними спеціальностями (видами та підвидами судових експертиз), які мають свої особливості, до того ж проводяться інколи різними експертними установами чи підрозділами та в достатньо тривалі терміни, особливого значення набуває послідовність їх призначення, правильність визначення суб'єкта їх проведення, а також підготовки матеріалів. З цією метою важливими є як знання та досвід самого слідчого, який набувається у процесі початкового навчання, підвищення кваліфікації, службової підготовки, самоосвіти та практичної роботи, так і консультативно-довідкове супроводження розслідування особами, які володіють спеціальними знаннями (слідчі-криміналісти, інспектори-криміналісти, співробітники кіберполіції, судові експерти за напрямками тощо).

8. Для усунення недоліків (помилки), пов'язаних з проведенням слідчих (розшукових) дій під час розслідування злочинів даної категорії і призначенням експертизи комп'ютерної техніки та програмних продуктів, які ускладнюють або унеможливають проведення такої експертизи, потрібні комплексні заходи, що передбачають: 1) постійне підвищення кваліфікації осіб, які здійснюють досудове розслідування злочинів; 2) за можливості до призначення експертизи проведення огляду об'єктів із залученням фахівця в галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, що дасть змогу встановити наявність даних, які можуть мати доказове значення у кримінальному провадженні та загалом вирішити питання щодо доцільності подальшого призначення експертизи; 3) узгодження переліку питань за конкретними об'єктами з фахівцями в галузі використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, оптимізацію кількості таких питань та об'єктів, які надаються на експертизу; 4) збільшення кількості наукових розробок та, відповідно, кількості науково-практичних і методичних видань за вказаною проблематикою; 5) нормативно-правове закріплення різновидів судових експертиз, які проводить Експертна служба МВС України, визначення питань, які вони можуть вирішити, а також вимог до наданих на експертизу матеріалів; 6) розроблення окремого порядку залучення вузькопрофільних спеціалістів (судових експертів) до виконання традиційних експертиз, які безпосередньо не пов'язані з дослідженнями комп'ютерної техніки, але в процесі їх проведення виникає потреба в дослідженні цифрових носіїв інформації та (або) інформаційних слідів на віддалених пристроях збереження даних, серверах, хмарних сховищах тощо.

9. Оскільки на етапі досудового розслідування обов'язок щодо оцінки зібраних доказів, у тому числі висновків судових експертів, та вирішення питання їх достатності для завершення розслідування покладається насамперед на слідчих та детективів, то для розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, враховуючи існуючу їх специфіку, має бути запроваджено

відповідну спеціалізацію слідчих Національної поліції України, а також у вимогах до цих посад крім юридичної слід передбачити необхідність професійно-технічної або вищої технічної освіти принаймні початкового рівня (короткого циклу) за відповідним напрямом.

Використання висновків судових експертиз як джерела доказів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можливо за такими напрямками: 1) забезпечення потреб розслідування кримінально-правової кваліфікації злочину, висунення версій та їх перевірки, планування й організації розслідування загалом та окремих слідчих (розшукових) дій, з'ясування фактів (обставин) кримінального правопорушення, збирання та перевірки доказів, обґрунтування процесуальних дій, рішень; 2) забезпечення експертної профілактики кіберзлочинності, попередження слідчих та експертних помилок призначення і проведення експертизи комп'ютерної техніки та програмних продуктів й інших судових експертиз.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Теплицький Б. Б. Завдання, об'єкти й питання комп'ютерно-технічної судової експертизи. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 3 (108). С. 303–315.

2. Теплицький Б. Б. Використання зарубіжного досвіду техніко-криміналістичного забезпечення розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *KELM*. 2020. № 3-3. С. 112–116. (Республіка Польща).

3. Теплицький Б. Б. Застосування техніко-криміналістичних засобів при проведенні обшуку під час розслідування злочинів у сфері використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука*. 2020. № 5. С. 143–148.

4. Теплицький Б. Б. Особливості застосування техніко-криміналістичних засобів при проведенні окремих слідчих (розшукових) дій під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Юридична наука*. 2020. № 6. С. 177–183.

5. Теплицький Б. Б. Сучасні можливості судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Юридичний часопис Національної академії внутрішніх справ*. 2021. № 1 (21). С. 30–37.

6. Теплицький Б. Б. Актуальні питання призначення експертизи комп'ютерної техніки і програмних продуктів під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2021. № 3 (120). С. 28–34.

7. Теплицький Б. Б. Щодо завдань комп'ютерно-технічних експертиз при розслідуванні незаконного зайняття гральним бізнесом в Україні. *Судова*

експертиза: сучасність та майбутнє: матеріали круглого столу (м. Львів, 25 січ. 2018 р.); за заг. ред. д-ра тех. М. О. Кузіна / Львів. наук.-дослід. ін-т судових експертиз М-ва юстиції України. Львів, 2019. С. 127–129.

8. Теплицький Б. Б. Практичні проблемні питання призначення комп'ютерно-технічної судової експертизи в кримінальних провадженнях. *Актуальні проблеми криміналістики та судової експертології*: матеріали міжвідом. наук.-практ. конф. (м. Київ, 22 листоп. 2018 р.) / [редкол.: В. В. Черней, С. Д. Гусарев, С. С. Чернявський та ін.]. Київ: Нац. акад. внутр. справ, 2018. С. 406–409.

9. Теплицький Б. Б. Особливості оцінки результатів судових експертиз під час розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. *Використання досягнень сучасної науки й техніки в розкритті злочинів* : матеріали міжвідом. наук.-практ. круглого столу (Київ, 25 лют. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 223–225.

10. Теплицький Б. Б. Особливості суб'єктної складової техніко-криміналістичного забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку. *Кримінальне судочинство: сучасний стан та перспективи розвитку*: матеріали Всеукр. наук.-практ. конф. (Київ, 28 трав. 2021 р.). Київ : Нац. акад. внутр. справ, 2021. С. 384–387.

11. Теплицький Б. Б. Щодо визначення терміну «техніко-криміналістичне забезпечення розслідування кримінальних правопорушень». *Актуальні питання вдосконалення судово-експертної та правоохоронної діяльності*: зб. матеріалів засідання № 1 постійно діючої Міжнар. наук.-практ. конф. (м. Кропивницький, 24 верес. 2021 р.). Кропивницький: ТОВ «Центрально-Українське видавництво», 2021. С. 71–74.

12. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: спеціальні питання кваліфікації, проведення слідчих (розшукових) дій, призначення комп'ютерно-технічних судових експертиз: наук.-практ. посіб. / Б. Б. Теплицький, Л. Г. Шарай, К. М. Ковальов, С. А. Кузьмін. Київ: ПАЛИВОДА А.В., 2019. 168 с.

АНОТАЦІЯ

Теплицький Б. Б. Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. – Рукопис.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність» (081 – Право). – Національна академія внутрішніх справ, Київ, 2021.

У дисертації з'ясовано стан наукового розроблення проблем техніко-криміналістичного забезпечення розслідування злочинів у сфері використання

електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Визначено найкращий зарубіжний досвід техніко-криміналістичного забезпечення розслідування злочинів даного напрямку, який можливо впроваджувати у вітчизняну науку та практику.

Розкрито особливості техніко-криміналістичного забезпечення проведення окремих слідчих (розшукових) дій, зокрема негласних, у зазначеній категорії кримінальних проваджень, надано пропозиції з удосконалення такого забезпечення. Виявлено типові помилки при призначенні експертизи комп'ютерної техніки і програмних продуктів, запропоновано шляхи попередження таких помилок.

Ключові слова: кіберзлочинність, злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, техніко-криміналістичне забезпечення, техніко-криміналістичні засоби, експертиза комп'ютерної техніки і програмних продуктів, експертиза телекомунікаційних систем і засобів.

АННОТАЦІЯ

Теплицкий Б. Б. Техничко-криминалистическое обеспечение расследования преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. – Рукопись.

Диссертация на соискание ученой степени кандидата юридических наук по специальности 12.00.09 «Уголовный процесс и криминалистика; судебная экспертиза; оперативно-розыскная деятельность» (081 – Право). – Национальная академия внутренних дел, Киев, 2021.

В диссертации определено состояние научной разработки проблем технико-криминалистического обеспечения расследования преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи. Сделан вывод, что отдельного комплексного исследования технико-криминалистического обеспечения расследования преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и сетей и сетей электросвязи не проводилось.

На основе анализа существующих определений технико-криминалистического обеспечения расследования преступлений в целом и содержания такого обеспечения при расследовании преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи сформулировано понятие такого обеспечения. Охарактеризованы субъекты технико-криминалистического обеспечения расследования преступлений данной категории. Определен лучший зарубежный опыт технико-криминалистического обеспечения расследования преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, который можно внедрять в отечественную науку и практику.

Предложены понятие и классификация технико-криминалистических средств, применяемых при досудебном расследовании преступлений данной категории. Раскрыты особенности технико-криминалистического обеспечения проведения отдельных следственных (розыскных) действий, в том числе негласных, в указанной категории уголовных производств, даны предложения по усовершенствованию такого обеспечения.

Раскрыты особенности назначения наиболее типичных видов судебных экспертиз при расследовании преступлений в данной сфере. Выявлены типичные ошибки при назначении экспертизы компьютерной техники и программных продуктов как наиболее распространенной разновидности судебных экспертиз по преступлениям данной категории, предложены пути недопущения таких ошибок. Определены особенности оценки результатов судебных экспертиз и направления их использования при расследовании преступлений в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи.

Ключевые слова: киберпреступность, преступления в сфере использования электронно-вычислительных машин (компьютеров), систем и компьютерных сетей и сетей электросвязи, технико-криминалистическое обеспечение, технико-криминалистические средства, экспертиза компьютерной техники и программных продуктов, экспертиза телекоммуникационных систем и средств.

SUMMARY

Teplytsky B.B. Technical and forensic support for the investigation of crimes in the sphere of electronic computer systems, computer and telecommunications networks usage. – *Manuscript.*

The dissertation on competition of a scientific degree of The Candidate of Legal Sciences on a specialty 12.00.09 «Criminal process and criminology; forensic examination; operational and investigative activities» (081 – Law). – National Academy of Internal Affairs, Kyiv, 2021.

The dissertation clarifies the state of scientific development of problems of technical and forensic support of crime investigations in the field of use of computers, systems and computer networks and telecommunication networks. The best foreign experience of technical and forensic support of crime investigation in this area, which can be implemented in domestic science and practice, has been identified.

The peculiarities of technical and forensic support of certain investigative (search) actions, in particular covert, in this category of criminal proceedings are revealed, proposals for improving such support are given. Typical errors in the examination of computer hardware and software products have been identified, and ways to prevent such errors have been suggested.

Key words: cybercrime, crimes in the field of electronic computer systems, computer and telecommunications networks usage, forensic software, forensic tools, examination of computer equipment and software, examination of telecommunication systems and means.