МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ХАРКІВСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ВНУТРІШНІХ СПРАВ

ДОВЖЕНКО ОЛЕКСІЙ ЮРІЙОВИЧ

УДК 343.985:(343.222.4:004)(477)(043.3)

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ КІБЕРЗЛОЧИНІВ

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

Автореферат дисертації на здобуття наукового ступеня
кандидата юридичних наук

Харків - 2020

Дисертацією є рукопис.

Науковий керівник: доктор юридичних наук, доцент
Дрозд Валентина Георгіївна,
Державний науково-дослідний інститут
МВС України
начальник 3-го науково-дослідного відділу
науково-дослідної лабораторії
з проблем правового та
організаційного забезпечення
діяльності Міністерства

Офіційні опоненти: доктор юридичних наук, професор
Чаплинський Костянтин Олександрович,
Дніпропетровський державний
університету внутрішніх справ,
завідувач кафедри криміналістики,
судової медицини та психіатрії

кандидат юридичних наук, доцент
Абламський Сергій Євгенович,
Харківський національний університет
внутрішніх справ, доцент кафедри
кримінального процесу та організації
досудового слідства факультету № 1

Захист відбудеться 24 грудня 2020 р. о 13 годині на засіданні спеціалізованої вченої ради Д 64.700.01 у Харківському національному університеті внутрішніх справ за адресою: 61080, м. Харків, просп. Льва Ландау, 27.

З дисертацією можна ознайомитися в бібліотеці Харківського національного університету внутрішніх справ за адресою: 61080, м. Харків, просп. Льва Ландау, 27.

Автореферат розісланий 20 листопада 2020 року.

Вчений секретар
спеціалізованої вченої ради **Л. В. Могілевський**

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Основним напрямком розвитку сучасного світу є зростання кількості та значущості комп'ютерних технологій. Відбувається нова науково-технічна революція, внаслідок якої електронні пристрої та електронні мережі стають невід'ємною частиною будь-якої людської діяльності. Більша частина людства вже представлена в глобальній комп'ютерній мережі, охоплення якої безперервно зростає. Очевидно, що протягом найближчих десятиліть, якщо не років, практично все людство буде об'єднано глобальною системою електронних комунікацій. Відбувається становлення нової реальності, і цій реальності притаманні всі явища, що вже існують в реальності матеріальній. Не є виключенням і злочинна діяльність.

Згідно із підрахунками Управління ООН з наркотиків та злочинності, щорічно в світі фіксуються понад три мільярди спроб незаконного доступу до електронних поштових скриньок та понад п'ять мільярдів вірусних атак. Близько третини компаній в світі зазнають щорічно цілеспрямованих кібератак проти їхніх активів та інфраструктури. До 2021 року очікується зростання шкоди від кібератак та витрат на захист від них до шести трильйонів доларів щорічно. Україна не є виключенням з цієї тенденції, про свідчить зростання кількості зафіксованих кіберзлочинів щороку на дві з половиною тисячі.

Можна констатувати, що злочинна діяльність, так саме як і все людське життя, стають все більш «діджиталізованими». За таких умов, розробка нових підходів до боротьби з кіберзлочинністю є однією з найбільш гострих завдань кримінально-правової та криміналістичної науки. Мова йде не просто про нову групу злочинів, а про новий та такий, що швидко розвивається, тип злочинної поведінки – кіберзлочинність. Особливої складності цій проблемі додає інтернаціоналізований характер злочинних посягань, скоєних за допомогою електронних пристроїв та мережі Інтернет. Ефективна боротьба з кіберзлочинністю силами лише однієї країни неможлива. Потрібна спільна діяльність кримінальних відомств всіх країн, з використанням єдиної методології розслідування кіберзлочинів, що забезпечувала б засудження кіберзлочинців незалежно від національних кордонів.

Необхідно констатувати, що чинний Кримінальний процесуальний кодекс України 2012 року (далі: КПК України) недостатньо регулює питання організації розслідування кіберзлочинів. Було зроблено ряд спроб винести зміни до КПК України, зокрема щодо застосування окремих видів забезпечення кримінального провадження при розслідуванні кіберзлочинів. Водночас, при існуючому характері правового регулювання, слідство щодо кіберзлочинів залишається обмеженим традиційними слідчими методиками, які не завжди застосовні до нового типу правопорушень. Цим зумовлюється актуальність обраної теми дослідження.

Кіберзлочинність є об'єктом пильної уваги дослідників та розглядалася ними з різних точок зору. Основою будь-якого криміналістичного дослідження є роботи провідних науковців, таких як Р. С. Бєлкін, В. К. Весельський,

А. І. Вінберг, Л. Я. Драпкін, А. Ф. Зелінський, Д. О. Крилов, В. М. Куц, С. М. Потапов, М. В. Салтевський, В. В. Тіщенко, В. В. Топчій.

Проблематика боротьби з кіберзлочинністю як особливим видом злочинності досліджується в працях Д. С. Азарова, П. Д. Біленчука, С. В. Бренера, В. М. Бутузова, В. П. Верченка, В. Б. Вехова, А. Г. Волеводза, С. Ю. Гаврилюка, В. Д. Гавловського, О. В. Гайдука, В. С. Герасимюка, В. О. Голубєва, К. В. Грюліха, Б. В. Дзюндзюка, І. В. Європіної, А. І. Журби, О. Ю. Іванченка, М. В. Карчевського, В. А. Коршенка, М. О. Кравцова, Б. Д. Леонова, А. В. Микитчика, О. І. Мотляха, Г. В. Муляра, В. А. Поливанюка, Б. В. Романюка, Р. В. Сабадаша, Н. А. Савінової, Т. І. Савчук, В. С. Серьогіна, З. М. Топорецької, О. С. Ховцуна, Є. С. Хижняка, В. С. Цимбалюка, О. В. Шведової, Є. В. Шевченка, В. П. Шеломенцева, А. І. Щура, М. М. Федотова, К. В. Юртаєвої.

На особливу увагу заслуговують монографічні дослідження О. І. Мотляха «Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій (Київ, 2005), Н. І. Козак «Криміналістичні прийоми, способі і засоби виявлення, розкриття та розслідування комп'ютерних злочинів» (Ірпінь, 2011), С. М. Павлюка «Інформаційні правопорушення» (Київ, 2015), С. А. Буяджи «Правове регулювання боротьби з кіберзлочинністю: теоретико-правовий аспект» (Київ, 2018), Ю. М. Піцика «Кіберзлочини проти власності: кримінально-правова та кримінологічна характеристика», І. В. Діордіци «Адміністративно-правове регулювання кібербезпеки в Україні» (Запоріжжя, 2018), Д. О. Ричка «Особливості кримінально-правової кваліфікації злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (Ірпінь, 2019).

Водночас, всі наведені роботи або виконані до 2012 року, тобто до набрання чинності новим КПК України, або стосуються окремих вузьких питань, або виконані з дисциплін, суміжних з кримінальним процесом та криміналістикою, таких як кримінальне право та кримінологія. Таким чином, наразі комплексні монографічні дослідження кримінально-процесуальних та криміналістичних аспектів протидії кіберзлочинності наразі відсутні.

Така ситуація негативно впливає на законодавчу та правозахисну практику, що і зумовило обрання теми дисертаційного дослідження та підтверджує її обґрунтованість та актуальність.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація спрямована на реалізацію положень Закону України від 11.07.2001 р. № 2623-III (у редакції від 12.10.2010 р.) «Про пріоритетні напрями розвитку науки і техніки» та Плану заходів Міністерства внутрішніх справ, спрямованих на реалізацію норм КПК України, затвердженого наказом МВС України від 08.08.2012 № 685. Тема відповідає положенням додатку 10 Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років, затвердженого наказом МВС України від 16.03.2015 № 275, теми наукових досліджень кафедри кримінального процесу «Актуальні проблеми досудового розслідування»

(державний реєстраційний номер 0114U004018), яка є складовою частиною наукового дослідження Одеського державного університету внутрішніх справ – «Пріоритетні напрямки розвитку та реформування ОВС в умовах розгортання демократичних процесів у державі» (державний реєстраційний номер 0114U004015).

Мета і завдання дослідження. *Метою* дисертації є комплексний науковий аналіз проблем, пов'язаних з методикою розслідування кіберзлочинів, тобто сукупністю методів, способів та прийомів такого розслідування, а також формулювання на його основі науково-обґрунтованих практичних і методологічних рекомендацій щодо вдосконалення чинного процесуального законодавства і практики його застосування.

Ця мета конкретизується такими *завданнями*:

– визначити стан наукової розробки проблем розслідування кіберзлочинів;

– встановити основні підходи до класифікації кіберзлочинів та запропонувати на їх основі інтегрований підхід;

– надати криміналістичну характеристику кіберзлочинів як особливого типу злочинів;

– визначити перелік обставин, що підлягають встановленню при розслідуванні кіберзлочинів;

– охарактеризувати типові слідчі ситуації, що виникають при розслідуванні кіберзлочинів;

– виявити особливості наступного етапу при розслідуванні кіберзлочинів;

– встановити особливості огляду місця події як слідчої дії в рамках розслідування кіберзлочинів;

– розглянути особливості допиту потерпілих, свідків, підозрюваних і обвинувачуваних у справах про кіберзлочини;

– виявити особливості отримування доказів та проведення експертиз у справах про кіберзлочини.

Об'єкт дослідження – суспільні відносини, що виникають у зв'язку з розслідуванням кіберзлочинів в рамках кримінального провадження.

Предмет дослідження – основи методики розслідування кіберзлочинів.

Методи дослідження. Методологічну основу дисертації складає система загальнонаукових та спеціальних методів пізнання правових явищ. Зокрема, діалектичний метод пізнання дав можливість розглянути поставлені проблеми в динаміці та взаємозв'язку (підрозділи 1.1, 1.3, 2.1, 2.2, 2.3). Історичний метод використано для аналізу становлення і розвитку явища кіберзлочинів, а також еволюції методологічних підходів до боротьби з такими злочинами (підрозділи 1.1, 1.2, 2.1). Структурно-функціональний метод дозволив виділити кіберзлочини як особливу категорію злочинності, дослідити наявні класифікації кіберзлочинів та запропонувати на їхній підставі інтегровану класифікацію (підрозділи 1.2, 1.3). Системно-структурний метод застосовано для розмежування окремих понять та категорій в методиці розслідування кіберзлочинів (підрозділи 2.2, 2.3, 3.1, 3.2, 3.3). Формально-логічний метод застосовувався в роботі з метою встановлення змісту норм чинного КПК

України, обґрунтування пропозицій щодо внесення до них змін (підрозділи 2.2, 2.3, 3.3). Статистичний метод використано з метою узагальнення даних щодо динаміки кіберзлочинності та розширення сфери її охоплення (підрозділи 1.1, 1.2, 3.1, 3.2, 3.3).

Емпіричну базу дослідження склали статистичні данні, отримані за інформацією Управління ООН з наркотиків та злочинності та інших міжнародних та національних організацій, судова практика, зокрема практика Європейського суду з прав людини.

Наукова новизна отриманих результатів полягає в тому, що одним з перших після набрання чинності новим КПК України в 2012 році було проведено комплексне монографічне дослідження теоретичних і практичних засад методики розслідування кіберзлочинів. Це дозволило автору за результатами дослідження сформулювати низку наукових положень, висновків і пропозицій, а саме:

уперше:

– надано визначення поняття кіберзлочину як особливої форми протиправної поведінки, що, що посягає на охоронювані кримінальним законом суспільні інтереси, та скоюється у кіберпросторі або з використанням можливостей кіберпростору;

– запропоновано класифікацію кіберзлочинів, що ґрунтується на методі ґрупофікації та полягає в поєднання класифікацій, які засновані на особливій природі кіберзлочинів та чинного підходу КПК України, що полягає в класифікації в залежності від предмету та об'єкту злочину;

– розкрито особливості методології проведення кіберзлочинів, зокрема розслідування на початковому наступному етапі, а також охарактеризовано типові слідчі ситуації, що дозволяють переходити від початкового до наступного етапу розслідування кіберзлочину;

удосконалено:

– окремі теоретичні положення щодо методології слідчих дій на початковому етапі розслідування кіберзлочинів з урахуванням вимог статей 246 та 258 КПК України так, аби забезпечити відповідність цих слідчих дій вимогам щодо захисту приватного життя осіб;

– концептуальні напрацювання щодо кіберпростору як особливого простору, що створюється за допомогою комп'ютерної техніки та комп'ютерних мереж, який є середовищем, в якому або за допомогою якого здійснюються кіберзлочини, а також відбувається спілкування кіберзлочинців;

дістали подальшого розвитку:

– теоретичний доробок щодо методології дій слідчого в різних слідчих ситуаціях при розслідуванні кіберзлочину, зокрема ситуацій, пов'язаних з наявністю або відсутністю зізнання підозрюваного/ підозрюваних у вчиненні злочину;

– положення щодо інформаційного забезпечення слідчих дій при розслідуванні кіберзлочинів, а саме щодо інформаційного забезпечення допиту підозрюваних, свідків та потерпілих;

– пропозиції щодо удосконалення статей 240–245 КПК України з метою покращення законодавчого забезпечення організації слідчих дій при розслідуванні кіберзлочинів.

Практичне значення отриманих результатів полягає в тому, що викладені в дисертації висновки і пропозиції можуть бути використані:

– *у навчальному процесі* – під час підготовки посібників із навчальних курсів кримінального процесу і криміналістики, а також розроблення текстів лекцій та навчально-методичних матеріалів для проведення семінарів і практичних занять;

– *у практичній діяльності* – сформульовані дисертантом пропозиції щодо методики розслідування кіберзлочинів під час провадження слідчих дій використовують слідчі ГУ НП України в Одеській області;

– *у науково-дослідній роботі* – як основа для подальшого дослідження проблеми організації розслідування кіберзлочинів в Україні;

– *у сфері правотворчості* – для удосконалення чинного кримінального процесуального законодавства України.

Апробація матеріалів дисертації. Основні теоретичні положення, що містяться в дисертації, були оприлюднені на Міжнародній юридичній науково-практичній Інтернет-конференції «Модернізація законодавства та правозастосування: вимоги часу» (м. Київ, 6 грудня 2018 р.); Міжнародній науковій конференції «Конгрес міжнародного та європейського права» (м. Одеса, 25–26 травня 2018 р.); VI Всеукраїнській науково-практичній конференції «Сучасні тенденції соціально-гуманітарного розвитку України та світу» (м. Харків, 27 вересня 2019 р.); Міжнародній науково-практичній конференції «Кримінальне правопорушення: національний та зарубіжний виміри» (м. Одеса, 24 травня 2019 р.); Міжнародній науково-практичній конференції «Міжнародне та національне законодавство: способи удосконалення» (м. Дніпро, 29–30 березня 2019 р.); Міжнародній науково-практичній конференції «Пріоритетні напрями розвитку сучасної юридичної науки» (м. Харків, 20–21 вересня 2019 р.).

Публікації. Основні положення дисертації відображено у 12 публікаціях, у тому числі у 6 статтях, опублікованих у виданнях, включених до переліку наукових фахових видань з юридичних наук, 1 – у зарубіжному періодичному виданні, та 6 тезах доповідей на наукових та науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з вступу, трьох розділів, що включають дев’ять підрозділів, висновків, списку використаних джерел, додатків. Загальний обсяг дослідження становить 200 сторінки, із яких 171 – основного тексту. Список використаних джерел складається із 260 найменувань на 29 сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **Вступі** обґрунтовується вибір теми дослідження, розкривається ступінь наукової розробленості проблеми, визначаються мета і завдання дослідження відповідно до предмета та об’єкта дослідження, методи дослідження,

аргументуються наукова новизна, наводиться інформація про апробацію матеріалів дисертації, публікації, висвітлюється структура та обсяг дисертації, вказується на зв'язок роботи з науковими програмами, планами, темами, грантами, наводиться практичне значення отриманих результатів.

Перший розділ «Науково-методологічні засади розслідування кіберзлочинів» складається з трьох підрозділів і присвячений розгляду стану наукової розробленості проблеми, історичних аспектів виникнення та розвитку та класифікації кіберзлочинів.

У *підрозділі 1.1. «Стан наукової розробки проблем розслідування кіберзлочинів»* досліджується історія виникнення та дослідження кіберзлочинів, розглядаються доктринальні підходи до проблеми кіберзлочинів та боротьби з ними та наявні класифікації кіберзлочинів. Визначено історію дослідження поняття кіберзлочинів та встановлено, що злочинна діяльність з використанням електронних обчислювальних пристроїв виникла як самостійне явище з появою електронних комп'ютерних мереж в 1980-х роках. Наголошується, що протягом тривалого часу злочини, які були скоєні за допомогою електронних обчислювальних пристроїв, не усвідомлювалися в якості окремої самостійної кримінально-правової категорії. Вони розглядалися як одна з форм звичайних злочинів, таких, як злочини проти власності чи проти комерційної таємниці. Лише виникнення розвинутих комп'ютерних мереж, а разом з ними й поява можливостей зі злочинного впливу через ці мережі, який міг би призводити до масштабних згубних наслідків, призвів до усвідомлення необхідності виділення комп'ютерних злочинів в особливу групу. В цей період починається усвідомлення проблеми кіберзлочинів в науковій думці, а також з'являються перші правові норми національного та міжнародного права, що врегулювали питання боротьби з комп'ютерною злочинністю. Виникає саме поняття «кіберзлочин». Розглядається історія дослідження явища кіберзлочинів в українській та іноземній доктрині. Приділяється увага формуванню правового регулювання законодавства щодо боротьби з кіберзлочинністю в Україні.

У *підрозділі 1.2. «Криміналістична характеристика кіберзлочинів»* зазначено, що в праві та доктрині найбільшого визнання серед багатьох альтернативних термінів набув термін «кіберзлочин», проте визначення поняття кіберзлочину досі відсутнє. На підставі аналізу літератури визначається, що кіберзлочин доцільно характеризувати через категорію кіберпростору. Визначається, що на заваді дослідженню та класифікації кіберзлочинів, та врешті створенню єдиного визначення кіберзлочинів в кримінальному праві стає недостатня концептуальна розробленість самого поняття кіберзлочину та розмитість «кордонів» між кіберзлочинами та рештою злочинних посягань. Шлях до розв'язання цієї проблеми вбачається в використанні концепції кіберпростору як особливої реальності, що створюється електронними технологіями та за допомогою комп'ютерних мереж. Це нематеріальний простір, що виникає на базі матеріальних об'єктів, таких як електронне обладнання, однак сам не є цими об'єктами, а є цифровим відображенням впливів, що здійснюються за допомогою предметів матеріального світу. Кіберпростір набуває все більше значення для людства,

оскільки він відкриває нові можливості, тому слід очікувати його подальшого розширення. Кіберзлочин відрізняється від звичайного злочину тим, що існує в кібернетичному світі. За допомогою кіберпростору можливі практично будь-які види злочинного впливу, що можуть бути охарактеризовані в категоріях звичайного злочину, аж до нанесення тілесних ушкоджень чи вбивства. Саме використання віртуального простору кіберсвіту відділяє кіберзлочини від подібних ним злочинів, що відбуваються в матеріальному просторі.

У *підрозділі 1.3. «Криміналістична класифікація кіберзлочинів»* автором, на підставі аналізу ряду теоретичних положень, пропонується власна оригінальна класифікація злочинів, що вчиняються у кіберпросторі. Розглядаються та досліджуються встановлені в теоретичній літературі та практиці класифікації кіберзлочинів, зокрема ті, що запропоновані в Конвенції Ради Європи про кіберзлочинність та доктрині. Підкреслюється, що старі доктринальні підходи до класифікації кіберзлочинів є незадовільними в силу їхніх особливостей, оскільки вони охоплюють злочини, що скоюються в реальному, а не в віртуальному світі. Найбільш простою та очевидною класифікацією є та, що використана в Конвенції Ради Європи про кіберзлочини. Ця класифікація спирається на об'єкт злочинного посягання, а її підставами є правовідносини, що страждають внаслідок злочинного посягання. Цей підхід можна назвати кримінально-правовим. Інший підхід, що можна визначити як криміналістичний, проводить класифікацію кіберзлочинів в залежності від способу злочинного посягання. Нарешті, класифікацію в залежності від особистості злочинця слід позначити як кримінологічну. Встановлюється, що класифікація, яка ґрунтується на аналогії з «звичайними» злочинами є недосконалою та не може використовуватись для подальшої наукової розробки проблематики кіберзлочинності. Показується, що класифікацію кіберзлочинів слід проводити в залежності від характеру злочинного впливу, що відбувається в кіберпросторі.

Другий розділ «Організація розслідування кіберзлочинів» складається з трьох підрозділів, у яких висвітлюються основні положення методології розслідування кіберзлочинів на початковому та наступному етапі їхнього розслідування.

У *підрозділі 2.1. «Обставини, що підлягають встановленню при розслідуванні кіберзлочинів»*, показується, що розслідування кіберзлочинів повинно відбуватися на основі наявних норм процесуального права. Встановлюється, що кримінальне провадження у справах про кіберзлочини спирається на загальні норми КПК України щодо кримінальних проваджень. Зокрема, мова йде про статтю 91 КПК України, якою визначаються обставини, що підлягають доказуванню в кримінальному провадженні. Водночас, при розслідуванні кіберзлочинів слід брати до уваги їхній «ідеальний» характер, що зумовлює особливості проведення слідчих дій. Так, такі слідчі дії як огляд місця події можуть втрачати сенс через відсутність цього місця в реальності. Вирішального значення набувають прийоми, способи та техніки роботи з інформацією та проведення відповідних слідчих дій з метою виявлення цієї інформації, яка дозволяє встановити характер злочинного діяння у

кіберпросторі. Водночас, доводиться, що при розслідуванні кіберзлочинів слід брати до уваги їхній віртуальний характер, що зумовлює вирішальну роль у розслідуванні прийомів, способів та технік роботи з інформацією та проведення відповідних слідчих дій з метою виявлення цієї інформації, що дозволяю встановити характер злочинного діяння у кіберпросторі. Робиться висновок, що розслідування кіберзлочину переважно повинно бути спрямоване на виявлення подій в кіберпросторі, що призвели до настання злочинного результату в реальному світі.

Підрозділ 2.2. «Типові слідчі ситуації на початковому етапі розслідування кіберзлочинів», присвячений висвітленню особливостей типових слідчих ситуацій на початковому етапі розслідування кіберзлочинів. Визначається, що типова слідча ситуація на початковому етапі розслідування кіберзлочинів характеризується, зазвичай, як виявлення ознак злочину, що відбувається одразу після його скоєння, або через певний час. Показується, що з урахуванням особливостей кіберзлочину, здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів, уявляється неможливим, через фізичну відсутність злочинця в місці настання злочинного результату та здійснення злочинного впливу на відстані. Єдиною невідкладною слідчою дією, що можна проводити практично в усіх випадках виявлення ознак кіберзлочину, є огляд місця події. Слідчо-оперативні групи, що формуються для здійснення огляду при розслідуванні кіберзлочинів, повинні включати в себе фахівців в галузі комп'ютерної техніки. Окрім огляду, на початковому етапі розслідування доцільно також проведення слідчих дій, спрямованих на встановлення особистості злочинця, або виявлення ознак, що вказували б на особистість злочинця. Доводиться, що здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів неможливе через фізичну відсутність злочинця в місці настання злочинного результату та здійснення злочинного впливу на відстані. Практично єдиною невідкладною слідчою дією, яку доцільно проводити на початковому етапі розслідування кіберзлочинів є огляд.

У *підрозділі 2.3. «Наступний етап розслідування кіберзлочинів»*, розглянуто особливості слідчих дій на наступному етапі розслідування кіберзлочинів. Розглянуто основні версії, що можуть висуватися за результатами початкового етапу розслідування. Показано, що оскільки на даному етапі розслідування, як правило, вже сформоване коло підозрюваних, особливе значення набуває подолання їхньої протидії розслідуванню та викриття повної картини злочину та ролі підозрюваного (підозрюваних) у ньому. Підозрювані в кіберзлочинах, зазвичай, мають такий рівень технічної підготовки, що переважає рівень знань про комп'ютерну техніку слідчого, тому особливого значення набувають експертні висновки, отримані за результатами дослідження виявлених доказів. Використовуючи результати експертних досліджень та інших слідчо-розшукових дій, слідчий може здолати опір підозрюваного та спонукати його до визнання провини, або зібрати достатні докази, що вказують на вину особи, незалежно від визнання вини цією особою, або виявити, що зібраних доказів недостатньо для встановлення вини особи. В

останньому випадку, слідчий вирішує питання про проведення подальших слідчих дій. Проаналізовано та показано особливості тактичних прийомів допиту, обшуку та експертизи в кримінальних провадженнях про кіберзлочини. Доводиться, що на наступному етапі розслідування кіберзлочинів головним завданням слідчого стає подолання протидії слідству з боку підозрюваного. Вирішальне значення для досягнення цієї мети є створення інтелектуальної переваги слідчого над підозрюваним, яка досягається завдяки вмілому використанню інформації, отриманої під час проведення слідчих дій.

Третій розділ «Особливості проведення окремих слідчих дій при розслідуванні кіберзлочинів» складається з трьох підрозділів, в яких досліджуються прикладні аспекти методології окремих слідчих дій при розслідуванні кіберзлочинів.

У *підрозділі 3.1. «Особливості огляду місця події при розслідуванні кіберзлочинів»* демонструється, що особливості тактики слідчих дій при розслідуванні кіберзлочинів зумовлені «віддаленим» характером діяння, що розслідується. Надається характеристика особливостей СРД, які проводяться з урахуванням «віддаленого» характеру розслідуваного діяння. Так, при проведенні огляду слід зосередитися на об'єктах реального світу, що відображують злочинний вплив, такий як підготовка, скоєння та приховання кіберзлочину. Слід мати на увазі, що статичні сліди в реальному світі вказують на динамічну ситуацію кіберсвіту. До проведення огляду місця події кіберзлочину завжди повинен залучатися спеціаліст в галузі комп'ютерних технологій. Йому варто ще до початку огляду поставити питання, на які необхідно звернути увагу та які підлягають встановленню, він має брати участь в здійсненні всіх елементів огляду, а також попередити слідчого при виявленні ознак стороннього впливу під час огляду. Запорукою успішності проведення огляду, виявлення всіх слідів та встановлення динамічної картини злочину, є взаємодія слідчого і спеціаліста. Так, при проведенні огляду слід зосередитися на об'єктах реального світу, що відображують злочинний вплив, такий як підготовка, скоєння та приховання кіберзлочину. Встановлюється, що статичні сліди в реальному світі вказують на динамічну ситуацію кіберсвіту, отже до проведення огляду місця події кіберзлочину завжди повинен залучатися спеціаліст в галузі комп'ютерних технологій. Досліджується приблизний перелік питань, які необхідно ставити експерту при проведенні та які підлягають встановленню при огляді, зокрема щодо виявлення ознак стороннього впливу під час огляду. Демонструється, що завданням огляду виступає встановлення динамічної картини віртуального злочину, яка відображується в слідах, які існують в реальному світі.

У *підрозділі 3.2. «Допит потерпілих, свідків, підозрюваних і обвинувачуваних у справах про кіберзлочини»* підкреслюється особлива роль допиту як слідчої дії при розслідуванні кіберзлочинів. Показується, що на наступному етапі розслідування допит дозволяє визначити стратегію розслідування. З урахуванням технічної складності кіберзлочинів, допит набуває особливого значення, а отже значну увагу слід приділяти підготовці до допиту, в тому числі, шляхом вивчення слідчим спеціальної літератури та

консультації зі спеціалістом. Другим елементом підготовки стає встановлення якомога більш повної інформації конкретної особи, яка підозрюється у скоєнні злочину, або загального психологічного портрету. Поінформованість слідчого дозволяє йому досягнути психологічної переваги над злочинцем, що є запорукою успішності допиту. Розглядаються особливості підготовки та проведення допиту при розслідуванні кіберзлочинів. Наводяться два елементи підготовки до допиту: технічний та особистий. Технічний елемент дозволяє слідчому оволодіти необхідними технічними знаннями, які дають змогу усвідомити картину кіберзлочину. Особистий елемент стосується особистості злочинця, визначення рис його характеру та рівня підготовки, що дозволяє підвищити ефективність визначення кола підозрюваних та проведення їхнього допиту.

У *підрозділі 3.3. «Особливості отримування доказів та проведення експертиз у справах про кіберзлочини»*, доводиться, що при розслідуванні кіберзлочинів саме експертиза є найбільш ефективною для виявлення доказів слідчою дією. В роботі доводиться, що При їхньому розслідуванні, за необхідності, можливе застосування будь-якого виду експертизи, проте найчастіше мова йде про комп'ютерно-технічну експертизу, яка, з точки зору чинного КПК України, є різновидом інженерно-технічної експертизи. Запорукою вдалої експертизи є правильність постановки завдань слідчим. Визначити вичерпні рекомендації щодо таких питань уявляється неможливим, і їхнє формулювання залежить від конкретних обставин справи та рівня технічної підготовки слідчого. Водночас, можна встановити ряд загальних питань, які спрямовані на виявлення основних рис досліджуваних подій. Це питання про можливість скоєння злочину за допомогою конкретного виду комп'ютерної техніки, про використання цієї техніки в момент скоєння злочину, про можливість використання техніки підозрюваним, тощо. Для встановлення динаміки кіберзлочину доцільно скористатися таким прийомом як ситуаційна експертиза. Вона полягає у проведенні безпосередньо на місці події в матеріальному світі співставлення слідів, що виявляють динаміку процесу, який впливав на віртуальний світ. Зібрані експертизою докази щодо події злочину та особистості злочинця надають необхідну інформацію для подальших слідчих дій, зокрема для допитів. Зазначається, що при розслідуванні кіберзлочинів доцільним може виявитись будь-який вид експертизи, проте найчастіше мова йде про комп'ютерно-технічну експертизу, яка, з точки зору чинного КПК України, є різновидом інженерно-технічної експертизи. Запорукою вдалої експертизи є правильність постановки завдань слідчим. Визначити вичерпні рекомендації щодо таких питань уявляється неможливим, і їхнє формулювання залежить від конкретних обставин справи та рівня технічної підготовки слідчого. Водночас, можна встановити ряд загальних питань, які спрямовані на виявлення основних рис досліджуваних подій. Це питання про можливість скоєння злочину за допомогою конкретного виду комп'ютерної техніки, про використання цієї техніки в момент скоєння злочину, про можливість використання техніки підозрюваним, тощо. Досліджуються перспективи використання методу ситуаційної експертизи для

розслідування кіберзлочинів, зокрема в аспекті визначення динаміки кіберзлочину. Вказується, що по своїй суті, ситуаційна експертиза знаходиться на перетині віртуального й реального світу і дозволяє зібрати достатню інформацію для того, аби в подальшому проводити «огляд» в віртуальному світі, тобто експертизу злочинного впливу, що мав місце в комп'ютерній реальності.

ВИСНОВКИ

У дисертації на основі наукових позицій учених, чинного законодавства та практики його застосування здійснено теоретичне узагальнення і вирішення наукового завдання, що полягає в отриманні нових результатів у вигляді наукових висновків, що полягає у визначенні особливостей методики розслідування кіберзлочинів, а також формулюванні на його основі науково-обґрунтованих практичних і методологічних рекомендацій щодо вдосконалення чинного процесуального законодавства і практики його застосування.

1. Як і будь-яка сфера людського існування, комп'ютерні технології відкривають не тільки можливості, але й простір для злочинних посягань. Доведено, що злочини в комп'ютерній сфері (кіберзлочини) виникли практично одночасно з виникненням цих технологій та розвивалися паралельно з ними. З удосконаленням технологій удосконалювалися і способи діяльності злочинців. Разом з тим, протягом тривалого часу злочини, які були скоєні за допомогою електронних обчислювальних пристроїв, не усвідомлювалися в якості окремої самостійної кримінально-правової категорії. Вони розглядалися як одна з форм звичайних злочинів, таких, як злочини проти власності чи проти комерційної таємниці. Лише виникнення розвинутих комп'ютерних мереж, а разом з ними й поява можливостей зі злочинного впливу через ці мережі, який міг би призводити до масштабних згубних наслідків, призвів до усвідомлення необхідності виділення комп'ютерних злочинів в особливу групу. Відповідні норми виникають спочатку в національному, а потім і в міжнародному праві. Про виділення окремої категорії кіберзлочинів слід говорити з 1980-х років. В 1990-ті та на початку 2000-х років відбулося закріплення їхньої кримінальної протиправності в національному та міжнародному праві. Україна брала участь в цих процесах, хоча й з помітним запізненням та під значним впливом норм міжнародного права, зокрема тих, що були розроблені в рамках Ради Європи. Завдяки цим нормам, загального визнання набуває поняття «кіберзлочин», яким позначаються всі злочини, що здійснюються за допомогою комп'ютерних технологій.

2. На заваді дослідженню та класифікації кіберзлочинів, та врешті створенню єдиного визначення кіберзлочинів в кримінальному праві стає недостатня концептуальна розробленість самого поняття кіберзлочину та розмитість «кордонів» між кіберзлочинами та рештою злочинних посягань. Шлях до розв'язання цієї проблеми вбачається в використанні концепції кіберпростору як особливої реальності, що створюється електронними технологіями та за допомогою комп'ютерних мереж. Це нематеріальний простір, що виникає на базі матеріальних об'єктів, таких як електронне

обладнання, однак сам не є цими об'єктами, а є цифровим відображенням впливів, що здійснюються за допомогою предметів матеріального світу. Кіберпростір набуває все більше значення для людства, оскільки він відкриває нові можливості, тому слід очікувати його подальшого розширення. Саме розвиток кіберпростору, що стає не менш важливим, ніж реальний простір, зумовлює потребу в науковому дослідженні злочинів, які можуть скоюватися в кіберпросторі, тобто кіберзлочинів.

3. Єдина класифікація кіберзлочинів наразі відсутня, що можна пояснити як тим, що дослідження самого явища триває, так і особливостями цієї групи злочинів, які визначають різність підходів. Очевидним є лише те, що старі доктринальні підходи до класифікації кіберзлочинів є незадовільними в силу їхніх особливостей, оскільки вони охоплюють злочини, що скоюються в реальному, а не в віртуальному світі. Найбільш простою та очевидною класифікацією є та, що використана в Конвенції Ради Європи про кіберзлочини. Ця класифікація спирається на об'єкт злочинного посягання, а її підставами є правовідносини, що страждають внаслідок злочинного посягання. Цей підхід можна назвати кримінально-правовим. Інший підхід, що можна визначити як криміналістичний, проводить класифікацію кіберзлочинів в залежності від способу злочинного посягання. Нарешті, класифікацію в залежності від особистості злочинця слід позначити як кримінологічну.

4. Розслідування кіберзлочинів спирається на загальні норми кримінально-процесуального права щодо кримінальних проваджень, проходить ті ж самі стадії та має вести до того ж результату у вигляді розкриття злочину та притягнення винного до кримінальної відповідальності. Кримінальне провадження у справах про кіберзлочини спирається на загальні норми КПК України щодо кримінальних проваджень. Зокрема, мова йде про статтю 91 КПК України, якою визначаються обставини, що підлягають доказуванню в кримінальному провадженні. Водночас, при розслідуванні кіберзлочинів слід брати до уваги їхній «ідеальний» характер, що зумовлює особливості проведення слідчих дій. Так, такі слідчі дії як огляд місця події можуть втрачати сенс через відсутність цього місця в реальності. Вирішального значення набувають прийоми, способи та техніки роботи з інформацією та проведення відповідних слідчих дій з метою виявлення цієї інформації, яка дозволяє встановити характер злочинного діяння у кіберпросторі. Також слід брати до уваги складні причинно-наслідкові зв'язки між діями в реальному світі та результатом, що настає в кіберпросторі та через нього знов таки в реальному світі. Розслідування кіберзлочину переважно повинно бути спрямоване на виявлення подій в кіберпросторі, що призвели до настання злочинного результату в реальному світі.

5. Типова слідча ситуація на початковому етапі розслідування кіберзлочинів характеризується, зазвичай, як виявлення ознак злочину, що відбувається одразу після його скоєння, або через певний час. З урахуванням особливостей кіберзлочину, здійснення більшості невідкладних слідчих дій, що передбачені процесуальним законом для звичайних злочинів, уявляється неможливим, через фізичну відсутність злочинця в місці настання злочинного

результату та здійснення злочинного впливу на відстані. Єдиною невідкладною слідчою дією, що можна проводити практично в усіх випадках виявлення ознак кіберзлочину, є огляд місця події. Слідчо-оперативні групи, що формуються для здійснення огляду при розслідуванні кіберзлочинів, повинні включати в себе фахівців в галузі комп'ютерної техніки. Окрім огляду, на початковому етапі розслідування доцільно також проведення слідчих дій, спрямованих на встановлення особистості злочинця, або виявлення ознак, що вказували б на особистість злочинця. Завдяки цим діям, можливим стає встановлення кола підозрюваних та перехід до наступного етапу розслідування кіберзлочину.

6. На наступному етапі розслідування кіберзлочину стає можливим відпрацювання версій, що були висунуті на початковому етапі розслідування та їхня перевірка зі здійсненням таких слідчих дій як допит, обшук, експертиза. Оскільки на даному етапі розслідування, як правило, вже сформоване коло підозрюваних, особливе значення набуває подолання їхньої протидії розслідуванню та викриття повної картини злочину та ролі підозрюваного (підозрюваних) у ньому. Підозрювані в кіберзлочинах, зазвичай, мають такий рівень технічної підготовки, що переважає рівень знань про комп'ютерну техніку слідчого, тому особливого значення набувають експертні висновки, отримані за результатами дослідження виявлених доказів. Використовуючи результати експертних досліджень та інших слідчо-розшукових дій, слідчий може здолати опір підозрюваного та спонукати його до визнання провини, або зібрати достатні докази, що вказують на вину особи, незалежно від визнання вини цією особою, або виявити, що зібраних доказів недостатньо для встановлення вини особи. В останньому випадку, слідчий вирішує питання про проведення подальших слідчих дій.

7. Можна виділити особливості слідчо-розшукових дій при розслідування кіберзлочинів. Головною з таких особливостей є сам набір СРД, які проводяться з урахуванням «віддаленого» характеру розслідуваного діяння. Так, при проведенні огляду слід зосередитися на об'єктах реального світу, що відображують злочинний вплив, такий як підготовка, скоєння та приховання кіберзлочину. Слід мати на увазі, що статичні сліди в реальному світі вказують на динамічну ситуацію кіберсвіту. До проведення огляду місця події кіберзлочину завжди повинен залучатися спеціаліст в галузі комп'ютерних технологій. Йому варто ще до початку огляду поставити питання, на які необхідно звернути увагу та які підлягають встановленню, він має брати участь в здійсненні всіх елементів огляду, а також попередити слідчого при виявленні ознак стороннього впливу під час огляду. Запорукою успішності проведення огляду, виявлення всіх слідів та встановлення динамічної картини злочину, є взаємодія слідчого і спеціаліста.

8. Встановити подію злочину та визначити подальші перспективи й напрямки розслідування можливо лише завдяки допиту фізичних осіб, таких як потерпілі та свідки. Технічна складність кіберзлочину зумовлює особливу важливість стадії підготовки до допиту, в тому числі, вивчення слідчим спеціальної літератури та консультації зі спеціалістом. Другим елементом підготовки стає встановлення якомога більш повної інформації конкретної

особи, яка підозрюється у скоєнні злочину, або загального психологічного портрету. Поінформованість слідчого дозволяє йому досягнути психологічної переваги над злочинцем, що є запорукою успішності допиту.

9. Експертиза є найбільш ефективним способом виявлення доказів на наступному етапі розслідування кіберзлочинів. При їхньому розслідуванні, за необхідності, можливе застосування будь-якого виду експертизи, проте найчастіше мова йде про комп'ютерно-технічну експертизу, яка, з точки зору чинного КПК України, є різновидом інженерно-технічної експертизи. Запорукою вдалої експертизи є правильність постановки завдань слідчим. Визначити вичерпні рекомендації щодо таких питань уявляється неможливим, і їхнє формулювання залежить від конкретних обставин справи та рівня технічної підготовки слідчого. Водночас, можна встановити ряд загальних питань, які спрямовані на виявлення основних рис досліджуваних подій. Це питання про можливість скоєння злочину за допомогою конкретного виду комп'ютерної техніки, про використання цієї техніки в момент скоєння злочину, про можливість використання техніки підозрюваним, тощо. Для встановлення динаміки кіберзлочину доцільно скористатися таким прийомом як ситуаційна експертиза. Вона полягає у проведенні безпосередньо на місці події в матеріальному світі співставлення слідів, що виявляють динаміку процесу, який впливав на віртуальний світ. По своїй суті, ситуаційна експертиза знаходиться на перетині віртуального й реального світу і дозволяє зібрати достатню інформацію для того, аби в подальшому проводити «огляд» в віртуальному світі, тобто експертизу злочинного впливу, що мав місце в комп'ютерній реальності.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

наукові праці у фахових наукових виданнях

1. Довженко О. Ю. Поняття кіберзлочину з криміналістичної позиції. Юридичний вісник. 2018. № 3. С. 79–83.

2. Довженко О. Ю. Класифікація кіберзлочинів у криміналістиці. Південноукраїнський правничий часопис. 2019. № 1. С. 19–22.

3. Довженко О. Ю. Деякі питання призначення комп'ютерно-технічної експертизи під час розслідуванні кіберзлочинів. Науковий вісник Ужгородського національного університету. Серія «Право». 2019. Вип. 55, т. 2. С. 124–127.

4. Довженко О. Ю. До питання про тактику допитів у справах про кіберзлочини. Науковий вісник Міжнародного гуманітарного університету. Серія «Юриспруденція» : зб. наук. пр. Одеса, 2019. Вип. 37. С. 143–145.

5. Довженко А. Ю. Историко-правовые условия становления категории киберпреступности в международном и национальном праве. Legea şi viaţa = Закон и жизнь (Республика Молдова). 2019. № 6/2. С. 55–258.

6. Довженко О. Ю. Особливості проведення допиту у справах про кіберзлочини. Право та державне управління : зб. наук. пр. Запоріжжя. 2019. № 3, т. 2. С. 56–60.

тези доповідей на науково-практичних конференціях

1. Довженко О. Ю. До питання про визначення поняття кіберзлочину. *Модернізація законодавства та правозастосування: вимоги часу* : матеріали Міжнар. юрид. наук.-практ. інтернет-конф. (м. Київ, 6 груд. 2018 р.). Київ, 2018. С. 191–193. URL: http://www.legalactivity.com.ua/index.php?option=com_content&view=article&id=1950%3A051218-14&catid=232%3A5-122018&Itemid=286&lang=ru (дата звернення: 20.01.2020).

2. Довженко О. Ю. Становлення міжнародно-правового регулювання боротьби з кіберзлочинністю. *Конгрес міжнародного та європейського права* : матеріали Міжнар наук. конф. (м. Одеса, 25–26 трав. 2018 р.) / Нац. ун-т «Одес. юрид. акад.». Одеса, 2018. С. 131–136.

3. Довженко О. Ю. Збирання інформації про особу як етап підготовки до допиту при розслідуванні кіберзлочинів. *Соціально-гуманітарний вісник* : зб. наук. пр. [за матеріалами VI Всеукр. наук.-практ. конф. «*Сучасні тенденції соціально-гуманітарного розвитку України та світу*» (м. Харків, 27 верес. 2019 р.)]. 2019. Вип. 28. С. 102–103. URL: http://www.newroute.org.ua/wp-content/uploads/2019/09/Vypusk-28.-Blok..pdf (дата звернення: 20.01.2020).

4. Довженко О. Ю. Історико-правові умови виникнення кіберзлочинності. Кримінальне правопорушення: національний та зарубіжний виміри : матеріали Міжнар. наук.-практ. конф. (м. Одеса, 24 трав. 2019 р.) / Півден. регіон. центр НАПрН України, НУ «ОЮА». Одеса, 2019. С. 201-203.

5. Довженко О. Ю. Методика дослідження особистості злочинця при розслідуванні кіберзлочинів. Міжнародне та національне законодавство: способи удосконалення : матеріали Міжнар. наук.-практ. конф. (м. Дніпро, 29–30 берез. 2019 р.) / Дніпров. гуманітар. ун-т. Дніпро, 2019. 173-175.

6. Довженко О. Ю.Особливості підготовки до проведення допиту при розслідуванні кіберзлочинів. *Пріоритетні напрями розвитку сучасної юридичної науки* : матеріали Міжнар. наук.-практ. конф. (м. Харків, 20–21 верес. 2019 р.) / Асоціація аспірантів-юристів. Харків, 2019. С. 94–95.

АНОТАЦІЯ

Довженко Олексій Юрійович. Основи методики розслідування кіберзлочинів. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 «кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». –Одеський державний університет внутрішніх справ, Одеса, 2019.

Дисертація є комплексним науковим дослідженням теоретичних, нормативно-правових та організаційних засад методології розслідування кіберзлочинів.

Здійснене комплексне наукове дослідження проблем методології боротьби з кіберзлочинами та кіберзлочинністю відповідно до вимог чинного Кримінального процесуального кодексу України. Визначено стан наукової розробки проблеми, охарактеризовано історичні аспекти та сучасний стан методології боротьби з кіберзлочинністю.

Визначено теоретичні основи методології розслідування кіберзлочинів відповідно до приписів чинного кримінального процесуального законодавства та з урахуванням віртуального характеру кіберзлочинності. Проведено дослідження типових слідчих ситуацій, що виникають при розслідуванні кіберзлочинів, зокрема тих, що існують на початковому та наступному етапі розслідування.

Розглянуто тактику проведення окремих слідчих дій та їхні особливості, що визначаються «віддаленим», віртуальним характером діяння. Показано особливості тактики проведення слідчих дій з метою визначення динаміки розвитку подій в кіберсвіті.

Ключові слова: кіберзлочин, комп'ютерний злочин, методика розслідування кіберзлочинів, кібербезпека, слідчо-розшукові дії, процесуальні дії, кримінальний процес, криміналістика.

АННОТАЦИЯ

Довженко Алексей Юрьевич. Основы методики расследования киберпреступлений. - Квалификационная научная работа на правах рукописи.

Диссертация на соискание ученой степени кандидата юридических наук (доктора философии) по специальности 12.00.09 «уголовный процесс и криминалистика; судебная экспертиза; оперативно-розыскная деятельность». - Одесский государственный университет внутренних дел, Одесса, 2019.

Диссертация является комплексным научным исследованием теоретических, нормативно-правовых и организационных основ методологии расследования киберпреступлений.

Рассматривается история возникновения и исследования киберпреступлений, доктринальные подходы к проблеме киберпреступности и борьбы с ними и имеющиеся классификации киберпреступлений. Рассматривается история исследования явления киберпреступлений в украинской и иностранной доктрине. Уделяется внимание формированию правового регулирования борьбы с киберпреступностью в Украине. Даётся определение понятию киберпреступления, обосновывается применение этого термина. Проводится его характеристика через категорию киберпространства. Предлагается оригинальная классификация киберпреступлений в зависимости от характера преступного воздействия в киберпространстве.

Определены теоретические основы методологии расследования киберпреступлений. Показывается, что расследование киберпреступлений должно происходить на основе имеющихся норм процессуального права. Делается вывод, что расследование киберпреступлений преимущественно должно быть направлено на выявление событий в киберпространстве, которые привели к наступлению преступного результата в реальном мире. Исследованы типичные следственные ситуации, возникающие при расследовании киберпреступлений. Доказывается, что осуществление большинства неотложных следственных действий, предусмотренных процессуальным законом для обычных преступлений невозможно из-за физического отсутствия преступника в месте наступления преступного результата и осуществления преступного влияния на расстоянии.

Рассмотрены особенности следственных действий на последующем этапе расследования киберпреступлений, в том числе, основные версии, которые могут выдвигаться по результатам первоначального этапа расследования. Проанализированы и показаны особенности тактических приемов допроса, обыска и экспертизы по уголовным производствах о киберпреступления. Доказывается, что на последующем этапе расследования киберпреступлений главной задачей следователя становится преодоления противодействия следствию со стороны подозреваемого. Решающее значение для достижения этой цели является создание интеллектуального превосходства следователя над подозреваемым, которая достигается благодаря умелому использованию информации, полученной при проведении следственных действий.

Рассматривается тактика проведения отдельных следственных действий. Демонстрируется, что особенности тактики следственных действий при расследовании киберпреступлений обусловленные «удаленным» характером деяния, расследуется. Устанавливается, что статические следы в реальном мире указывают на динамическую ситуацию кибермира, следовательно к проведению осмотра места происшествия киберпреступления всегда должен привлекаться специалист в области компьютерных технологий. Исследуется примерный перечень вопросов, которые необходимо задавать эксперту при проведении и подлежащих установлению при осмотре, в частности по выявлению признаков постороннего влияния при осмотре.

Ключевые слова: киберпреступления, компьютерное преступление, методика расследования киберпреступлений, кибербезопасность, следственно-розыскные действия, процессуальные действия, уголовный процесс, криминалистика.

SUMMARY

Dovzhenko O.Y. The basics of methodology of investigation of cybercrime. – Qualifying scientific work on the rights of manuscript.

Thesis for the degree of Candidate of Law (Doctor of Philosophy) in specialty 12.00.09 - Criminal Procedure and Criminology; Forensic Examination; Operative-Investigative Activity.- Odesa State University of Internal Affairs, Odesa, 2017.

The dissertation is a complex scientific study of theoretical, regulatory and organizational principles of the methodology of investigation of cybercrime.

Complex scientific study of the problems of the methodology of combating cybercrime and cybercrime in accordance with the requirements of the current Criminal Procedure Code of Ukraine. The state of scientific elaboration of the problem, the historical aspects and the current state of the methodology of combating cybercrime are defined.

The theoretical bases of the methodology of investigation of cybercrime are determined in accordance with the prescriptions of the current criminal procedural legislation and taking into account the virtual nature of cybercrime. Typical investigative situations that arise in the investigation of cybercrime are investigated, in particular those that exist at the initial and subsequent stages of the investigation.

The tactics of individual investigative actions and their peculiarities determined by the "remote", virtual nature of the act are considered. The peculiarities of the tactics of investigative actions to determine the dynamics of events in the cyberspace are shown.

Keywords: cybercrime, cybercrime, cybercrime investigation technique, cybersecurity, investigative and investigative activities, procedural actions, criminal process, criminalistics.

Підписано до друку _____
Формат паперу 60х84 1/16. Папір для множних апаратів
Друк цифровий. Умовн. друк. арк. 0,9. Обл.-вид. арк. 1,1
Тираж 100 прим.

Надруковано у копі-центрі «Panda-Print»
(ФО-П Панарін В.С.)
61050, м. Харків, м. Фейєрбаха, 11-б