МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

КУЛІУШ В'ЯЧЕСЛАВ МИКОЛАЙОВИЧ

УДК 343.346.8:004

ДИСЕРТАЦІЯ
ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ВЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

08 – Право
081 – Право

Подається на здобуття ступеня доктора філософії

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело
_____ **В. М. Куліуш**

Науковий керівник **Антощук Андрій Олександрович,**
кандидат юридичних наук, доцент

Київ – 2024

АНОТАЦІЯ

Куліуш В. М. Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору. – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття ступеня доктора філософії за спеціальністю 081 – Право. – Національна академія внутрішніх справ, Київ, 2024.

Дисертація є монографічним дослідженням, у якому на підставі аналізу матеріалів практики й теоретичних положень розроблено засади комплексної методики виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору. Дослідження побудоване на основі висновків і положень, що ґрунтуються на сучасних розробках у галузі філософії, криміналістики, кримінального права, кримінального процесуального права, теорії оперативно-розшукової діяльності, соціології.

Визначено, що формами реакції держави на трансформацію соціально-економічного життя у зв'язку з розвитком кіберпростору є: по-перше, криміналізація окремих форм людської діяльності, невід'ємною частиною якої є використання електронно-обчислювальних машин; по-друге, встановлення як кваліфікуючої ознаки використання електронно-обчислювальних машин під час вчинення окремих видів традиційних злочинів, зокрема шахрайства; по-третє, створення спеціалізованих суб'єктів, діяльність яких спрямована на виявлення та документування кримінально протиправної діяльності у сфері інформаційних технологій.

У дослідженні вперше виокремлено та схарактеризовано взаємозв'язки між розвитком кіберпростору й окремими формами кримінально протиправної діяльності економічної спрямованості. Крім того, у дисертації сформульовано визначення кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, її слід тлумачити як систематичну, багатоетапну протиправну діяльність особи (групи осіб), що здійснюють за допомогою використання інформаційних технологій,

забезпечують створенням необхідної інфраструктури та яка спрямована проти функціонування фінансово-економічної системи держави, фінансової діяльності юридичних і фізичних осіб. Розглянуто її структурні елементи. Також схарактеризовано основні моделі оперативного обслуговування кіберпростору як складової виявлення злочинів економічної спрямованості, вчинених із використанням кіберпростору, виокремлено організаційні засади формування оперативних позицій на об'єктах, які становлять оперативний інтерес, а також види організації оперативного обслуговування залежно від територіальної специфіки функціонування відповідного оперативного підрозділу. Уперше проаналізовано види та внутрішню структуру тактичних операцій початкового етапу розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, зокрема: «Аналітичне опрацювання та оцінка матеріалів»; «Встановлення особи злочинця»; «Фіксація цифрових слідів і формування цифрових доказів»; «Виявлення та вилучення речових доказів».

З'ясовано, що основними завданнями, які вирішують під час реалізації тактичної операції *«Аналітичне опрацювання та оцінка матеріалів»*, є: 1) визначення сутності кримінально релевантної події, яку схарактеризовано в матеріалах оперативного підрозділу; 2) встановлення якості попереднього документування кримінально протиправної діяльності; 3) виокремлення обставин кримінально протиправної діяльності, які потребують першочергової фіксації шляхом проведення слідчих (розшукових) і негласних слідчих (розшукових) дій.

Аналітична робота слідчого під час реалізації тактичної операції *«Встановлення особи злочинця»* виконує такі завдання: 1) формування типового портрета (моделі) особи (групи осіб), яка могла вчинити таке кримінальне правопорушення; 2) звуження кола осіб, серед яких необхідно здійснювати пошукові заходи та слідчі (розшукові) дії; 3) прогнозування можливих моделей протидії досудовому розслідуванню, зокрема: а) приховування невстановлених епізодів кримінально протиправної

діяльності; б) знищення елементів слідової картини встановлених фактів кримінально протиправної діяльності.

Встановлено, що особливостями слідчих (розшукових) дій у межах проведення тактичної операції *«Фіксація цифрових слідів і формування цифрових доказів»* є: 1) обов'язкове залучення до проведення будь-якої слідчої дії експерта, спеціаліста у сфері інформаційних технологій; 2) вибір і підготовка оптимальних апаратних засобів та програмного забезпечення, яке може бути використано для коректної фіксації відповідної доказової інформації; 3) підготовка належних носіїв для копіювання та фіксації цифрової інформації у випадках, якщо апаратні засоби і програмне забезпечення не можуть бути вилучені для подальшого дослідження та приєднані до матеріалів кримінального провадження; 4) планування заходів технічного характеру, спрямованих на нейтралізацію можливості знищення суб'єктом цифрової інформації під час безпосереднього проведення слідчої дії; 5) у випадку, коли слідча дія передбачає обов'язкове залучення понятих, ужиття заходів щодо залучення понятих, які володіють достатнім рівнем знань у сфері інформаційних технологій, розуміють сутність дій працівників правоохоронних органів під час її проведення, а також, за необхідності, зможуть дати показання щодо особливостей процесу вилучення слідчим цифрових слідів і коректності останнього.

Обґрунтовано, що тактична операція *«Виявлення та вилучення речових доказів»* спрямована на вилучення: 1) апаратних засобів, які використовували в злочинній діяльності; 2) інструктивних матеріалів і літератури щодо роботи з відповідними апаратними засобами та програмним забезпеченням; 3) платіжних карток й інших платіжних інструментів, які мають відповідну фізичну сутність і можуть бути застосовані під час здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору; 4) документів, зокрема чорнових записів щодо економічних операцій та руху активів під час кримінально протиправної діяльності; 5) готівкових коштів у національній та іноземній валюті, отриманих за

результатами кримінально протиправної діяльності; 6) «традиційних речових доказів», які: а) підтверджують перебування особи у конкретному місці та роботу за відповідними апаратними засобами; б) забезпечують встановлення періодизації перебування особи в конкретному місці; в) деталізують роль особи в механізмі кримінально протиправної діяльності.

Обґрунтовано, що ознаками цифрових кримінальних ринків є: по-перше, транснаціональний характер і можливість функціонування на таких ринках агентів з будь-якої юрисдикції; по-друге, високий рівень анонімності агентів таких ринків і підвищення рівня активності за рахунок створення відповідної репутації на ринку; по-третє, можливість безконтактної передачі окремих видів товарів і послуг з використанням кіберпростору, зокрема певних типів програмного забезпечення чи інших протиправних даних та/або контенту; по-четверте, використання специфічних інструментів оплати, зокрема криптовалютних та інших нетрадиційних засобів платежів.

У дисертації вдосконалено положення щодо організації і тактики проведення окремих слідчих (розшукових) дій під час розслідування в частині формування рекомендацій щодо планування та проведення огляду апаратних засобів у різних тактичних ситуаціях, підготовки до обшуку та конкретизації предмета допиту окремих учасників кримінально протиправної діяльності, а також положення щодо функціональної спрямованості окремих негласних слідчих (розшукових) дій під час розслідування такої кримінально протиправної діяльності в частині конкретизації їх функціональної спрямованості, особливостей підготовки й організаційно-тактичних засад безпосереднього проведення.

За результатами здійсненого дослідження вдосконалено положення щодо типових моделей організації оперативного (ініціативного) пошуку, з огляду на форми кримінально протиправної діяльності; виокремлено такі моделі реалізації оперативної інформації про злочинну діяльність, яку вчиняють з використанням кіберпростору: по-перше, виявлення та документування такої кримінально протиправної діяльності працівником

оперативного підрозділу з подальшим поданням рапорту керівнику слідчого підрозділу; по-друге, документування такої кримінально протиправної діяльності із залученням слідчого для надання методичної допомоги, а також конкретизації етапів оперативно-пошукової роботи, чинників, які ускладнюють оперативний пошук, формування алгоритму оперативно-пошукової роботи щодо окремих форм кримінально протиправної діяльності, яку вчиняють з використанням кіберпростору.

Визначено, що на підготовчому етапі з метою конкретизації предмета допиту аналізують: а) роль конкретної особи в злочинній діяльності; б) на підставі раніше побудованої працівниками оперативного підрозділу чи безпосередньо слідчим матриці зв'язків – ступінь інтенсивності зв'язків цієї особи з іншими учасниками кримінально протиправної діяльності; в) тривалість участі особи в злочинній діяльності.

Обґрунтовано, що предмет допиту виконавця злочину, який входить до складу злочинного угруповання, охоплює такі блоки: 1) дані, які характеризують механізм залучення особи до кримінально протиправної діяльності; 2) дані, які характеризують безпосередню кримінально протиправну діяльність виконавця; 3) дані, які характеризують структуру й чисельність злочинного угруповання, що вчиняє злочини економічної спрямованості з використанням кіберпростору; 4) дані щодо розподілу доходів, отриманих за результатами кримінально протиправної діяльності.

З'ясовано, що обов'язковими елементами предмета допиту організатора кримінально протиправної діяльності є: мотиви та передумови створення злочинного угруповання для здійснення такої кримінально протиправної діяльності; модель структурної побудови угруповання (розподіл ролей) і модель безпосереднього здійснення кримінально протиправної діяльності; біографічні дані організатора й активних учасників, зокрема щодо їх попередньої трудової діяльності з метою виявлення інших осіб, які можуть бути причетними до вчинення злочинів і не відомі працівникам правоохоронних органів; особливості забезпечення злочинного угруповання

загалом й окремих виконавців необхідними апаратними засобами та програмним забезпеченням для вчинення злочинів; дані щодо інфраструктурних елементів такої кримінально протиправної діяльності, зокрема системи зв'язків, які використовують для її забезпечення; форми та фінансові інструменти, які використовували для легалізації доходів, отриманих злочинним шляхом; модель добору нових учасників угруповання.

За результатами здійсненого наукового пошуку набули подальшого розвитку положення щодо узагальнення стану наукової розробленості проблеми виявлення та розслідування кримінально протиправної діяльності, вчиненої з використанням кіберпростору, у частині систематизації теоретичного підґрунтя для формування засад методики виявлення та розслідування таких злочинів, а також спектру практичних проблем, які потребують наукового забезпечення.

Ключові слова: кіберпростір, злочини економічної спрямованості, розслідування протиправної діяльності, кримінальне провадження, криміналістична класифікація, слідчі (розшукові) дії, негласні слідчі (розшукові) дії, тактичні операції, спеціальні знання, взаємодія, кіберполіція.

SUMMARY

Kuliush V. M. Detection and investigation of economic crimes committed using cyberspace. – Qualifying scientific work on manuscript rights.

Dissertation for the degree of Doctor of Philosophy in specialty 081 «Law». – National Academy of Internal Affairs, Kyiv, 2024.

The dissertation is a monographic study in which, based on the analysis of practice materials and theoretical provisions, the foundations of a complex methodology for the detection and investigation of economic crimes committed using cyberspace have been developed. The study is built on the basis of conclusions and provisions substantiated by modern developments in the field of philosophy, criminology, criminal law, criminal procedural law, the theory of operative and investigative activity, sociology.

It was determined that the forms of the state's reaction to the transformation of socio-economic life in connection with the development of cyberspace are: first, the criminalization of certain forms of human activity, an integral part of which is the use of computers; secondly, establishing as a qualifying feature the use of computers during the commission of certain types of traditional crimes, in particular fraud; thirdly, the creation of specialized entities whose activities are aimed at identifying and documenting criminal and illegal activities in the field of information technologies.

In the study, the relationships between the development of cyberspace and certain forms of economic-oriented criminal activities were identified and characterized for the first time. In addition, the dissertation formulates the definition of criminal and illegal activity of an economic orientation, which is carried out using cyberspace, which is understood as systematic, multi-stage illegal activity of a person (group of persons), which is carried out with the help of information technologies, is ensured by the creation of the necessary infrastructure and is directed against the functioning financial and economic system of the state, financial activity of legal entities and individuals, as well as characterized its structural elements.

Also, the main models of operative service of cyberspace as a component of the detection of crimes of an economic nature committed with the use of cyberspace are characterized, in particular, the organizational principles of forming operational positions at objects of operational interest are highlighted, as well as types of organization of operational service depending on the territorial specificity of the functioning of the corresponding operational division. For the first time, the work developed separate types and the internal structure of tactical operations of the initial stage of the investigation of criminal and illegal activity of an economic orientation, which is carried out using cyberspace, in particular, "Analytical processing and evaluation of materials"; "Establishing the identity of the criminal"; "Fixation of digital traces and formation of digital evidence"; "Identification and recovery of physical evidence".

It was determined that the main tasks that are solved during the implementation of the tactical operation "Analytical processing and evaluation of materials" are: first, determining the essence of the criminally relevant event, which is characterized in the materials of the operative unit; secondly, establishing the quality of preliminary documentation of criminal and illegal activity; thirdly, the identification of circumstances of criminal and illegal activity that require priority fixation by means of investigative (search) and covert investigative (search) actions.

Analytical work of the investigator during the implementation of the tactical operation "Establishing the identity of the criminal" solves the following tasks: first, the formation of a typical portrait (model) of a person (group of persons) who could have committed such a criminal offense; secondly, narrowing the circle of persons, among whom it is necessary to carry out search measures and investigative (search) actions; thirdly, forecasting possible models of counteraction to pre-trial investigation, in particular: a) concealment of unidentified episodes of criminal and illegal activity; b) destruction of elements of the trace picture of established facts of criminal and illegal activity.

It was established that the features of investigative (search) actions within the scope of the tactical operation "Fixation of digital traces and formation of digital

evidence" are: first, the mandatory involvement of an expert, a specialist in the field of information technologies in any investigative action; secondly, the selection and preparation of optimal hardware and software that can be used for correct recording of relevant evidentiary information; third, the preparation of appropriate media for copying and recording digital information in cases where hardware and software cannot be removed for further investigation and attached to criminal proceedings; fourth, the planning of technical measures aimed at neutralizing the possibility of destruction of digital information by the subject during the direct investigation; fifth, in the case when the investigative action involves the mandatory involvement of witnesses, taking measures to involve witnesses who have a sufficient level of knowledge in the field of information technologies, understand the essence of the actions of law enforcement officers during its conduct, and also, according to if necessary, they will be able to give evidence about the peculiarities of the process of extraction of digital traces by the investigator and the correctness of the latter.

It is substantiated that the tactical operation "Identification and recovery of physical evidence" is aimed at the recovery of: first, hardware used in criminal activity; secondly, instructional materials and literature on working with relevant hardware and software; thirdly, payment cards and other payment instruments that have a corresponding physical entity and can be used during the implementation of criminal and illegal activities of economic orientation using cyberspace; fourthly, documents, in particular, draft records regarding economic transactions and movement of assets during criminal and illegal activities; fifth, cash funds in national and foreign currency obtained as a result of criminal and illegal activities; sixth, "traditional material evidence", which: a) confirms the presence of a person in a specific place and work with the appropriate hardware; b) ensure the establishment of the periodization of a person's stay in a specific place; c) detail the role of the person in the mechanism of criminal and illegal activity.

It is substantiated that the signs of digital criminal markets are: first, the transnational character and the possibility of agents from any jurisdiction operating on such markets; secondly, the high level of anonymity of the agents of such markets

and increasing the level of their activity due to the creation of an appropriate reputation on the market; thirdly, the possibility of contactless transmission of certain types of goods and services using cyberspace, in particular, certain types of software or other illegal data and/or content; fourth, the use of specific payment tools, including cryptocurrency and other non-traditional means of payment.

In the dissertation, the regulations regarding the organization and tactics of conducting individual investigative (search) actions during the investigation have been improved in terms of the formation of recommendations for planning and conducting a review of hardware in various tactical situations, preparing for a search and specifying the subject of questioning of individual participants in criminal and illegal activities, as well as regulations regarding the functional orientation of individual secret investigative (detective) actions during the investigation of such criminal and illegal activity, in terms of specifying their functional orientation, specifics of preparation and organizational and tactical principles of direct implementation.

According to the results of the research, the provisions regarding typical models of the organization of operational (initiative) search have been improved, taking into account the forms of criminal and illegal activity, in particular, the following models of implementation of operational information about criminal activity committed using cyberspace have been singled out: firstly, detection and documentation of such criminal – illegal activity by an employee of the operational unit with subsequent submission of a report to the head of the investigative unit; secondly, the documentation of such criminal and illegal activity with the involvement of an investigator to provide methodological assistance, as well as the specification of the stages of operational and search work, factors that complicate operational search, the formation of an algorithm of operational and search work in relation to certain forms of criminal and illegal activity that is committed using cyberspace.

It was determined that at the preparatory stage, in order to specify the subject of the interrogation, the following are analyzed: a) the role of a specific person in

criminal activity; b) on the basis of the relationship matrix previously built by the operative unit or directly by the investigator, to determine the degree of intensity of ties of this person with other participants in criminal and illegal activities; c) duration of a person's participation in criminal activity.

It is substantiated that the subject of interrogation of the perpetrator of the crime, who is a member of the criminal group, includes the following blocks: first, data characterizing the mechanism of the person's involvement in criminal and illegal activities; secondly, data characterizing the direct criminal and illegal activity of the performer; thirdly, data characterizing the structure and number of a criminal group that commits crimes of economic orientation using cyberspace; fourth, data on the distribution of income obtained as a result of criminal and illegal activities.

It was determined that the mandatory elements of the subject of questioning of the organizer of criminal and illegal activity are: first, the motives and prerequisites for the creation of a criminal group for the implementation of such criminal and illegal activity; secondly, the model of structural construction of the group (distribution of roles) and the model of direct implementation of criminal and illegal activities; thirdly, biographical data of the organizer and active participants, in particular regarding their previous work activities in order to identify other persons who may be involved in committing crimes and are unknown to law enforcement officers; fourth, the specifics of providing the criminal group in general and individual perpetrators with the necessary hardware and software for committing crimes; fifth, data on the infrastructural elements of such criminal activity, including communication systems used to support it, etc.; sixth, the forms and financial instruments that were used to legalize proceeds obtained through crime; seventh, the model of selection of new members of the group. According to the results of the conducted scientific search, the provisions regarding the generalization of the state of scientific development of the problem of detection and investigation of criminal and illegal activities committed using cyberspace in the part of systematizing the theoretical basis for the formation of the foundations of the

methodology of detection and investigation of such crimes, as well as the spectrum of practical problems that require scientific support.

Keywords: cyberspace, crimes of economic orientation, investigation of illegal activities, criminal proceedings, forensic classification, investigative (detective) actions, undercover investigators (detective actions), tactical operations, special knowledge, interaction, cyber police.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковано основні наукові результати дисертації:

1. Куліуш В. М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. № 2. С. 190–193. URL: http://www.lsej.org.ua/2_2022/42.pdf.

2. Куліуш В. М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178–183. URL: http://www.sulj.oduvs.od.ua/archive/2022/3/29.pdf.

3. Куліуш В. М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. № 1. С. 80–84. URL: http://www.sulj.oduvs.od.ua/archive/2023/1/14.pdf.

4. Куліуш В. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) дій під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Правові новели*. 2021. № 15. С. 217–224. URL: http://legalnovels.in.ua/journal/15_2021/29.pdf.

які засвідчують апробацію матеріалів дисертації:

5. Куліуш В. М. обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали Міжнар. наук.-практ. конф. (Дніпро, 14–15 січ. 2022 р.). Дніпро, 2022. С. 92–94.

6. Куліуш В. М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнар. наук.-практ. конф. (Львів, 18–19 лют. 2022 р.). Львів, 2022. С. 14–17.

7. Куліуш В. М. Окремі аспекти оперативного (ініціативного) пошуку ознак злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Актуальні питання кримінального провадження у сучасних умовах* : матеріали Міжнар. наук.-практ. конф. (Одеса, 31 трав. 2023 р.). Одеса, 2023. С. 137–139. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/391cb1b2-076a-4807-8a7f-e1475032c703/content.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

ДКІБ СБУ – Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України

ДКП НПУ – Департамент кіберполіції Національної поліції України

ЄРДР – Єдиний реєстр досудових розслідувань

ЄС – Європейський Союз

КК – Кримінальний кодекс

КПК – Кримінальний процесуальний кодекс

МВС – Міністерство внутрішніх справ

НСРД – негласні слідчі (розшукові) дії

ОРД – оперативно-розшукова діяльність

СРД – слідчі (розшукові) дії

ВСТУП

Обґрунтування вибору теми дослідження. Одним зі стратегічних завдань держави та її інституцій є забезпечення економічної безпеки, створення сприятливих умов для розвитку економіки й фінансової системи. Водночас виконання такого завдання супроводжується перманентним подоланням ризиків і загроз, які виникають під впливом внутрішніх і зовнішніх чинників та дестабілізують фінансово-економічну систему. Однією з таких загроз залишається злочинність економічної спрямованості, структура якої постійно ускладнюється, а динаміка залишається стабільно високою.

Незворотний процес інформатизації нашого суспільства зумовив диджиталізацію економічних процесів, появу нових фінансових інструментів і ринків, а значна частина фінансово-господарських операцій перемістилася в кіберпростір. Поряд із позитивними процесами, наявні тенденції призвели до появи та розвитку нових форм кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, оскільки злочинність як адаптивна система швидко пристосовується до зміни соціально-економічних реалій та здійснює постійний пошук нових форм і методів отримання незаконних прибутків. Така кримінально протиправна діяльність утворюється сукупністю злочинів, передбачених ст. 190 КК України та статтями розділу XVI КК України, залежно від суті дії для отримання доступу до інформації (ст. 361 КК України та ст. 361-1 КК України або ст. 363-1 КК України). Водночас останніми роками спостерігається істотне збільшення кількості вчинених злочинів цієї категорії.

Відповідно до статистичної інформації Офісу Генерального прокурора, загальна кількість облікованих злочинів, передбачених ч. 2–5 ст. 190 КК України, становила: 2020 року – 14 744, з них повідомлено про підозру – 7734, направлено до суду з обвинувальним актом – 6412; 2021 року – 14 760, з них повідомлено про підозру – 7634, направлено до суду з обвинувальним актом – 6274; 2022 року – 19 430, з них повідомлено про підозру – 6043, направлено до

суду з обвинувальним актом – 4370; за 11 місяців 2023 року – 51 873, з них повідомлено про підозру – 15 499, направлено до суду з обвинувальним актом – 11 727. Крім цього, загальна кількість облікованих злочинів, передбачених ст. 361, 361-1, 363-1 КК України, становила: 2020 року – 1187/114/16, з них повідомлено про підозру – 682/81/1, направлено до суду з обвинувальним актом – 114/78/0; 2021 року – 1679, з них повідомлено про підозру – 1201/12/0, направлено до суду з обвинувальним актом – 1018/10/0; 2022 року – 1403/280/3, з них повідомлено про підозру – 986/264/0, направлено до суду з обвинувальним актом – 888/264/0; за 11 місяців 2023 року – 2245/35/12, з них повідомлено про підозру – 1670/13/1, направлено до суду з обвинувальним актом – 1479/8/1[1].

Такі статистичні дані засвідчують щорічне відсоткове збільшення питомої ваги зареєстрованих злочинів економічної спрямованості, вчинених із використанням кіберпростору, причому такі показники значно вищі за кількість повідомлень особам про підозру та направлених кримінальних правопорушень до суду з обвинувальним актом.

Необхідно зауважити, що з боку держави здійснено своєчасну оцінку таких загроз і ризиків, унаслідок чого створено спеціалізовані суб'єкти для забезпечення ефективного виявлення та розслідування різних форм протиправної діяльності в кіберпросторі, зокрема й такої, що посягає на нормальне функціонування фінансово-економічної системи.

Засвідчуючи високу ефективність роботи підрозділів кіберполіції, слід зосередити увагу й на окремих наявних проблемах, пов'язаних зі швидкою зміною криміногенних процесів у кіберпросторі, необхідністю постійного пошуку нових організаційно-тактичних рішень, а також формування усталених моделей виявлення та розслідування такої кримінально протиправної діяльності.

---

[1] Звіт Офісу Генерального прокурора про зареєстровані кримінальні правопорушення та результати їх досудового розслідування за 2017–2023 рр. *Офіс Генерального прокурора :* [сайт]. URL: https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2.

Зазначене ставить нові завдання для науки криміналістики, яка, з огляду на об'єкт, спрямована на вивчення та осмислення інноваційних форм кримінально протиправної діяльності, систематизації типових форм вчинення злочинів і розроблення їх криміналістичних характеристик, а також формування наукового продукту для забезпечення оптимізації роботи оперативних і слідчих підрозділів у частині виявлення та розслідування окремих форм кримінально протиправної діяльності.

В умовах сьогодення негативно позначається на розслідуванні кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, брак розробленої криміналістичної методики виявлення та розслідування останньої, що значно знижує ефективність слідчої та оперативно-розшукової практики.

Розробленню криміналістичних методик розслідування кримінальних правопорушень присвячено праці вчених-криміналістів, зокрема: Ю Аленіна, А. Антощука, Л. Аркуші, В. Бахіна, В. Берназа, А. Волобуєва, В. Журавля, А. Іщенка, Н. Клименко, В. Коновалової, І. Лузгіна, В. Лисенка, М. Салтевського, М. Селіванова, Р. Степанюка, В. Тіщенка, Ю. Чорноус, В. Шевчука, В. Шепітька, Б. Щура, В. Юсупова та ін.

Проблематику виявлення, попередження та розслідування злочинів, вчинених у кіберпросторі, досліджували П. Біленчук, А. Білоусов, С. Буяджи, А. Волобуєв, В. Гавловський, М. Гуцалюк, Д. Дубов, С. Демедюк, М. Карчевський, О. Котляревський, М. Кравцова, О. Лепеха, М. Літвінов, О. Манжай, В. Марков, А. Марущак, О. Мотлях, І. Осика, Л. Паламарчук, Д. Пашнєв, В. Плетинець, А. Реуцький, С. Рогозін, Б. Романюк, О. Самойленко, М. Салтевський, С. Самойлов, Є. Скулиш, О. Тарасенко, К. Тітуніна, Д. Цехан, В. Цимбалюк, І. Хараберюш, В. Хахановський, В. Шеломенцев, В. Чернєй, С. Чернявський та ін. Серед останніх криміналістичних розробок, що найбільше пов'язані з предметом дослідження, можна виокремити дисертаційне дослідження Т. Романенко «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки» (2021).

Не заперечуючи значущість здобутків учених, слід зазначити, що засади методики виявлення та розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, залишаються нерозробленими, оскільки науковці зосереджують увагу переважно на висвітленні проблем розслідування комп'ютерних злочинів, окремих форм кримінально протиправної діяльності в кіберпросторі та криміналістичному забезпеченні розслідування таких злочинів. Це і зумовлює актуальність та новизну теми представленого дисертаційного дослідження.

Зв'язок роботи з науковими програмами, планами, темами, грантами. Дисертаційне дослідження виконано відповідно до Цілей сталого розвитку України на період до 2030 року (Указ Президента України від 30 вересня 2019 року № 722/2019); Річної національної програми під егідою Комісії Україна – НАТО на 2021 рік (Указ Президента України від 11 травня 2021 року № 189/2021), Плану дій з реалізації Національної стратегії у сфері прав людини на 2021–2023 роки (розпорядження Кабінету Міністрів України від 23 червня 2021 року № 756-р); Тематики наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України від 11 червня 2020 року № 454). Тему дисертації затверджено на засіданні Вченої ради Одеського державного університету внутрішніх справ від 30 жовтня 2020 року (протокол № 3) і включено до Переліку тем дисертаційних досліджень Національної академії правових наук України (№ 767, 2020 рік).

Мета і завдання дослідження. *Метою* роботи є розроблення на підставі аналізу матеріалів практики й теоретичних положень оперативно-розшукової діяльності та криміналістики засад методики виявлення та розслідування кримінально протиправної діяльності економічної спрямованості, вчиненої з використанням кіберпростору.

Для досягнення поставленої мети в дисертації було виконано такі *завдання*:

– окреслити сучасний стан наукового забезпечення розслідування злочинів, учинених у кіберпросторі;

– схарактеризувати взаємозв’язки між окремими формами кримінально протиправної діяльності економічної спрямованості та функціонуванням кіберпростору;

– визначити поняття та проаналізовано структурні елементи кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору;

– виокремити та розглянути основні складові оперативного обслуговування кіберпростору як складової виявлення злочинів економічної спрямованості;

– сформувати типові алгоритми оперативного (ініціативного) пошуку ознак різних форм кримінально протиправної діяльності економічної спрямованості, які вчиняють з використанням кіберпростору;

– встановити, які завдання виконують тактичні операції на початковому етапі розслідування досліджуваної кримінально протиправної діяльності;

– розробити рекомендації з оптимізації організаційно-тактичних засад проведення СРД під час розслідування досліджуваної категорії злочинів;

– проаналізувати тактичні особливості проведення окремих НСРД під час розслідування злочинів економічної спрямованості, які вчиняють з використанням кіберпростору.

Об’єкт дослідження – правовідносини, що виникають у діяльності правоохоронних органів щодо виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору.

Предмет дослідження – виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору.

Методи дослідження. Відповідно до поставленої мети й завдань у роботі використано сукупність загальнонаукових, міждисциплінарних і спеціально-наукових методів пізнання. За допомогою *методів гносеології* з’ясовано сучасний стан наукового забезпечення розслідування кіберзлочинів,

систематизовано наявний науковий доробок дослідників і виокремлено спектр невирішених питань (підрозділ 1.1); визначено типи й інтенсивність зв'язків між розвитком кіберпростору та окремими формами кримінально протиправної діяльності економічної спрямованості (підрозділ 1.2); типізовано сучасні форми кримінально протиправної діяльності економічної спрямованості, які вчиняють з використанням кіберпростору (підрозділ 1.3); окреслено особливості пізнання та функціонування цифрових кримінальних ринків (підрозділ 1.2); розроблено моделі оперативного обслуговування як складової виявлення таких злочинів (підрозділ 2.1), а також типові тактичні операції початкового етапу розслідування (підрозділ 3.1). *Логіко-юридичний метод* надав можливість запропонувати класифікацію форм кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, визначити їх структуру (підрозділ 1.3). *Порівняльно-правовий метод* використано під час порівняння кримінального процесуального й оперативно-розшукового законодавства (підрозділи 3.1, 3.2). За допомогою *методу герменевтики* з'ясовано сутність окремих наукових положень різних галузей знань щодо змісту наукових характеристик і класифікацій (підрозділи 1.2, 1.3, 1.4). *Соціологічний та статистичний методи* використано під час вивчення думок працівників кіберполіції НПУ щодо основних положень виявлення та розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору (підрозділи 1.2, 1.3, 2.1–2.3, 3.1, 3.2).

Емпіричну базу дослідження становлять узагальнені матеріали вивчення 257 кримінальних проваджень, передбачених ст. 190, 361, 361-1, 363-1 КК України, за період 2020–2023 років з Вінницької, Волинської, Дніпропетровської, Івано-Франківської, Житомирської, Закарпатської, Запорізької, Київської, Львівської, Рівненської, Тернопільської, Хмельницької областей, м. Києва; зведені дані анкетування 143 працівників кіберполіції НПУ в межах відповідних структурних міжрегіональних підрозділів за період

з 2020-го до 2023 року, а також власний досвід роботи автора в кіберполіції НПУ.

Наукова новизна отриманих результатів дисертації полягає в тому, що вона є одним із перших комплексних криміналістичних досліджень методики виявлення та розслідування злочинів економічної спрямованості, які вчиняють з використанням кіберпростору. У роботі обґрунтовано низку нових концептуальних положень, висновків і рекомендацій, зокрема:

вперше:

– виокремлено та схарактеризовані взаємозв'язки між розвитком кіберпростору й окремими формами кримінально протиправної діяльності економічної спрямованості, а саме: 1) криміналізація окремих діянь, зумовлена широкомасштабним упровадженням інформаційних технологій та їх структурної складової – кіберпростору в усі форми суспільного життя; 2) якісна трансформація інфраструктури економічної злочинності, що зумовлена перетворенням кіберпростору у невід'ємну складову економічних відносин; 3) трансформація окремих способів вчинення економічних злочинів у складні технології кримінально протиправної діяльності; 4) якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій; 5) формування цифрових кримінальних ринків;

– сформульовано дефініцію кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, яку визначено як систематичну, багатоетапну протиправну діяльність особи (групи осіб), що здійснюють за допомогою використання інформаційних технологій, забезпечують створенням необхідної інфраструктури і яка спрямована проти функціонування фінансово-економічної системи держави, фінансової діяльності юридичних та фізичних осіб; виокремлено її структурні елементи;

– схарактеризовано основні моделі оперативного обслуговування кіберпростору як складової виявлення злочинів економічної спрямованості,

вчинених із використанням кіберпростору, розглянуто організаційні засади формування оперативних позицій на об’єктах, які становлять оперативний інтерес, а також види організації оперативного обслуговування залежно від територіальної специфіки функціонування відповідного оперативного підрозділу;

– розроблено окремі види та внутрішню структуру тактичних операцій початкового етапу розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, зокрема: «Аналітичне опрацювання та оцінка матеріалів»; «Встановлення особи злочинця»; «Фіксація цифрових слідів і формування цифрових доказів»; «Виявлення та вилучення речових доказів»;

удосконалено:

– положення щодо організації і тактики проведення окремих СРД під час розслідування в частині формування рекомендацій щодо планування та проведення огляду апаратних засобів у різних тактичних ситуаціях, підготовки до обшуку та конкретизації предмета допиту окремих учасників кримінально протиправної діяльності;

– положення щодо функціональної спрямованості окремих НСРД під час розслідування такої кримінально протиправної діяльності в частині конкретизації їх функціональної спрямованості, особливостей підготовки та організаційно-тактичних засад безпосереднього проведення;

– положення щодо типових моделей організації оперативного (ініціативного) пошуку, з огляду на форми кримінально протиправної діяльності; виокремлено такі моделі реалізації оперативної інформації про злочинну діяльність, яку вчиняють із використанням кіберпростору: 1) виявлення та документування такої кримінально протиправної діяльності працівником оперативного підрозділу з подальшим поданням рапорту керівнику слідчого підрозділу; 2) документування такої кримінально протиправної діяльності із залученням слідчого для надання методичної допомоги, а також конкретизації етапів оперативно-пошукової роботи,

чинників, які ускладнюють оперативний пошук, формування алгоритму оперативно-пошукової роботи щодо окремих форм кримінально протиправної діяльності, яку вчиняють із використанням кіберпростору;

дістало подальший розвиток:

– узагальнення щодо стану наукової розробленості проблеми виявлення та розслідування кримінально протиправної діяльності, вчиненої з використанням кіберпростору, у частині систематизації теоретичного підґрунтя для формування основ методики виявлення та розслідування таких злочинів, а також спектру практичних проблем, які потребують наукового забезпечення.

Практичне значення отриманих результатів полягає в тому, що сформульовані й аргументовані в дисертації теоретичні положення, висновки та пропозиції впроваджено й використовуються у:

– *правозастосовній діяльності* – для організаційного, методичного, інформаційного забезпечення роботи оперативних і слідчих підрозділів (акт впровадження Департаменту кіберполіції НПУ від 31 жовтня 2023 року);

– *освітньому процесі* – під час викладання навчальних дисциплін «Криміналістика», «Методика і тактика розслідування злочинів» у закладах вищої освіти, а також у процесі підготовки підручників, навчальних посібників, практикумів із зазначених дисциплін (акти впровадження в освітній процес Національного університету «Одеська юридична академія» від 6 вересня 2023 року, Національної академії внутрішніх справ від 4 грудня 2023 року).

Апробація результатів дисертації. Основні положення та результати дисертації оприлюднено на міжнародних науково-практичних конференціях: «Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього» (м. Дніпро, 14–15 січня 2022 року), «Право як ефективний суспільний регулятор» (м. Львів, 18–19 лютого 2022 року), «Актуальні питання кримінального провадження у сучасних умовах» (м. Одеса, 31 травня 2023 року).

Структура дисертації. Робота складається з анотації (українською та англійською мовами), переліку умовних позначень, вступу, трьох розділів, які містять вісім підрозділів, висновків, списку використаних джерел (209 найменувань на 23 сторінках) і додатків (4 додатки на 19 сторінках). Загальний обсяг дисертації становить 241 сторінка, з яких основного тексту – 199 сторінок.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ОСНОВИ ВИЯВЛЕННЯ ТА РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ВЧИНЕНИХ ІЗ ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

1.1. Сучасний стан наукового забезпечення розслідування злочинів, вчинених у кіберпросторі

Розвиток сучасного суспільства супроводжується значною кількістю інституційних, соціальних, економічних, культурологічних та інших трансформацій. Водночас динаміка наявних перетворень дає підстави констатувати постійну транзитивність соціуму, оскільки повсякчас з'являються новації, які потребують переформатування не лише технологічних елементів, а й власне мережі їх підтримки, тобто соціальних структур. Аналітичний огляд досліджень експертів засвідчує, що швидкість змін і впровадження новацій збільшуватиметься, а ключовим інструментарієм їх забезпечення стануть високі інформаційні технології. На нашу думку, розуміння сутності та змісту інформаційних технологій неможливе без ґрунтовного розгляду соціального середовища їх функціонування, тобто сучасного суспільства. Стадію, яка змінює індустріальне суспільство, учені називають по-різному: «зріле індустріальне суспільство», стадія «високого масового споживання» [208], «ера техноелектроніки» [204], «сторіччя інформації» або «постіндустріальне суспільство» [203]. Усі ці назви акцентують на посиленні ролі інформації, технічних знань і послуг через скорочення сегмента важкої промисловості, як наслідок – зміну «філософії» ведення господарської діяльності. Теорія постіндустріального суспільства нині є однією з найпоширеніших соціально-філософських і соціологічних концепцій розвитку суспільства, що безпосередньо підтверджує історична практика.

На початку 60-х років XX ст. відбувся синтез різнопланових наукових поглядів і підходів щодо наукового аналізу сучасного суспільства, що зумовило виникнення низки різних теорій постіндустріального суспільства.

Теорію інформаційного суспільства досліджували у своїх працях такі знані вчені: Р. Кац [205], Й. Масуда [206], М. Порат [207], Т. Стоуньєр [209] та ін.

Можна стверджувати, що в сучасній науковій доктрині термін «інформаційне суспільство» використовують умовно, оскільки залишаються невизначеними його змістова характеристика, сутнісні ознаки, які мають динамічний характер. Крім того, значний вплив на формування єдиного підходу до трактування аналізованого явища здійснюють науковці, які критично ставляться до цієї концепції загалом. Констатуючи значущість інформації та інформаційних ресурсів протягом усього історичного розвитку, вважаємо обґрунтованою позицію М. Карчевського, який стверджував, що головною ознакою інформаційного суспільства є *принципова* зміна ролі інформації: на ній вибудовується економіка; вона є основним ресурсом, який за показником економічної ефективності відіграє визначальну роль, відтіснивши на другий план сировину й енергію [66]. Крім того, концепція інформаційного суспільства стала важливим методологічним доповненням концепції постіндустріалізму. Аналітичний огляд наукових праць і проведення дослідження засвідчують, що на рівні суспільної свідомості інформаційне суспільство асоціюється з розвитком інформаційних і телекомунікаційних технологій, що притаманно технологічному підходу. Проте, визнаючи його вагоме методологічне значення для досягнення мети дослідження, необхідно використати ширший підхід щодо розуміння інформаційного суспільства та систематизації його ознак.

На підставі аналізу наукових праць можна визначити типові підходи до розуміння інформаційного суспільства [46, с. 6]:

– суспільство нового типу, що формується внаслідок нової глобальної соціальної революції, породженої розвитком і конвергенцією інформаційних та комунікаційних технологій;

– суспільство знання, у якому головною умовою добробуту людини й держави стають знання, одержані завдяки безперешкодному доступу та вмінню працювати з інформацією як з найважливішим соціальним і економічним ресурсом, основним джерелом продуктивності праці та влади;

– глобальне мережеве суспільство, у якому обмін інформацією не має часових, просторових і політичних меж;

– суспільство, що формується під впливом довгострокових тенденцій попереднього соціально-економічного розвитку, який передбачає збільшення ролі інформації та знань, а також формування і споживання інформаційних ресурсів у всіх сферах життєдіяльності суспільства за допомогою розвитку інформаційно-комунікаційних технологій, що діють у глобальних масштабах.

Аналіз наявних підходів засвідчує, що вони в переважній більшості акцентують увагу на трансформації не лише соціальних структур, а й економічних інституцій.

Пізнання будь-якого об’єкта соціальної дійсності відбувається поступово в кореляційних залежностях із його розвитком, формуванням методологічного інструментарію для здійснення такого пізнання, а також значенням об’єкта, явища чи процесу для соціальної дійсності. Пізнання об’єктів наукового дослідження може відбуватися двома шляхами: по-перше, систематичне наукове вивчення об’єкта скеровує його подальше прикладне застосування; по-друге, прикладне використання об’єкта здійснюється поза науковим осмисленням як результат застосування певного об’єкта, унаслідок чого формуються відповідні похідні явища чи процеси, що потребують наукового пізнання в межах різних наук з використанням їхнього специфічного інструментарію.

Одним з таких об’єктів стали високі інформаційні технології, які після входження до сфери суспільного життя стали предметом наукового

дослідження вчених у різних галузях наукового знання. Ми поділяємо позицію Д. Цехана, який зазначає, що високі інформаційні технології – це система методів і прийомів обробки інформації, яка відбувається на основі заздалегідь визначеного алгоритму з обов'язковим використанням апаратних засобів і програмного забезпечення, що володіють високим ступенем конвергенції та стандартизації. До змістовно-функціональних елементів характеристики інформаційних технологій належать: апаратне, програмне, інтелектуальне забезпечення та мережа підтримки. Високим інформаційним технологіям притаманні такі ознаки: 1) кардинальна зміна мережі підтримки, яка існувала раніше; 2) соціокультурний ефект, що полягає у відході від традиційного поділу розумової та фізичної праці; 3) здатність до інтеграції (конвергенції) та створення нових техніко-соціальних середовищ; 4) високий рівень стандартизації; 5) швидке моральне старіння їхніх продуктів [186, с. 133].

Формування інформаційних технологій як відповідного соціокультурного явища зумовило появу й доволі просте використання окремих засобів, які стали знаряддями вчинення злочинів, зокрема різного типу ЕОМ, комп'ютерних мереж та окремого феномену кіберпростору, який, з одного боку, став засобом вчинення значної кількості кримінальних правопорушень, а з другого – унікальним середовищем для різних видів високотехнологічної кримінально протиправної діяльності.

З огляду на це, з боку держави відбулася необхідна реакція на зміну соціально-технологічного життя суспільства шляхом: по-перше, криміналізації окремих форм людської діяльності, невід'ємною частиною якої є використання ЕОМ; по-друге, встановлення як кваліфікуючої ознаки використання ЕОМ під час вчинення окремих видів традиційних злочинів, серед яких шахрайство; по-третє, створення спеціалізованих суб'єктів, діяльність яких спрямована на виявлення та документування кримінально протиправної діяльності у сфері інформаційних технологій.

Ситуація, що склалася, поставила нові виклики перед криміналістикою і теорією ОРД щодо наукового забезпечення протидії таким злочинам та

розроблення дієвих криміналістичних методик їх розслідування. Водночас наукові дослідження цієї проблематики мають значну специфіку, передусім у частині необхідності їх постійного та безперервного проведення, що зумовлено такими чинниками: 1) постійним розширенням переліку кримінальних правопорушень, які можуть бути вчинені за допомогою різних складових інформаційних технологій; 2) безперервна модифікація способів вчинення таких злочинів, що прямо корелює з механізмом слідоутворення і, як наслідок, організаційно-тактичними моделями проведення СРД і НСРД; 3) формування нових типів доказів – цифрових доказів, які постійно видозмінюються та потребують систематичного вивчення.

Найпродуктивнішим і методологічно виваженим шляхом на початку будь-якого наукового пошуку є систематизація та узагальнення наукових ідей вчених, а також отриманих ними наукових результатів для виявлення сегментів проблеми, що залишилися недостатньо дослідженими або результати дослідження яких потребують перегляду у зв’язку із суттєвим оновленням емпіричних даних та об’єктів дослідження.

Аналітичне опрацювання наукових досліджень у контексті предмета нашого наукового пошуку актуалізує необхідність систематизації наявних напрацювань учених у відповідні блоки. Насамперед огляду й аналізу потребують наукові роботи, присвячені формам і напрямам використання інформаційних технологій та їх складових у боротьбі зі злочинністю.

Витоки дослідження цієї проблематики у вітчизняній криміналістиці знаходимо в праці Є. Д. Лук’янчикова «Інформаційне забезпечення розслідування злочинів (правові та тактико-криміналістичні аспекти)» [99], у якій закладено методологічні основи використання сучасних здобутків електронно-обчислювальної техніки під час розслідування злочинів, акцентовано увагу на видах засобів інформаційного забезпечення розслідування, зокрема детальному аналізі адміністративних, процесуальних, оперативно-розшукових засобів забезпечення розслідування. Крім того, в

окремому розділі дослідження проаналізовано напрями сучасного стану підвищення ефективності інформаційного забезпечення розслідування.

Згодом цю проблему досліджував В. Бірюков у дисертації «Використання комп'ютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування» [18]. У дослідженні автор проаналізував особливості використання комп'ютерних технологій у слідчій практиці, а також розробив практичні рекомендації щодо використання комп'ютерної техніки для фіксації інформації. Детальний аналіз цієї праці засвідчує, що оскільки її було укладено на початку впровадження інформаційних технологій у практику роботи правоохоронних органів, автор зосередив увагу на характеристиці використання основних засобів фіксації цифрової інформації та подальшому використанні отриманих результатів як доказів у суді. Унаслідок активного впровадження інформаційних технологій у практику правоохоронної діяльності порушену проблему обрав для вивчення Д. Цехан у монографії «Використання інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ» [186]. Автор проаналізував змістовно-функціональну характеристику інформаційних технологій; схарактеризував взаємозв'язки між розвитком інформаційних технологій та окремими формами кримінально протиправної діяльності; питання алгоритмізації використання інформаційних технологій в ОРД; оптимізації використання інформаційних технологій в оперативному пошуку; специфіку використання інформаційних технологій в оперативній розробці, а також використання цифрових доказів у кримінальному судочинстві. Слід зауважити, що в межах криміналістики окреслена проблематика не була предметом комплексного монографічного дослідження, а її окремі аспекти аналізували в контексті вивчення проблем техніко-криміналістичного забезпечення виявлення та розслідування окремих категорій злочинів [7; 38; 62; 132].

Одним із феноменів, який виник як наслідок розвитку інформаційних технологій, є кіберпростір, що став самостійним середовищем і водночас

засобом вчинення кримінальних правопорушень. Тому наступним блоком, який потребує огляду й аналізу, є наукові дослідження щодо сутності та основних складових кіберпростору як відповідного явища. У межах криміналістики й теорії ОРД кіберпростір не був об'єктом самостійного комплексного дослідження, і для розуміння його сутності необхідно аналізувати наукові роботи, виконані в межах інших галузей знань, де вчені досліджували:

– поняття, сутність, функції кіберпростору та його співвідношення з іншими суміжними категоріями [33; 34; 127; 177; 184];

– особливості кіберпростору як об'єкта кримінологічного пізнання крізь призму злочинності, її причин та умов, а також загальних моделей превентивної діяльності [48; 57; 130; 165; 198].

Важливість використання наукових підходів, сформованих у межах інших наук, зумовлена логікою розвитку сучасного наукового знання, для якого традиційним стає використання міждисциплінарних підходів, а також екстраполяція ідей та концепцій одних досліджень, об'єкта і предмета інших наукових сфер. Водночас необхідно зауважити, що така екстраполяція відбувається двома шляхами: по-перше, через використання положень, розроблених іншими науками, без змін, оскільки вони забезпечують виконання завдань конкретної науки; по-друге, доповнення та доопрацювання відповідних понять і категорій з огляду на потреби конкретної галузі знань.

Проаналізовані наукові праці буде використано в дослідженні для визначення сутності кіберпростору як відповідного соціального феномену, його ознак і ключових функцій, а також тенденцій впливу на окремі соціальні процеси, зокрема злочинність, яка є соціальним явищем.

Зауважимо, що в межах криміналістики кіберпростір на концептуальному рівні досліджено в роботі О. Самойленко [160]. У своїй роботі авторка проаналізувала кіберпростір у дуалістичному вимірі крізь його технологічну та соціальну складові. За результатами такого аналізу науковиця обґрунтовано дійшла висновку, що, з огляду на технічну та соціальну складові

такого змісту кіберпростору, останній здійснює суттєвий вплив на механізм правопорушень. У цьому аспекті кіберпростір у криміналістичних дослідженнях можна розглядати як:

а) середовище (обстановка), у якому окремі його елементи (телекомунікаційна мережа, комп'ютерна система тощо) можуть бути використані як знаряддя досягнення протиправної мети – порушення нормального функціонування цього середовища або заволодіння об'єктами інтелектуальної власності, платіжними засобами, матеріальними цінностями;

б) специфічна обстановка, у яку було внесено зміни внаслідок правопорушення (його сліди), які можуть бути джерелом доказів у кримінальному провадженні.

Системний аналіз дисертаційних досліджень, виконаних у межах криміналістики, щодо проблеми розслідування комп'ютерних злочинів дає змогу класифікувати їх за групами.

До першої групи може бути віднесено дослідження, присвячені розслідуванню комп'ютерних злочинів загалом. У межах цієї класифікаційної групи необхідно виокремити дисертаційне дослідження О. Мотляха «Питання методики розслідування злочинів у сфері комп'ютерних технологій» [110]. У цій праці здійснено криміналістичну характеристику злочинів у сфері інформаційних комп'ютерних технологій; визначено зміст планування початкового та подальшого етапів розслідування злочинів цієї категорії; досліджено слідчі ситуації, які складаються під час розслідування таких злочинів; схарактеризовано особливості висунення та перевірки версій під час розслідування злочинів цієї категорії; надано характеристику тактичних особливостей проведення слідчих дій, а також призначення судових експертиз за злочинами цієї категорії.

Крім того, слід акцентувати на дисертації Н. Козак «Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів» [69]. У цій праці висвітлено складові криміналістичної характеристики комп'ютерних злочинів; досліджено види

способів вчинення комп'ютерних злочинів та їх класифікацію; розглянуто механізми вчинення комп'ютерних злочинів у взаємозв'язку зі слідовою картиною; окреслено тактико-криміналістичні прийоми розкриття та розслідування таких злочинів.

До цієї класифікаційної групи можна віднести й дисертаційне дослідження О. Самойленко «Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій» [159]. У роботі визначено криміналістичні особливості викрадень майна, вчинених із використанням комп'ютерних технологій, та їх зв'язок з іншими злочинами; специфіку застосування спеціальних знань під час розслідування таких злочинів; розроблено типові слідчі ситуації та тактичні завдання для розслідування цієї категорії злочинів; визначено та схарактеризовано тактику проведення слідчих дій.

На нашу думку, до другої групи належать дисертаційні дослідження щодо криміналістичного аналізу комп'ютерних об'єктів і комп'ютерних злочинів як специфічного об'єкта криміналістичного пізнання. Серед них виокремимо дисертацію Л. Борисової «Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження» [22]. У цьому дослідженні визначено поняття «транснаціональний комп'ютерний злочин»; окреслено сутність транснаціональних комп'ютерних злочинів; типізовано слідчі ситуації початкового етапу розслідування; особливості виявлення та закріплення слідів цього виду злочинів. Крім того, до цієї групи може бути віднесено дослідження А. Білоусова «Криміналістичний аналіз об'єктів комп'ютерних злочинів» [15], у якому автор виокремив і визначив криміналістичні особливості комп'ютерних об'єктів; з'ясував сутність і зміст використання спеціальних знань у галузі комп'ютерних технологій під час розслідування; визначив особливості тактики пошуку інформації в комп'ютері, системі й мережі з огляду на особливості комп'ютерних об'єктів.

До третьої групи належать дисертаційні дослідження щодо криміналістичного забезпечення процесу розслідування комп'ютерних

злочинів й особливостей використання спеціальних знань під час досудового розслідування цієї категорії кримінальних правопорушень. У межах цієї групи необхідно виокремити дисертацію Л. Паламарчук на тему «Криміналістичне забезпечення розслідування незаконного втручання у роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж» [124]. Виконуючи завдання цього дослідження, авторка схарактеризувала взаємозв'язки та взаємозалежності між елементами криміналістичної характеристики таких злочинів; узагальнила способи підготовки та вчинення злочинів цієї категорії; систематизувала обставини, що підлягають встановленню під час досудового розслідування таких злочинів; типізувала слідчі ситуації початкового етапу їх розслідування; з'ясувала особливості організації і тактики проведення слідчих дій.

Також слід спрямувати увагу на дисертацію Д. Пашнева «Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій» [126]. У цьому дослідженні здійснено криміналістичний аналіз злочинів, вчинених із застосуванням комп'ютерних технологій; визначено та проаналізовано основні способи використання комп'ютерних технологій у злочинній діяльності; розглянуто структуру та форми використання спеціальних знань під час розслідування таких злочинів; розроблено систему методів фіксації слідів, які залишаються внаслідок вчинення комп'ютерних злочинів; уточнено структуру судово-комп'ютерної експертизи.

У дисертації Б. Теплицького «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [173] визначено поняття, зміст і суб'єкти техніко-криміналістичного забезпечення розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем і комп'ютерних мереж, мереж електрозв'язку; висвітлено найкращий зарубіжний досвід техніко-криміналістичного забезпечення розслідування злочинів у цій сфері; запропоновано поняття та

здійснено розподіл техніко-криміналістичних засобів, що застосовують під час досудового розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; висвітлено особливості техніко-криміналістичного забезпечення проведення окремих СРД у досліджуваній категорії кримінальних проваджень, надано пропозиції з удосконалення такого забезпечення; визначено специфіку та запропоновано рекомендації з удосконалення техніко-криміналістичного забезпечення проведення окремих НСРД під час розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; окреслено особливості призначення найтиповіших видів судових експертиз під час розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку; виявлено типові помилки під час призначення експертизи комп'ютерної техніки та програмних продуктів як найпоширенішого різновиду судових експертиз за злочинами цієї категорії, запропоновано шляхи їх попередження; визначено особливості оцінки результатів судових експертиз і напрями їх використання під час розслідування злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

Аналіз наявних дисертаційних досліджень дає змогу окреслити тенденційні напрями пізнання кіберзлочинності у вітчизняній криміналістичній науці. Огляд хронології наукового дискурсу засвідчує, що пік наукової активності в контексті дослідження цього специфічного об'єкта на монографічному рівні відбувся невдовзі після встановлення в КК України кримінальної відповідальності за цю категорію кримінальних правопорушень. Видається, що розвиток наукового знання за такою траєкторією має логічне пояснення та зумовлений низкою чинників, серед яких: напрацювання теоретичних моделей та практичних рішень щодо кримінально-правової оцінки та кваліфікації аналізованої категорії злочинів; напрацювання слідчої практики щодо розслідування таких злочинів, що стала основою для наукового аналізу та формування типових моделей їх розслідування.

Водночас слушно зауважити, що стрімкий розвиток інформаційних технологій призводить до порівняно швидкої втрати актуальності результатів наукових досліджень за цим напрямом, що додатково відбулося у зв'язку з прийняттям нового кримінального процесуального законодавства. Однак проаналізовані нами дослідження є фундаментальним внеском у розвиток криміналістичних знань за цим напрямом, оскільки в них закладено методологічні підвалини наукового аналізу проблеми: запропоновано структуру криміналістичної характеристики таких злочинів, яку може бути використано як теоретичну основу в подальших наукових роботах, присвячених цій проблематиці; сформовано засади тактики проведення слідчих дій під час розслідування злочинів цієї категорії; закладено теоретико-прикладні основи використання спеціальних знань під час розслідування комп'ютерних злочинів.

Водночас у цих дослідженнях недостатньо дослідженим є питання організації розслідування таких злочинів, що створює певний науковий вакуум у висвітленні цієї проблематики. Крім того, бракує наукового аналізу криміналістичної класифікації злочинів, вчинених у кіберпросторі, що, на нашу думку, пов'язано з обмеженою слідчою практикою щодо цієї проблематики.

Учені-криміналісти досліджували й дотичні проблеми, зокрема особливості розслідування злочинів, які не можна віднести виключно до категорії комп'ютерних злочинів, але вчинення яких передбачає використання інформаційних технологій як знарядь та засобів їх вчинення та невід'ємної складової технології кримінально протиправної діяльності, зокрема наукові дослідження, присвячені:

– розслідуванню економічних злочинів, які вчиняють з використанням кіберпростору й інших складових інформаційних технологій [4; 25; 161; 191];

– розслідуванню злочинів, пов'язаних із порушенням авторських і суміжних прав, а також інших кримінальних правопорушень у сфері інтелектуальної власності [39; 78; 169];

– розслідуванню злочинів, вчинених у сфері мобільних комунікацій [123];

– кримінальним процесуальним питанням розслідування злочинів цієї категорії [55; 108];

– міжнародно-правовому співробітництву у сфері боротьби з кіберзлочинністю [202].

Слушно зазначають дослідники, що в науках соціогуманітарного циклу дослідження інформаційних технологій здебільшого йде від практики. Тобто спершу високі технології змінюють дійсність або її частину, що помічають практики, які змушені змінювати свою діяльність, і лише після цього відбувається теоретичне осмислення окреслених змін [186].

У контексті формування моделей виявлення та розслідування кіберзлочинів зауважимо, що поряд з науковим дослідженням цю проблему активно вивчали працівники практичних підрозділів, які, узагальнюючи наявний практичний досвід, розробляли відповідні методичні рекомендації щодо оптимізації протидії кіберзлочинності [29; 50; 120; 122; 154; 155].

Формування відповідного масиву наукового знання в межах криміналістики закономірно актуалізувало питання розроблення концепції розслідування злочинів, вчинених у кіберпросторі. Однією зі спроб обґрунтування такої системної концепції стало монографічне дослідження О. Самойленко на тему «Основи методики розслідування злочинів, вчинених у кіберпросторі» [158]. Комплексний характер цього дослідження зумовив аналіз майже всього спектру питань, пов’язаних із порушеною науковою проблематикою. У межах роботи авторка, використовуючи матеріали практики, ґрунтовно дослідила особливості кіберпростору як об’єкта криміналістичного дослідження та середовища вчинення злочинів, а також запропонувала власну криміналістичну класифікацію злочинів, вчинених у кіберпросторі. Зауважимо, що на теренах вітчизняної криміналістики криміналістичну класифікацію злочинів цієї категорії здійснено вперше.

Крім того, особливість представленої роботи полягає в тому, що дослідниця розглянула та послідовно проаналізувала складові криміналістичної характеристики злочинів, вчинених у кіберпросторі, зокрема: а) визначила її структуру; б) схарактеризувала типові предмети злочинного посягання та їх взаємозв'язок з мотивами вчинення таких злочинів; в) з'ясувала взаємозв'язок типової особи злочинця й типових слідів злочинів, вчинених у кіберпросторі; г) дослідила типові способи й технології вчинення злочинів у кіберпросторі.

Увагу в аналізованій роботі також зосереджено на процесуальних особливостях розслідування злочинів, вчинених у кіберпросторі. З огляду на специфіку попереднього документування та формування матеріалів, які можуть стати підставами для початку кримінального провадження за злочинами цієї категорії, дослідниця проаналізувала всі можливі організаційно-тактичні моделі початку кримінального провадження з розробленням конкретних рекомендацій щодо дій слідчого в кожній із запропонованих моделей. Важливим здобутком є аналіз компетенції суб'єктів, які здійснюють взаємодію зі слідчим під час досудового розслідування таких злочинів.

Водночас у проаналізованих вище дослідженнях недостатньо висвітленими є питання організації розслідування таких злочинів, а в праці О. Самойленко цю проблему майже комплексно розглянуто в контексті аналізу особливостей періодизації розслідування, характеристики типових слідчих ситуацій, а також розроблення системи тактичних операцій розслідування злочинів, вчинених у кіберпросторі.

Водночас у цій науковій роботі знайшли подальший розвиток питання використання спеціальних знань під час розслідування злочинів, вчинених у кіберпросторі, і, що важливо, не лише в частині проведення судових експертиз, а й залучення спеціаліста до проведення окремих СРД. У контексті нашого дослідження положення проаналізованої роботи стануть теоретичною основою для характеристики кіберпростору як середовища для здійснення

різних форм кримінально протиправної діяльності з акцентуванням уваги на особливостях реалізації та характеристиці повноструктурних способів вчинення таких злочинів. Крім того, розроблені авторкою питання щодо організації розслідування таких злочинів буде використано як теоретичне підґрунтя для формування окремих блоків, які стосуються організації розслідування, а доробок щодо тактичних операцій – для розроблення тактики проведення окремих СРД і НСРД.

У контексті організаційного блоку розслідування необхідно зауважити, що авторка поза увагою залишила значний пласт питань, серед яких: система обставин, що підлягає встановленню під час розслідування злочинів цієї категорії; інформаційно-аналітичне забезпечення розслідування; оперативне обслуговування кіберпростору; кадрове забезпечення роботи підрозділів, які здійснюють виявлення та розслідування таких кримінальних правопорушень.

Наступним комплексним дослідженням, яке потребує детального аналізу, є монографічна робота О. Тарасенка на тему «Теорія та практика протидії кримінальним правопорушенням, пов’язаним із обігом протиправного контенту у мережі Інтернет» [171]. У цій науковій роботі увагу зосереджено на оперативно-розшуковому та криміналістичному аспектах проблеми. Водночас теорія ОРД та криміналістика мають частково спільний об’єкт наукового пізнання, а саме злочинну діяльність. Тому наукові розробки в галузі теорії ОРД мають значний вплив на розвиток окремих теоретичних положень криміналістики, зокрема питань тактики проведення СРД і НСРД, організації інформаційно-аналітичного забезпечення розслідування, документування фактів кримінально протиправної діяльності під час розслідування.

Зокрема, в аналізованій монографії акцентовано на дослідженні теоретико-методологічних засад протидії кримінальним правопорушенням, пов’язаним з обігом протиправного контенту в мережі Інтернет. У межах цього блоку питань як теоретична основа нашого наукового дослідження вагоме значення має розроблена автором класифікація кримінальних

правопорушень, пов’язаних з обігом протиправного контенту в мережі Інтернет, що буде використана нами під час структурної характеристики кримінально протиправної діяльності в кіберпросторі, оскільки формує системне розуміння типових способів вчинення таких кримінальних правопорушень, базових моделей і технологій кримінально протиправної діяльності, системи знарядь та засобів, які використовують для вчинення таких злочинів. Основний акцент нашого дослідження пов’язаний з розробленням засад організації розслідування злочинів, вчинених у кіберпросторі, тож слушно виокремити в межах цього блоку доробок автора щодо міжнародного та зарубіжного досвіду протидії зазначеним правопорушенням, оскільки правоохоронні органи зарубіжних країн значно раніше відреагували на необхідність протидії такого типу правопорушенням. За результатами аналізу наукових та інших матеріалів, правоохоронні органи більшості зарубіжних країн на високому рівні забезпечують організацію протидії цій категорії кримінальних правопорушень, зокрема в аспекті вдалих управлінських рішень щодо структурно-функціональної побудови відповідних спеціалізованих правоохоронних органів та їх кадрового забезпечення. Саме тому поряд з іншими матеріалами й узагальненнями описаний автором зарубіжний досвід стане корисним для формування власних пропозицій щодо оптимізації структурно-функціонального та кадрового забезпечення відповідних правоохоронних органів України, які розслідують кримінальні правопорушення цієї категорії.

Не менш важливою в теоретико-прикладному значенні є розроблена автором характеристика досліджуваних кримінальних правопорушень. З огляду на те, що одним із завдань нашого дослідження є формування засад оперативного обслуговування кіберпростору як ключової передумови для своєчасного виявлення, документування та подальшого розслідування кіберзлочинів, важливе значення мають власне кримінологічні напрацювання автора щодо структури та географії такого типу злочинності, оскільки вони дають змогу: 1) конкретизувати конкретні територіальні одиниці, які

потребують посиленого оперативного перекриття, зокрема міста концентрації центрів, які вчиняють різні типи шахрайств із використанням засобів стільникового зв'язку й мережі Інтернет; 2) виокремити типи інформаційних ресурсів у мережі, які потребують постійного посиленого моніторингу з метою своєчасного виявлення кримінальної активності; 3) конкретизувати режими оперативного обслуговування відповідних об'єктів; 4) визначити та конкретизувати кваліфікаційні вимоги до конфіденційних співробітників, які можуть бути залучені для виконання таких завдань. Оскільки опрацювання масивів кримінологічних даних виходить за межі нашого дослідження, напрацювання автора стануть вагомим теоретичним підґрунтям для формування власних моделей та висновків.

Одним із завдань нашого дослідження є характеристика структури кримінально протиправної діяльності в кіберпросторі, тож вагоме значення мають напрацьовані науковцем системні положення щодо способів підготовки, вчинення та приховування злочинів, пов'язаних із розповсюдженням протиправного контенту в мережі Інтернет, передусім у частині ґрунтовної класифікації способів приховування (маскування) такої кримінально протиправної діяльності, яку класифіковано на загальні, способи зачистки й універсальні.

Закономірно, що організаційно-тактична модель розслідування будь-якого кримінального правопорушення безпосередньо пов'язана з тактичними особливостями його виявлення та попереднього документування. Саме тому ключове значення для розвитку й напрацювання власних теоретико-прикладних положень щодо організації розслідування кіберзлочинів мають напрацювання вченого щодо виявлення досліджуваних ним кримінальних правопорушень, зокрема питання щодо: загальних засад пошукової діяльності під час виявлення кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі Інтернет; системи виявлення таких кримінальних правопорушень; особливостей застосування пошукових систем

під час виявлення кримінальних правопорушень, пов’язаних з обігом протиправного контенту в мережі Інтернет.

Попри оперативно-розшукове та кримінологічне спрямування представленого дослідження, автор також розглянув низку власне криміналістичних проблем, зокрема: проведення СРД і НСРД під час розслідування таких кримінальних правопорушень, а також використання спеціальних знань у процесі розслідування кримінальних правопорушень, пов’язаних з обігом протиправного контенту в мережі Інтернет. Безумовно, під час аналізу цих питань автор акцентував увагу на доволі вузькому колі кримінальних правопорушень, які вчиняють у кіберпросторі та пов’язані з розповсюдженням протиправного контенту в мережі Інтернет. Водночас, з огляду на схожість структури механізму кримінально протиправної діяльності, яку здійснюють у кіберпросторі, запропоновані науковцем тактичні моделі можуть бути частково екстрапольовані й на розслідування інших кіберзлочинів, оскільки, слушно зазначає А. Колодіна, необхідно спрямувати посилену увагу на те, що у своїй практичній діяльності на сучасному етапі слідчі постають перед інформаційною невизначеністю в контексті застосування криміналістичних методик, що зумовлено такими чинниками: політика держави щодо криміналізації окремих форм протиправної поведінки та брак напрацьованих методик розслідування інноваційних форм кримінально протиправної діяльності; невідповідність окремих розроблених криміналістичних методик потребам практики, що пов’язано зі зміною моделі суспільних відносин та їх правового регулювання в окремих сферах, зокрема у сфері економіки та господарської діяльності; локалізація значної кількості наукових розробок у межах закладів вищої освіти й наукових установ і відсутність налагодженої співпраці з практичними підрозділами; відсутність наукових узагальнень стосовно розслідування окремих категорій злочинів у зв’язку з браком напрацьованої практики кримінальних проваджень за цими статтями КК України [71].

Крім того, слід виокремити дослідження Т. Коршикової «Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки» У межах цієї роботи визначено предмет злочинного посягання та способи шахрайств, учинених з використанням ЕОТ; висвітлено слідову картину й обстановку вчинення шахрайств, учинених з використанням ЕОТ; надано характеристику особи злочинця та особи потерпілого від шахрайств, учинених з використанням ЕОТ; окреслено обставини, що підлягають встановленню під час розслідування шахрайств, учинених з використанням ЕОТ; виокремлено типові слідчі ситуації та слідчі версії, що виникають під час розслідування шахрайств, учинених з використанням ЕОТ; окреслено основні напрями розслідування шахрайств, учинених з використанням ЕОТ; узагальнено особливості проведення вербальних СРД під час розслідування шахрайств, учинених з використанням ЕОТ; з'ясовано особливості проведення невербальних СРД під час розслідування шахрайств, учинених з використанням ЕОТ [76, с. 23].

Частково підсумовуючи викладене, доходимо таких попередніх висновків: *по-перше*, у межах криміналістики кіберзлочини досліджували переважно після кримінализації зазначених діянь, а згодом ця проблематика протягом тривалого часу залишалася поза увагою дослідників; *по-друге*, останніми роками цю проблему вивчали на комплексному рівні; *по-третє*, динаміка розвитку інформаційних технологій потребує постійної наукової уваги у зв'язку з динамічною трансформацією кримінально протиправної діяльності, як наслідок – моделей розслідування.

1.2. Взаємозв'язки між окремими формами кримінально протиправної діяльності у сфері економіки та функціонуванням кіберпростору

У попередньому підрозділі дослідження увагу було зосереджено на окремих наукових працях, які стосуються сутності кіберпростору як об'єкта криміналістичного аналізу. Водночас необхідно зазначити, що вчені здебільшого оминають питання визначення системи зв'язків і тенденцій їх розвитку між функціонуванням кіберпростору й окремими формами кримінально протиправної діяльності. Тож вважаємо за доцільне проаналізувати основні форми взаємозв'язків між розвитком кіберпростору та його опануванням різними економічними агентами і трансформацією окремих форм кримінально протиправної діяльності у сфері економіки. На думку вчених-економістів, основним глобальним трендом сучасного суспільного буття є перехід у віртуальний інформаційний простір, що прогресує, – онлайн простір. Цій об'єктивній революційній зміні неможливо й безглуздо чинити опір, проте можливо і вкрай необхідно враховувати нові тенденції та нові загрози. Революція у сфері зв'язку та комунікацій стала суттєвим чинником розвитку цифрової економіки, світового економічного зростання та вагомим інструментом забезпечення сталого розвитку. З одного боку, це надало можливість підприємствам і споживачам отримати вигоди від ефективності, швидкості та зручності цифрових операцій та обміну інформацією, а з другого – спричинило зростання ймовірності отримання фінансових збитків, витоку даних і репутаційних збитків через кіберзлочинів дії [125].

Аналітики слушно зауважують, що цифрова економіка істотно змінює традиційні бізнес-процеси. В умовах досягнення найскладніших рівнів цифровізації в економіці відбувається кардинальна трансформація виробничих відносин учасників, результатом якої є об'єднання виробництва й послуг в єдину (цифрову) систему, у якій: 1) усі елементи економічної системи наявні одночасно у вигляді фізичних об'єктів, продуктів і процесів, а також їх

цифрових копій (математичних моделей); 2) усі фізичні об’єкти, продукти й процеси за рахунок наявності цифрової копії та елемента «підключеності» стають частиною інтегрованої ІТ системи; 3) через наявність цифрових копій (математичних моделей) і як частина єдиної системи всі елементи економічної системи безперервно взаємодіють у режимі, близькому до реального часу, моделюють реальні процеси та прогнозовані етапи, забезпечують постійну оптимізацію всієї системи. Продовжуючи, аналітики акцентують на тому, що основними сегментами цифрової економіки є: а) сектор інформаційно-телекомунікаційних технологій, інфраструктура електронного бізнесу (мережі, софтвер, комп’ютери тощо); б) цифрове виробництво й електронний бізнес, тобто процеси організації бізнесу з використанням комп’ютерних мереж; в) електронна торгівля, тобто роздрібний інтернет продаж товарів [190].

Такі процеси не залишилися поза увагою злочинності, що доволі швидко підлаштовує протиправні соціальні практики до нових реалій, а іноді й використовує їх для формування нових сегментів кримінально протиправної діяльності та кримінальних ринків. Сучасна організована злочинність, слушно зауважує А. Бойко, становить високоорганізовану та впорядковану конспіративну протиправну діяльність злочинних організацій з ієрархічною структурою, стійкою взаємодією, розподілом функцій та сформованою статусно-рольовою системою всередині цих організацій, яка спрямована на отримання надприбутків через встановлення часткової чи повної монополії на обіг незаконних товарів і послуг, а також встановлення контролю за дохідними легальними видами діяльності з використанням корумпованих зв’язків з державними чиновниками як для посилення своєї діяльності, так і для організації ефективного захисту від соціального контролю [21, с. 170]. Інші науковці, характеризуючи сучасний стан злочинності, зокрема й у сфері економіки, є ще категоричнішими, оскільки зазначають, що організовані злочинні угруповання, діяльність яких до теперішнього часу обмежувалася національними масштабами, поширюватимуть свої операції за межі

національних кордонів з метою використання можливостей ринків в інших державах. Новітні технології дали новий поштовх не лише законній торгівлі, а й злочинній діловій активності. Широкі зв'язки організованої злочинності полегшили їй встановлення контактів з партнерами з інших континентів. Сучасні банківські можливості спростили реалізацію міжнародних злочинних операцій, а революція в галузі електроніки надала злочинним угрупованням доступ до нових засобів, які дозволили їм незаконно привласнювати мільйони й відмивати доходи, одержані злочинним шляхом. Розвиток суспільства протягом останніх років дав змогу організованим злочинним угрупованням озброїтися та об'єднати зусилля для обкрадання суспільства, що становить значну загрозу для всіх країн [117]. Подія злочину, як і будь-яке явище об'єктивної дійсності, є індивідуальною та неповторною. Тому її пізнання також вирізняється специфічними індивідуальними рисами. Водночас кожен злочин і способи проведення досудового розслідування мають ознаки, що повторюються, які своєю чергою слугують основою формування та розроблення типових прийомів розслідування загалом і відносно до однорідних за криміналістичною характеристикою злочинів [156].

Аналіз історичного досвіду суспільного розвитку переконливо засвідчує, що будь-які інновації завжди розглядають кримінальні угруповання з позиції можливості їх використання в злочинній діяльності. Відсутність правових, морально-етичних та інституційних обмежень у злочинній діяльності дає змогу кримінальним структурам значно швидше впроваджувати інновації у свою діяльність, перетворюючи окремі з них на повноцінний елемент своєї інфраструктури.

Учені стверджують, що протягом останніх років комп'ютерні технології істотно зрушили вперед. На думку фахівців, за темпами розвитку, впливу на соціально-економічну інфраструктуру, внеском у науково-технічну революцію, позитивними змінами в інтелектуалізації суспільства мікроелектронна та комп'ютерна галузі промисловості, що становлять базу розвитку інформаційного простору будь-якої країни, не мають аналогів.

Світова економіка, уряди, військові відомства не обходяться без обчислювальної техніки. Відбувається введення комунікаційних локальних, галузевих, загальнодержавних і міждержавних систем. Комп'ютеризація стосується майже всіх сфер громадського життя: від контролю за повітряним і наземним транспортом – до проблем забезпечення національної безпеки [37; 43]. Безумовно, така ситуація привернула увагу кримінальних угруповань.

Використання спеціальних технічних засобів і комп'ютерних мережевих технологій у злочинній діяльності суттєво активізується останніми роками. Це комп'ютерне хуліганство, комп'ютерний тероризм, фінансові злочини в інтернеті, шахрайство з кредитними картками, оплатою телефонних переговорів, мережева порнографія та виробництво контрафактної продукції, високоякісний компромат тощо.

Нині основним об'єктом уваги, вважає В. Дрьомін, є транснаціональні комп'ютерні злочини у сфері економіки, що ґрунтуються на використанні електронних грошей, віртуальних банків, бірж, магазинів тощо. Мережа Інтернет стала таким самим місцем діяльності злочинців, як і фізичний світ. Одним із видів злочинів є типові податкові злочини, які вчиняють у сфері функціонування комп'ютерної та інформаційної техніки й пов'язаних з нею послуг, фактично тіньова економіка в інформаційному середовищі. Як приклад можна назвати нелегальні конвертаційні центри, використовувані злочинними формуваннями для проведення протизаконних валютних операцій із застосуванням мережі Інтернет. Комп'ютерна злочинність тісно пов'язана з тим сектором економіки нашої держави, який часто називають не тіньовим, а віртуальним [51, с. 371]. Така проблема є і в розвинутих країнах, зокрема, протягом тривалого часу в США за допомогою комп'ютерної техніки здійснювали контроль за надходженням податків від приватних компаній. Комп'ютер порівнював оголошені прибутки компаній із фактично сплаченими податками й видавав на цій підставі звіти. 1975 року виникла проблема, оскільки з'ясувалося, що компанія «Вестерн Юніон» постійно готувала

завідомо неправдиві відомості для введення до ЕОМ і протягом восьми років ухилялася від сплати податків.

Переходячи до безпосереднього аналізу взаємозв'язків між розвитком кіберпростору й окремими формами кримінально протиправної діяльності, слушно зауважити про позицію Д. Цехана, який зазначав, що взаємозв'язки інформаційних технологій зі злочинною діяльністю виявляються в трьох напрямах: 1) поява інноваційних форм кримінально протиправної діяльності; 2) модифікація «традиційних» механізмів вчинення злочинів, а саме способу й особи злочинця; 3) створення інноваційних техніко-соціальних середовищ, що з плином часу криміналізуються та використовуються в окремих формах кримінально протиправної діяльності [186]. Загалом таку позицію ми поділяємо щодо взаємозв'язків інформаційних технологій та злочинності загалом. Водночас аналітичний огляд наукових робіт, вивчення матеріалів оперативно-розшукових справ, кримінальних проваджень і проведене опитування працівників правоохоронних органів дають підстави стверджувати, що в контексті економічної злочинності така система взаємозв'язків має дещо інший характер, який потребує додаткового дослідження.

Слід констатувати, що взаємозв'язки між розвитком кіберпростору й окремими формами кримінально протиправної діяльності у сфері економіки проявляються у таких формах:

– криміналізація окремих діянь, зумовлена широкомасштабним упровадженням інформаційних технологій та їх структурної складової – кіберпростору в усі форми суспільного життя (71 %, п. 1 додатка Б);

– якісна трансформація інфраструктури економічної злочинності, що зумовлена перетворенням кіберпростору на невід'ємну складову економічних відносин (69 %, п. 1 додатка Б);

– трансформація окремих способів вчинення економічних злочинів у складні технології кримінально протиправної діяльності (61 %, п. 1 додатка Б);

– якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій (51 %, п. 1 додатка Б);

– формування цифрових кримінальних ринків (92 %, п. 1 додатка Б).

Безумовно, усі ці напрями знаходяться в системних зв'язках між собою, але, попри особливості кожного з них, їх може бути досліджено відокремлено з подальшим узагальненням.

Першим напрямом взаємозв'язків є ***криміналізація окремих діянь, зумовлена широкомасштабним використанням кіберпростору в усіх сферах суспільного життя.***

Ґрунтовно дослідивши теорію криміналізації, Д. Балобанова зазначає, що до підстав кримінально-правової заборони слід відносити: 1) суспільну небезпеку – неможливо встановити універсальний критерій, за яким можна було б визначити достатній для криміналізації ступінь суспільної небезпеки. Під час обговорення кожної кримінально-правової новели необхідно вирішувати питання про наявність такої в конкретному виді діянь. Суспільна небезпека охоплює наявність достатньо серйозної матеріальної або моральної шкоди, заподіюваної потерпілим, що впливає на пеналізацію і не є самостійною підставою криміналізації; 2) типовість і достатня поширеність антигромадської поведінки, однак з урахуванням ступеня їхньої суспільної небезпеки; 3) динаміка суспільно небезпечних діянь з урахуванням причин й умов, що їх породжують; 4) необхідність впливу кримінально-правовими заходами, за якого необхідно враховувати, що кримінальна репресія – крайня форма протидії найнебезпечнішим формам девіантної поведінки. Криміналізація діяння доречна тоді, коли немає й не може бути норми, що ефективно регулює відповідні відносини методами інших галузей права; 5) урахування можливостей системи кримінальної юстиції в протидії певним формам антигромадської поведінки і як їхня складова – наявність матеріальних ресурсів для реалізації кримінально-правової заборони;

6) співвідношення позитивних і негативних наслідків криміналізації [11, с. 176–177].

Нині науковці активно досліджують проблеми криміналізації та кримінально-правової протидії суспільно небезпечним діянням, генеза яких безумовно пов’язана з розвитком кіберпростору.

У контексті нашого дослідження слушною видається позиція Д. Азарова, який зазначає, що існування кримінально-правових норм не може зумовлюватися лише поширеністю певних посягань. Порівняно незначна кількість зареєстрованих у нашій країні суспільно небезпечних діянь у сфері комп’ютерної інформації не повинна істотно впливати на встановлення кримінальної відповідальності за їх вчинення. Насамперед необхідно враховувати характер і ступінь суспільної небезпечності означених діянь. Саме суспільну небезпеку слід розглядати як головну підставу їх криміналізації (декриміналізації) [2, с. 16]. Тому, на нашу думку, попри незначну кількість зареєстрованих на початковому етапі освоєння кіберпростору громадянами нашої держави високотехнологічних злочинів, було вжито заходів щодо кримінально-правової охорони суспільних відносин, які пов’язані з використанням інноваційних форм представлення інформації та використанням комп’ютерної техніки. Аналіз чинного КК України засвідчує, що найпоширеніші види протиправних діянь у цій сфері закріплено в окремому розділі Особливої частини КК України «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку».

На підставі аналізу норм КК України доходимо висновку, що, формуючи концепцію кримінально-правової протидії економічній злочинності, вітчизняний законодавець не пішов шляхом закріплення окремих норм кримінального закону щодо економічних злочинів, які вчиняють за допомогою кіберпростору, а лише встановив використання ЕОМ як кваліфікуючу ознаку для окремих складів кримінальних правопорушень, зокрема шахрайства. Такий підхід, з одного боку, є виправданим оскільки

збільшення кількості економічних злочинів, які можуть бути вчинені за допомогою кіберпростору, призвело б до значного та необґрунтованого розширення складів кримінальних правопорушень і дисбалансу кримінального законодавства України. Водночас такий підхід не враховує підвищений рівень суспільної небезпечності злочинів, учинених із використанням кіберпростору.

Необхідно зауважити, що з розвитком цифрових процесів і процедур в економіці України підхід законодавця до реагування на відповідні дії на рівні кримінального закону зазнає змін.

Другим напрямом взаємозв'язків є якісна трансформація інфраструктури економічної злочинності, що зумовлена перетворенням кіберпростору в невід'ємну складову економічних відносин. У контексті цього зазначимо, що розроблення ефективних організаційно-тактичних моделей виявлення злочинів неможливе без аналізу середовища функціонування злочинності як соціального явища, зокрема й легальних соціальних, економічних і технологічних структур, які можуть бути використаними для забезпечення кримінальної активності. З огляду на викладене, вітчизняні вчені досліджують таку категорію, як «інфраструктура злочинності».

Д. Цехан, аналізуючи форми злочинності, визначав, що інфраструктуру злочинності можна визначити як систему суб'єктів і засобів, що не наділені чіткими криміногенними ознаками, проте забезпечують злочинну діяльність, а також є інструментом взаємодії між злочинністю та соціально-економічними інститутами [187].

Водночас слід зазначити, що сучасні вчені-криміналісти кіберпростір не розглядали крізь призму інфраструктури злочинності, акцентуючи увагу на аналізі кіберпростору як обстановки вчинення злочину та знаряддя вчинення злочину. Водночас, на нашу думку, такий науковий підхід є занадто спрощеним, адже виключає зі спектру уваги ті елементи кіберпростору, які можуть бути використані поза межами вчинення конкретного кримінального

правопорушення чи реалізації складної технології кримінально протиправної діяльності. На нашу думку, кіберпростір як складова інфраструктури економічної злочинності може виконувати такі функції:

– *інтелектуальне й інформаційне забезпечення кримінально протиправної діяльності* (97 %, п. 2 додатка Б). У контексті цього необхідно зазначити, що кіберпростір як відповідний соціально-технологічний феномен не реалізує цю функцію у формі безпосередньої активності, а є інформаційним ресурсом для отримання відповідних знань і компетенцій злочинцями, зокрема щодо: особливостей технологічного здійснення відповідних фінансових операцій у віртуальному середовищі; аналітичних узагальнень щодо недоліків окремих видів програмного забезпечення, технологічних циклів й окремих моделей фінансових транзакцій; загального підвищення інтелектуального рівня злочинців через узагальнення досвіду кримінально протиправної діяльності інших осіб; миттєвого отримання інформації щодо появи програмних продуктів та інструкцій з їх використання, які може бути застосовано в злочинній діяльності;

– *створення умов для формування стійких безконтактних зв'язків між особами, які надалі можуть здійснювати спільну кримінально протиправну діяльність* (98 %, п. 2 додатка Б). З огляду на викладене, розвиток кіберпростору як інфраструктурного елементу злочинності призвів до появи злочинних угруповань «мережевого типу», яким притаманні такі ознаки: а) відсутність чітко вираженого лідера (лідером під час вчинення конкретного правопорушення є особа, яка розробила ідею його вчинення, що дає змогу будь-якому члену злочинного угруповання посісти лідерську позицію під час реалізації конкретного епізоду кримінально протиправної діяльності); б) безконтактний спосіб функціонування таких груп, що виключає необхідність особистого знайомства, комунікації та використання особистих даних; в) можливість перебування членів такого угруповання в різних юрисдикціях під час здійснення кримінально протиправної діяльності. Використовуючи мережеву модель, злочинні організації, зазначає Г. Жаровська, створюють

гнучкіші й динамічніші структури. Злочинним мережам притаманні непостійне членство та високий рівень адаптації до політичних, економічних і соціальних змін, що відбуваються в суспільному житті, без централізованої системи контролю [53]. Інші вчені обґрунтовано зауважують, що організовані злочинні угруповання, побудовані за мережевим принципом, набувають високої адаптивності до змін у середовищі існування та є стійкими до зовнішніх впливів, що зумовлено низкою чинників: по-перше, мережева структура має гнучке управління, що забезпечує підвищену швидкість реакції на дії правоохоронних органів; по-друге, відсутність чітко локалізованої структури; функціональна динамічність ускладнює власне правоохоронну діяльність і створення в таких угрупованнях оперативних позицій; по-третє, здатність до швидкої зміни складу та перерозподілу ролей робить такі угруповання ефективнішими, порівняно з угрупованнями з традиційною ієрархічною структурою в аспекті виживання, оскільки угруповання не припиняє функціонування внаслідок затримання його окремих учасників; по-четверте, такі угруповання для виконання одного й того самого завдання обирають щоразу різні способи, які є оптимальними в контексті поточної ситуації, що ускладнює викриття протиправної діяльності, оскільки унеможливлює використання стандартних алгоритмів оперативно-тактичних ситуацій та криміналістичних методик [41];

– *забезпечення ринку збуту відповідних кримінальних послуг і кримінальних компетенцій* (90 %, п. 2 додатка Б). Безумовно, як інфраструктурний елемент економічної злочинності кіберпростір наділений ознакою легальності, що унеможливлює вплив на його функціонування звичними для оперативних підрозділів прийомами й методами. Водночас невід’ємною складовою кіберпростору як легальної структури став сегмент, який створено на його базі для систематичного та стійкого забезпечення кримінально протиправної діяльності, – Darknet. Darknet – це накладена мережа Інтернету, доступ до якої можна отримати лише за допомогою спеціалізованого програмного забезпечення, конфігурацій та спеціальних

авторизацій, він часто використовує нестандартні протоколи зв'язку, щоб Інтернет навмисно був недоступним. Darknet стосується мереж, які не індексуються пошуковими системами, такими як Google, Yahoo або Bing. Це мережі, які доступні лише для обраної групи людей, а не для широкої громадськості, доступні лише через авторизацію, певне програмне забезпечення та конфігурації. Це включає нешкідливі місця, такі як академічні бази даних і корпоративні сайти, а також ті, що мають «темніші» теми, такі як чорні ринки, фетиш-спільноти, хакерство й піратство. Darknet відрізняється від інших розподілених мереж P2P, оскільки обмін даними є анонімним, тому користувачі можуть спілкуватися поза урядовим контролем чи корпоративним втручанням. З цієї причини Darknet часто асоціюється з політичними комунікаціями дисидентів і незаконною діяльністю. Загалом термін «Darknet» може бути використано для опису всіх некомерційних вебсайтів в інтернеті або для позначення всіх «підпільних» вебкомунікацій і технологій, пов'язаних переважно з незаконною діяльністю. Технічно Darknet – це різновид віртуальної приватної мережі (VPN) з додатковими заходами, що забезпечують неможливість виявлення мережі та IP адрес учасників. Мета полягає в тому, щоб приховати не тільки повідомлення, а й факт обміну інформацією. Учасники приєднуються зі сподіванням на можливість обмінюватися інформацією або файлами з невисоким ризиком виявлення. Організовані злочинні угруповання, вважає М. Гуцалюк, у своїй діяльності часто використовують мережу Darknet, вебсайти якої не індексуються і на які неможливо потрапити через пошукові системи. У Darknet активно послуговуються криптографічними технологіями мережевої анонімності й онлайн розрахунків, які дали змогу злочинцям створити чорний ринок, де продають і купують наркотики, крадені та контрафактні товари, дитячу порнографію, зброю тощо. Ця частина інтернету не врегульована законодавчо, діяльність у ній майже неможливо проконтролювати, а тому організовані злочинні угруповання, використовуючи цю мережу, удосконалюють протиправну діяльність. У Darknet діє значна кількість хакерських спільнот,

які спеціалізуються на конкретних напрямах діяльності, зокрема неправомірному доступі до комп'ютерних систем, продажу шкідливого програмного забезпечення, організації кібератак, викраденні та продажі персональних даних [44].

Здійснений нами контент-аналіз п'яти сайтів у мережі Darknet засвідчує, що на час дослідження на них було розміщено близько 400 оголошень:

1) близько 200 оголошень, присвячених продажу/розповсюдженню наркотичних засобів чи психотропних речовин;

2) окремий розділ «Цифрові товари» містив 100 оголошень, на яких пропонували доступ до зламаних баз даних державних органів;

3) решта оголошень стосувалася можливості придбати документи на володіння транспортними засобами.

На підставі викладеного вище доходимо висновку про відособлену форму зв'язків між розвитком кіберпростору та злочинною діяльністю – ***появу цифрових кримінальних ринків.*** Необхідно зауважити, що передумовою цього явища було створення та розвиток легальних цифрових (електронних) ринків, які слід визначати як систему економічних відносин у віртуальному просторі, які складаються між суб'єктами економічної діяльності щодо торгівлі послугами/товарами через інноваційні середовища, створені на базі інформаційних технологій. Своєю чергою формування електронних ринків вимагало нових підходів щодо здійснення фінансових операцій. Саме тому ми поділяємо позицію науковців, які переконані, що конвергенція комп'ютерних мереж зумовила й конвергенцію фінансових операцій, наприклад, до переліку електронних банківських операцій належать: операції з картковими рахунками; операції з переказу грошей без відкриття банківського рахунку; операції з управління електронним банківським рахунком (системи «клієнт-банк» з доступом через мережу Інтернет); через комп'ютерні мережі здійснюють також низку операцій з оплатою: електронна комерція – створення віртуальних магазинів, реклама, продаж і проведення розрахунків засобами інформаційно-телекомунікаційних технологій (зокрема платіжними

картками); інтернет-банкінг – здійснення через мережу Інтернет міжбанківських операцій та обслуговування клієнтів; IP телефонія – здійснення двостороннього голосового контакту через мережу Інтернет [72, с. 5].

Електронні ринки стали привабливими об’єктами для перетворення їх на складову інфраструктури економічної злочинності, оскільки вони вирізняються диверсифікацією цін, ціновою еластичністю, зниженням витрат на сегментацію ринків тощо. Іншою вагомою причиною опанування електронних ринків кримінальними структурами є постійний пошук шляхів підвищення «рентабельності» кримінально протиправної діяльності, що забезпечують шляхом: скорочення витрат на збут, «рекламу» й утримання роздрібної мережі; зниженням витрат на зберігання товарів; оптимізації системи забезпечення ресурсами. Крім того, електронний ринок підтримує координацію кримінальних зв’язків між злочинними угрупованнями за рахунок оптимізації надійності й динамічності зв’язків; сприяння формуванню власного інформаційно-економічного простору.

Наступним вагомим елементом оптимізації кримінально протиправної діяльності є функціонування на електронних ринках спеціальних платіжних систем. Аналітичний огляд практики функціонування електронного бізнесу та наукових джерел дає змогу запропонувати класифікацію електронних платіжних систем, які використовують кримінальні угруповання. Насамперед розрізняють платежі офлайнові (взаємодія контрагентів відбувається з певним часовим запізненням) та онлайнові (у режимі реального часу). У системах електронної комерції залежно від моменту оплати під час здійснення комерційних угод вирізняють системи з передоплатою; у момент здійснення угоди; з оплатою в момент отримання товару.

Електронні платіжні системи можна умовно поділити на системи, що функціонують на основі пластикових карток (кредитних, дебетових), смарт-карток і систем, у яких функціонують електронні гроші, які є еквівалентом готівки. Електронні гроші – це фінансові товари з вартістю, що передплачена

або зберігається і дає змогу здійснювати транзакції з використанням ІКТ. Одним із різновидів електронних грошей є вебгроші.

Найпопулярнішими платіжними системами, які використовують у мережі Інтернет, є:

– WebMoney Transfer (електронна система, за допомогою якої можна проводити миттєві розрахунки в мережі Інтернет);

– E-Gold (міжнародна платіжна система, кошти якої переведено в дорогоцінні метали);

– PayPal (надає своїм користувачам можливість приймати й відправляти платежі за допомогою електронної пошти або мобільного телефону з доступом до мережі Інтернет);

– Яндекс (російська платіжна система);

– інтернет-гроші (національна небанківська платіжна система);

– Portmone (національна система платежів для оплати рахунків за допомогою банківських платіжних карт MasterCard і Visa).

Для використання таких систем необхідно зареєструватися, а користування відбувається за допомогою спеціального програмного забезпечення, що надсилається або завантажується з відповідних сайтів. За будь-які операції в системі, тобто переказ коштів, нараховують проценти в розмірі від 0,5 % до 3 % від суми переказу. Користування системою можна здійснювати за допомогою цифрових пристроїв, які мають доступ до мережі Інтернет (мобільні телефони, комп’ютери). Для реєстрації в системі необхідно мати номер мобільного телефону й доступ до інтернету.

Водночас поряд з легальними цифровими ринками, які активно опановують кримінальні структури, виникли й нові криміногенні феномени, зокрема цифрові кримінальні ринки. Слід зауважити, що питання протидії створенню та функціонуванню кримінальних ринків досліджували на шпальтах наукових видань. Водночас наявні наукові дослідження розглядають цю проблему в контексті кримінально протиправної діяльності злочинних угруповань загальнокримінальної спрямованості, які формують і

контролюють кримінальні ринки товарів та послуг на відповідних територіях, зокрема кримінальний ринок наркотиків, викрадених транспортних засобів, зброї тощо. Запропоновані вченими моделі протидії функціонуванню таких кримінальних ринків не можуть бути екстрапольовані на цифрові кримінальні ринки, які потребують застосування інших моделей у контексті: 1) організації оперативного обслуговування; 2) виявлення всієї технології постачання та реалізації відповідних товарів на кримінальних ринках; 3) ідентифікацію осіб, які здійснюють протиправну діяльність на таких ринках. Тож у цьому випадку постає необхідність комплексного підходу, зокрема з використанням традиційних методів і засобів ОРД.

На нашу думку, ***цифровими кримінальними ринками*** слід вважати стійку, централізовано не контрольовану систему, яка здатна до самовідтворення та саморегуляції, спрямовану на створення з урахуванням структури й динаміки попиту пропозиції заборонених у цивільному обігу товарів і послуг у кіберпросторі.

З огляду на викладене, можна виокремити типові ознаки кримінальних ринків, які відрізняються від аналогічних утворень у фізичному просторі:

по-перше, транснаціональний характер і можливість функціонування на таких ринках агентів з будь-якої юрисдикції;

по-друге, високий рівень анонімності агентів таких ринків і підвищення рівня власної активності за рахунок створення відповідної репутації на ринку;

по-третє, можливість безконтактної передачі окремих видів товарів і послуг з використанням кіберпростору, а саме певних типів програмного забезпечення чи інших протиправних даних. *Наприклад, у м. Києві до ЄРДР було внесено відомості за ч. 3 ст. 301 КК України, коли злочинні дії невстановлених осіб перекваліфіковано з ч. 1 ст. 301 КК України на ч. 3 ст. 301 КК України стосовно громадян А., Б. і В.*

У межах досудового розслідування встановлено, що громадяни А., Б. і В. у період з 2014 року до кінця 2017 року за попередньою змовою групою осіб на вебсайтах «Dark robbery», «Dark home pussy», «Dark video», «Dark collection»

розміщували продукцію порнографічного змісту за участю дітей, а також рекламні сайти, на яких розміщено картинки попереднього перегляду, після перегляду яких користувач мав можливість придбати безпосередній доступ до сайтів, на яких розміщено порнографічні матеріали. Під час спілкування між собою за допомогою інтернет-пейджера невстановлені особи використовували анонімні номери, псевдоніми. З метою отримання винагороди за збут у мережі Інтернет порнографічних матеріалів невстановлені особи використовували електронну платіжну систему, яка приймала грошові кошти за доступ користувачів до вебсайтів у мережі Інтернет, на яких розміщували порнографічні матеріали, виготовлені за участю дітей, а також рекламували та розповсюджували в мережі дитячу порнографію шляхом створення таких вебсайтів та наповнення їх відповідними фотозображеннями [81];

по-четверте, використання специфічних інструментів оплати, зокрема криптовалютних й інших нетрадиційних засобів платежів.

Одним із найвідоміших прикладів цифрового кримінального ринку є Hydra Market, який є нелегальним торговельним майданчиком, доступ до якого надається через мережу Tor з 2015 року. Лише 2020 року продажі на цьому ринку становили 1,23 млрд євро, а кількість клієнтів – 17 млн. Крім наркотиків, популярними товарами були фальшиві гроші й документи, інструкції щодо здійснення протиправної діяльності, послуги з інтернет-безпеки та злому акаунтів.

Частково підсумовуючи, слід зазначити, що розвиток кіберпростору перетворив його на самостійний елемент інфраструктури економічної злочинності. У переважній більшості випадків як інфраструктурний елемент використовують мережеві системи, які створено із соціально корисною метою. Крім того, декриміналізація мережі Інтернет, зокрема мінімізація можливостей її використання як складової інфраструктури злочинності, вимагають: формування правової основи здійснення фінансових, податкових і господарських операцій через мережу Інтернет; розроблення інституційної

основи контролю за національним сегментом мережі Інтернет; розроблення принципів, тактичних прийомів і належного кадрового забезпечення оперативного обслуговування національного сегменту мережі [24, с. 272].

Самостійними напрямами впливу кіберпростору на окремі форми економічної злочинності є поява нових злочинних технологій та зміна характеристик особи злочинця. Оскільки ці питання безпосередньо пов'язані з особливостями характеристики злочинів цієї категорії, ми зосередимо увагу на них у наступному підрозділі дослідження.

1.3. Криміналістичний аналіз кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору

У попередніх підрозділах дослідження під час аналізу стану наукового забезпечення виявлення та розслідування злочинів, які вчиняють з використанням кіберпростору, увагу зосереджено на тому, що вчені в більшості дисертаційних досліджень аналізували криміналістичну характеристику останніх. У сучасній криміналістичній доктрині криміналістичну характеристику злочинів розглядають як невід'ємну складову методики розслідування, що має власне функціональне призначення. Професор В. Тіщенко в структуру окремих методик розслідування пропонує включати такі елементи: 1) криміналістичну класифікацію злочинів конкретної категорії; 2) криміналістичну характеристику таких злочинів; 3) обставини, що підлягають встановленню; 4) особливості початкового етапу розслідування і типові вихідні слідчі ситуації; 5) типові стратегічні й тактичні завдання та слідчі версії на початковому етапі розслідування; типові програми розслідування, що містять засоби й методи розв'язання поставлених завдань і перевірки версій, форми взаємодії з оперативними підрозділами; 6) типові слідчі ситуації та програми розслідування на його наступному й

завершальному етапах; 7) організаційно-тактичні й техніко-криміналістичні особливості проведення слідчих дій, тактичних операцій у розслідуванні злочинів відповідної категорії [175]. Слушно зазначає В. Шепітько, що нині дискусійною проблемою є визначення внутрішнього змісту окремої криміналістичної методики, її структурних елементів. Останніми роками під час формування окремих криміналістичних методик, що відбувається переважно в процесі написання дисертаційного дослідження, до структурних елементів відносять криміналістичну характеристику певного виду злочинів, початковий етап розслідування, тактику проведення СРД. На думку науковця, такий підхід виконує лише «дисертаційну функцію» або описово-інформаційну [199].

Зауважимо, що ця наукова категорія є ефективною під час формування видових методик розслідування злочинів. Водночас в окремих випадках, зокрема й під час розроблення методик розслідування високотехнологічних злочинів, доволі складно системно й об’єктивно описати всі структурні елементи криміналістичної характеристики в контексті її традиційного розуміння в науковій доктрині.

З огляду на це, вважаємо, що в межах нашого дослідження доцільно використати інший методологічний підхід і висвітлити сутність досліджуваної нами форми кримінально протиправної діяльності крізь призму аналізу її структурних елементів, зокрема акцентувати увагу на стадіях формування умислу, підготовки, безпосередньої реалізації та посткримінальної поведінки. Задля виконання цієї мети необхідно зосередитися на наукових положеннях, розроблених у межах наук кримінально-правового циклу, щодо сутності та змісту кримінально протиправної діяльності загалом. На думку С. Денисюка, злочин і злочинна діяльність не рівнозначні: по-перше, тому що явище (злочин) специфічне та своєрідне, але нерідко доволі обмежене у своїх ознаках і виявах, а їхня сукупність (множинність) має низку характерних ознак, не властивих усім одиничним складовим; по-друге, з тієї причини, що злочин може бути одиничним епізодом і навіть за умови неодноразовості вчинення

злочинів певною особою або групою він не завжди набуває характеру кримінально протиправної діяльності, що відображає спосіб життя. Це виявляється лише на рівні узагальнення, що характеризує життєдіяльність злочинного середовища, усіх її складників як різновиду людської діяльності [47]. Учені Н. Карпов і С. Євдокименко, розглядаючи сутність процесу кримінально протиправної діяльності, слушно зазначали, що необхідно розрізняти злочин як одиничний (нерідко випадковий або емоційний) акт і кримінально протиправну діяльність як цілеспрямоване здійснення дій для забезпечення свого існування [64]. Злочин – це одиничне явище, злочинність – загальне, а злочинна діяльність – вияв і відображення соціальної сутності злочинів і злочинності як соціального елементу життя суспільства [63]. Крім того, вчені закономірно підсумовують, що у зв'язку зі злочинністю структуру діяльності можна розглядати у двох площинах – горизонтальній та вертикальній. Перша передбачає виокремлення в діяльності таких елементів, як мета, мотив, спосіб досягнення, результат. Горизонтальна площина дає змогу з'ясувати спільне й відмінне між злочином і злочинною діяльністю, що співвідносяться між собою як конкретне та особливе. Друга передбачає виокремлення таких елементів, як дії та рухи. Вертикальна площина дає змогу встановити психологічну сутність злочинного професіоналізму як сукупності вмінь і навичок. Адже саме професіоналізм становить основу кримінально протиправної діяльності та забезпечує її високу ефективність [65].

Аналізуючи проблематику організованої злочинності, професор Л. Аркуша відзначає, що злочинна діяльність – це система суспільно небезпечних діянь і тісно пов'язаних із ними дій, передбачених кримінальним законом, психологічно обумовлених загальною метою. Злочинна діяльність відображає спрямованість особи, її ставлення до оточення, є усвідомленою та вольовою, цілеспрямованою поведінкою, що охоплює різні протизаконні засоби здійснення звичайних видів людської діяльності, а також вид злочинних діянь [8].

У тлумаченні кримінально протиправної діяльності ми поділяємо позицію В. Тіщенка, який вважає, що це заздалегідь спланована та реалізована система дій особи (або організованої групи осіб) з підготовки, вчинення та приховування злочинів, а також дій, спрямованих на ухилення від кримінальної відповідальності, досягнення постійних злочинних результатів, а також розрахована на тривалий проміжок часу [176]. Це визначення обираємо за основу, оскільки в ньому чітко відображено фазовий підхід до кримінально протиправної діяльності. Розглядаючи кримінально протиправну діяльність з позицій структурно-діяльнісного підходу, необхідно дотримуватися таких положень: а) кримінально протиправна діяльність є різновидом людської діяльності; б) злочинною може бути вся діяльність загалом або ж лише окремі фрагменти діяльності, яка загалом може бути правомірною; в) діяльність передбачає різноманітну практичну активність, яка може бути спрямована на досягнення відповідної мети, тобто діяльність реалізується через систему дій, які спрямовані на виконання конкретних завдань і кінцевої мети; г) структурними елементами кримінально протиправної діяльності є: умови вчинення, мотив, потреби, завдання, суб'єкт діяльності з його необхідними навичками для вчинення злочину; д) діяльність необхідно розглядати не статично (описуючи не лише її окремі елементи), а динамічно, пофазово (розглядаючи елементи в розвитку).

На підставі теоретичних положень, а також матеріалів практики видається доцільним виокремити типові ознаки кримінально протиправної діяльності, які відрізняють останню від одиничного злочину. Вважаємо, що до типових ознак кримінально протиправної діяльності слід відносити такі:

– наявність прямого умислу, попереднього задуму й повноструктурного способу (технології) досягнення злочинної мети;

– вчинення на різних стадіях реалізації злочинного умислу дій, які утворюють самостійні склади злочинів. У контексті цього необхідно зазначити, що такі дії можуть бути вчинені не безпосередньо суб'єктом, а й іншими особами, але вони мають бути спрямовані на забезпечення реалізації

злочинного задуму суб'єкта в межах здійснення конкретної форми кримінально протиправної діяльності;

– систематичне вчинення конкретних дій для досягнення злочинного результату та їх відтворення в разі успіху;

– наявність у суб'єкта стратегічної злочинної мети, на яку спрямована кримінально протиправна діяльність, наприклад, побудова кримінальної кар'єри й досягнення відповідного статусу в злочинному середовищі. Загалом концепт побудови кримінальної кар'єри досліджували лише крізь призму загальнокримінальної злочинності, зокрема діяльності рецидивістів і лідерів кримінального середовища. Водночас вивчення практики протидії злочинності, яку вчиняють у кіберпросторі, дає підстави стверджувати, що для осіб, які здійснюють таку злочинну діяльність, типовим є прагнення до побудови кримінальної кар'єри у своєму середовищі, про що свідчить наявність «рейтингів» хакерів тощо;

– створення інфраструктури для забезпечення кримінально протиправної діяльності, зокрема встановлення корумпованих зв'язків тощо;

– вчинення кримінально протиправної діяльності групою осіб. Водночас необхідно зауважити, що цю ознаку можна розглядати як факультативну, оскільки автономна кримінально протиправна діяльність у кіберпросторі є доволі поширеною.

З огляду на викладене, на нашу думку, кримінально протиправна діяльність *економічної спрямованості, яку вчиняють із використанням кіберпростору,* – це систематична, багатоетапна протиправна діяльність особи (групи осіб), яку здійснюють за допомогою використання інформаційних технологій, забезпечують створенням необхідної інфраструктури та яка спрямована проти функціонування фінансово-економічної системи держави, фінансової діяльності юридичних і фізичних осіб.

Вважаємо, що подальший аналіз досліджуваної кримінально протиправної діяльності слід здійснювати крізь призму характеристики її етапів, зокрема: 1) формування задуму щодо здійснення кримінально

протиправної діяльності; 2) підготовка до здійснення кримінально протиправної діяльності; 3) безпосереднє здійснення кримінально протиправної діяльності; 4) приховування слідів кримінально протиправної діяльності.

На переконання науковців, будь-яка осудна особа, зокрема й злочинець, перш ніж перейти до певних дій, спочатку діє подумки. Перед вчиненням певного злочинного діяння у свідомості особи складається в загальних рисах уявлення про сутність злочину, способи його вчинення, формується психологічне ставлення до майбутнього злочинного діяння, злочинного результату у формі досягнення злочинної мети. Усі ці процеси, що відбуваються у свідомості особи, можна назвати формуванням умислу [61].

Зауважимо, що ***формування в особи задуму й умислу*** на здійснення кримінально протиправної діяльності з використанням кіберпростору безпосередньо залежить від таких чинників:

– рівня професійних знань і навичок особи щодо організації фінансово-економічних процесів у кіберпросторі й можливостей використання кіберпростору як інфраструктурної складової для здійснення кримінально протиправної діяльності. Згідно з результатами дослідження О. Тарасенка, майже половина (48,1 %) кіберзлочинців мають вищу (зокрема технічну) освіту, однак факт, що кожен третій злочинець (30,3 %) має загальну середню освіту, вказує на таке: з розвитком комп'ютерних технологій та систем комунікації, їх агресивною ескалацією у всі сфери нашої життєдіяльності дедалі поширенішим стає вчинення кіберзлочинів не фахівцями-комп'ютерниками, а пересічними користувачами кібертехнологій. Досягнення в цій сфері уможливили вчинення кіберзлочинів не за допомогою відповідної освіти, багажу знань і навичок, а на підставі матеріалів відповідних посібників [171];

– можливості застосування особою наявних знань і навичок у легальній сфері. У цьому випадку необхідно акцентувати на наявності прямої залежності між рівнем кваліфікації та рівнем оплати праці;

– становища особи в професійній спільноті та приналежності до груп, які керуються відповідною субкультурою. Як і під час формування мотивації кримінально протиправної діяльності загальнокримінальної спрямованості, особа керується потребою самоствердження та підвищення власного статусу у відповідній спільноті.

Проведене нами дослідження, узагальнені результати якого викладено в додатках до дисертації, засвідчує, що формування задуму на вчинення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору як система мисленнєво-конклюдентних актів охоплює:

а) формування установки на вчинення діяння, відповідальність за яке передбачена законодавством. У цьому випадку йдеться про формування в особи загальної установки щодо можливості порушення закону як прийнятної форми соціальної практики;

б) розумова оцінка власних компетенцій та реальної можливості здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору. Слід зауважити, що в разі несформованості в злочинця впевненості в достатній кількості власних компетенцій та навичок для здійснення кримінально протиправної діяльності в кіберпросторі, особа в переважній більшості випадків не відмовляється від реалізації задуму щодо здійснення кримінально протиправної діяльності, а здійснює на стадії підготовки пошук інших осіб, чиї знання та компетенції можуть бути використані, або осіб, які готові стати співучасниками кримінально протиправної діяльності;

в) оцінка ризиків і переваг від здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору. У контексті цього зауважимо, що стосовно цього виду кримінально протиправної діяльності на особу може бути екстрапольовано положення економічної теорії злочинності, згідно з якою злочинець у своїй мотивації діє аналогічно раціональному економічному агенту, прораховуючи всі ризики та

переваги кримінально протиправної діяльності. Необхідно зауважити, що в поведінці злочинців на цьому етапі спостерігається елемент «ірраціонального» мислення, оскільки вивчення кримінальних проваджень засвідчує, що навіть якщо витрати на вчинення злочину перевищують потенційну вигоду, то 45,8 % злочинців не відмовляються від реалізації злочинного задуму, а здійснюють пошук можливих шляхів оптимізації витрат;

г) остаточне формування умислу й задуму (моделі) подальшої кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору. Слушно зазначають вчені, що злочинцям, які діють у кіберпросторі, притаманний вольовий компонент людської психіки. Можна провести паралелі між вольовою дією особи та її злочинною діяльністю з використанням кіберпростору. По-перше, зловмисник змістовно вчиняє одиничний злочин шляхом елементарної вольової дії або комплекс органічно взаємопов'язаних злочинів шляхом складної вольової дії. По-друге, його діяльність завжди є вмотивованою, причому від складності кримінально протиправної діяльності в кіберпросторі залежить конкуренція мотивів вчинення. Наприклад, злочинець не зміг подолати всі технічні перешкоди на шляху отримання доступу до рахунків біржі криптовалют, тому опинився перед вибором виконати свій корисливий задум частково (заволодіти лише одним видом криптовалют) або пошкодити електронну систему біржі з метою помсти; незаконно отримавши доступ до конфіденційної інформації, злочинець опиняється перед вибором: вчинити заплановане вимагання або інший злочин з його використанням (шахрайство, привласнення, незаконні дії з платіжними картками). Розв'язання проблеми конкуренції мотивів вчинення злочину нерозривно пов'язане із психологічними властивостями злочинця (психотипом). Тому доволі часто банківські установи, ІТ компанії, фірми охорони й технічного обслуговування, добираючи персонал, проводять тестування з метою визначення рівня професіональності, а також психотипу майбутнього працівника. Результати таких тестувань можуть бути цінними для працівників кіберполіції під час первинної перевірки інформації та

слідчого з позицій визначення кола підозрюваних в установі-жертві [158, с. 118].

Аналіз практики роботи підрозділів кіберполіції, зокрема опрацювання 59 різних типів оперативних матеріалів, засвідчує, що розуміння структури формування в особи умислу й задуму на вчинення злочинів економічної спрямованості з використанням кіберпростору має важливе значення в контексті виявлення таких осіб у межах організації оперативного обслуговування окремих напрямів та ліній роботи, а також оперативного (ініціативного) пошуку, оскільки формування умислу й задуму кримінально протиправної діяльності доволі часто, крім психологічно-мисленнєвої діяльності, супроводжується вчиненням певних конклюдентних дій особи у відповідному середовищі.

Продовжуючи аналіз, детальніше розглянемо ***стадію підготовки*** до здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору. Необхідно зауважити, що в межах криміналістики питання підготовки до вчинення злочину досліджено на теоретичному рівні значно ґрунтовніше, ніж проблематика формування злочинного задуму, зокрема й щодо злочинів, які вчиняють із використанням можливостей кіберпростору, крізь призму аналізу способів вчинення таких злочинних діянь [84; 105; 152; 172; 181].

Криміналістичне дослідження способу злочину передбачає з’ясування закономірностей (кореляційних залежностей) його формування, встановлення особливостей злочинних дій, відображення їх у зовнішньому середовищі й те, як ці знання може бути використано для виявлення та розслідування конкретних видів злочинів. Отже, для криміналістики першочерговий пріоритет становлять не результат (як у кримінальному праві), а механізм злочинної дії, певна послідовність його етапів і процесів, зокрема підготування та приховування злочину [52].

Першим структурним елементом кримінально протиправної діяльності економічної спрямованості, яку вчиняють із використанням кіберпростору, є

вибір об’єкта злочинного посягання, що передбачає детальне вивчення інфраструктури його обслуговування. На цій стадії особи можуть додатково залучати й інших спеціалістів у сфері інформаційних технологій, якщо в суб’єкта (суб’єктів) кримінально протиправної діяльності недостатньо власних компетенцій для виконання цього завдання. Є декілька типових способів залучення спеціалістів на цій стадії:

– *спеціаліст у сфері інформаційних технологій, надаючи консультативні послуги, не знає, що бере участь у підготовці до вчинення злочинів.* У таких випадках особа-консультант доволі часто виконує «дружню» послугу знайомому, не вдаючись до з’ясування мотивації його поведінки. Крім того, у практиці роботи правоохоронних органів трапляються випадки, коли до аналізу потенційного об’єкта кримінального посягання залучають неповнолітніх, які мають кваліфіковану самопідготовку у сфері інформаційних технологій. Такий спосіб залучення особи зі спеціальними знаннями та навичками не завжди забезпечує беззаперечне досягнення злочинного результату, оскільки, не знаючи про мету аналізу, останній часто проводить його поверхнево;

– *спеціаліст у сфері інформаційних технологій, надаючи консультаційні послуги, знає, що бере участь у підготовці злочину.* Такий спосіб є «ефективнішим» з позиції досягнення злочинного результату. Згідно з матеріалами практики, такі суб’єкти проводять детальне вивчення об’єкта злочинного посягання. Також спостерігається зміна методів роботи аналітиків кримінальних угруповань й опанування інноваційних концепцій роботи з інформацією, наприклад, використання «великих даних», що передбачає стовідсотковий аналіз усієї наявної інформації стосовно об’єкта з використанням заздалегідь написаних програмних продуктів й алгоритмів.

Вивчення спеціалізованих видань засвідчує, що пошук потенційного об’єкта злочинного посягання відбувається шляхом сканування мережі Інтернет за допомогою спеціалізованого програмного забезпечення. За результатами опитування працівників оперативних підрозділів, у 92 %

випадків виявити підготовчі дії щодо вчинення злочину за допомогою технічних засобів фактично неможливо, тому ефективним є проведення традиційних оперативно-розшукових заходів.

Типовий набір спеціаліста у сфері інформаційних технологій, який використовують під час вивчення об'єкта злочинного посягання, містить: сканери телефонних ліній; зламувачі й генератори паролів, засоби шифрування, а також програмні пакети, які комплексно автоматизують операції зломів (наприклад CiberKit). Традиційно злочинці для визначення апаратних засобів, які мають модемний вхід, використовують спеціалізоване програмне забезпечення (PhoneSweep, Tolenoc), що поступово встановлює зв'язок з телефонними номерами, які знаходяться у відповідному діапазоні. Номери, на які відкликається модем, реєструють у відповідному файлі (аналогічні методи використовують для виявлення вразливих місць комп'ютерів, які підключені до інтернету). Досить часто з цією метою використовують стандартні програми пошуку вразливості мережі й сканувальні програми, які поступово підбирають усі можливі точки доступу до системи з метою визначення оптимального варіанту проникнення.

Серед найпоширеніших інструментів необхідно також виокремити сканери портів комп'ютера, які в автоматичному режимі запитують кожен порт комп'ютера, з'ясовуючи, який з них є відкритим. У цьому випадку комп'ютер автоматично відправляє звіт, надаючи необхідну для аналізу інформацію. Таке «зондування» портів дає змогу виявити ті з них, які є найвразливішими для атак.

Аналіз спеціалізованої комп'ютерної літератури засвідчує наявність значної кількості програм-сканерів, які передбачають різні алгоритми роботи та мають функціональне призначення. Один з найрозвинутіших пакетів CyberCorp Scanner має можливість перевіряти й оцінювати вразливість локальних корпоративних мереж, розширений набір додаткових інструментів для моніторингу ефективних втручань, може перевіряти робочі станції та

сервери, має концентратори, комутатори й охоплює спеціалізовані трасувальники пакетів для перевірки маршрутизаторів.

Традиційно на цьому підготовчому етапі злочинці намагаються отримати доступ до системних паролів, чого можна досягти шляхом перехоплення, підбирання з використанням програмних засобів або типової крадіжки фізичних носіїв з даними. Поширеними в перехопленні залишаються програмні засоби типу «сніффер», які вбудовуються в інші комп'ютери або системи та дозволяють здійснювати моніторинг й аналіз системи протягом тривалого часу без явних ознак кримінально протиправної діяльності.

Наступним етапом є ***формування групи та підготовка засобів.*** Увагу слід спрямувати на методику втягнення в кримінально протиправну діяльність персоналу установ чи організацій, де планується вчинення злочину. Вивчення кримінальних проваджень дає підстави стверджувати, що залучення персоналу до кримінально протиправної діяльності відбувається з використанням:

– погроз (застосування фізичного насильства, оприлюднення компрометаційних матеріалів тощо);

– підкупу (традиційно використовують стосовно працівників професійної ланки, які мають відповідний доступ, а також осіб, у яких є фінансові проблеми);

– інших чинників (інтимні стосунки зі злочинцем, помста керівництву, самоствердження тощо).

Пріоритетними об'єктами для встановлення злочинних зв'язків із персоналом нині є: фінансові структури; провайдери доступу; електронні магазини; міжнародні корпорації; сайти неурядових фінансових організацій.

Вважаємо, що способи сприяння персоналу установи (організації) злочинцям можна згрупувати в три блоки:

– умисне невжиття заходів щодо збереження паролів, іншої конфіденційної інформації та розголошення відомостей щодо конфіденційної інформації, яка знаходиться в мережі;

– невиконання належних заходів захисту, зокрема допуск до роботи в локальних мережах сторонніх осіб;

– неповідомлення керівництву чи правоохоронним органам про виявлені ознаки злочинної активності в мережі.

Основним етапом є ***безпосередня реалізація злочинного задуму.*** Зважаючи на те, що спектр аналізованих діянь є доволі широким, проаналізуємо типові способи реалізації найтиповіших форм кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору.

1. Шахрайства в мережі Інтернет. Поширення шахрайства в мережі Інтернет насамперед пов’язано з появою електронних магазинів, особливості функціонування яких і приваблюють злочинців. Витративши незначну суму на створення інтернет-магазину, можна імітувати законну торговельну діяльність з подальшим вчиненням шахрайських дій щодо споживачів. У практиці роботи правоохоронних органів виявлено випадки, коли злочинці, крім фіктивних інтернет-магазинів, використовують широкий спектр способів заволодіння грошовими коштами шляхом обману, зокрема через:

– псевдосайти благодійних, релігійних організацій тощо, які збирають пожертви;

– спам-розсилання, сайти з проханнями про матеріальну допомогу для лікування тощо;

– сайти фіктивних шлюбних агенцій, окремих віртуальних наречених;

– шахрайські онлайн банки й інвестиційні фонди, які обіцяють значні відсотки за вкладами;

– розсилання та сайти, які повідомляють інформацію про виявлені вразливі місця в платіжних системах, які дають змогу примножити прибуток, переказавши певну суму коштів на рахунок злочинців;

– шахрайські сайти й розсилання, які пропонують віддалену роботу, з перерахуванням початкового вкладу.

Усі перелічені способи мають спільний типовий алгоритм дій злочинців: розміщення інформації в інтернеті – встановлення анонімного контакту з потерпілим – отримання від нього коштів – зникнення з мережі та поява в подальшому за новою IP адресою.

Поряд з типовими способами вчинення цього злочину, необхідно проаналізувати окремі особливості інтернет-магазинів, які засвідчують, що їх створено з метою вчинення злочинів, що дасть змогу значно покращити оперативне обслуговування національного сегменту мережі Інтернет з боку працівників оперативних підрозділів. За результатами вивчення оперативно-розшукових справ й опитування працівників оперативних підрозділів виокремлено блоки відомостей, які свідчать про можливу злочинну мету створення інтернет-магазину:

– явна економія на утримання сайту, рекламі, персоналі, послугах зв'язку тощо (у цьому випадку злочинці не створюють повноцінний магазин, а обмежуються лише «фасадом», дизайн сайту, товарний знак часто запозичені, замовлення обробляють у ручному режимі, не використовують банківські рахунки);

– намагання приховати особу власника там, де її має бути зазначено (під час реєстрації доменного імені, придбання послуг зв'язку, розміщення реклами тощо);

– використання виключно таких способів оплати, які дають змогу приховати дані власника, неможлива оплата кур'єру під час отримання товару;

– період між замовленням товару та його доставкою максимально великий;

– немає товарів економкласу.

Іншим поширеним різновидом шахрайства є заволодіння грошовими коштами за допомогою фішингових сайтів (30 % діянь, кваліфікованих за ч. 3 ст. 190 КК України). Використовують сайти фіктивні, спеціально створені злочинцем з метою отримання від жертви інформації (персональних даних, логінів і паролів, зокрема до систем дистанційного банківського

обслуговування) або безпосередньо безготівкових коштів. Отримавши шляхом уведення в оману доступ до облікових записів жертв, злочинець блокує доступ законних користувачів до акаунтів через змінення паролів, налаштовує систему з власною корисливою метою. Ці технології постійно вдосконалюють, адже злочинець, що вчиняє шахрайство таким способом, є впевненим користувачем, здатним підвищувати власний професійний рівень, може відмовитися від участі в організованій злочинній групі та здійснювати індивідуальну кримінально протиправну діяльність (більше половини злочинців діють одноосібно). Як фахівець високої кваліфікації він використовує технології анонімізації доступу до ресурсів мережі Інтернет, унаслідок чого має високий ступінь географічної мобільності. Жертвами шахрайства стають занадто довірливі або неуважні користувачі, які самі (добровільно) надають конфіденційну інформацію, коли їх просять перейти за електронним посиланням на нібито справжній сайт сервісу, пошти, платіжної системи, сторінки в соціальній мережі тощо, повторити введення пароля, повідомити номер рахунка й пароль для реєстрації покупки або грошового переказу, зареєструватися на фіктивному сайті інтернет-магазину, інтернет-аукціону тощо [76, с. 54].

Крім діянь, які кваліфікують як шахрайство, злочинці розробили й значно складніші технології заволодіння коштами з використанням кіберпростору. Згідно з опрацьованими матеріалами практики, застосовують такі технології зазвичай злочинець – досвідчений користувач та/або злочинець – користувач-професіонал. Така кримінально протиправна діяльність утворюється сукупністю злочинів, передбачених ст. 185 (крадіжка) або ст. 190 (шахрайство) та статей розділу XVI КК України, залежно від суті дії для отримання доступу до інформації (ст. 361 (несанкціоноване втручання) та ст. 361-1 (дії щодо шкідливих програмних чи технічних засобів) або ст. 363-1 (шкідливий спам). Відмітна особливість цієї групи технологій полягає в застосуванні їх організованими злочинними групами.

Кожен учасник кримінально протиправної діяльності за відсутності транснаціонального компонента в такій групі виконує покладену на нього функцію, зокрема зі: 1) створення фіктивного підприємства для маскування кримінально протиправної діяльності; 2) здійснення несанкціонованого втручання в роботу комп'ютерної техніки та дій, спрямованих на забезпечення незаконної транзакції; 3) реалізації механізмів легалізації отриманих безготівкових коштів і переведення їх у готівкову форму. Показовою є діяльність групи осіб у м. Луцьку [28]. *Зокрема, 29 листопада 2012 року група осіб, серед яких не встановлені слідством особи, діючи за попередньою змовою з метою заволодіння чужим майном, маючи спеціальні знання, уміючи користуватися спеціалізованим програмним забезпеченням, призначеним для проникнення в комп'ютер через мережу Інтернет, проникли до системи електронних платежів «Приват24», сформували електронне платіжне доручення від 29 листопада 2012 року за № 1047, у якому зазначили, що Луцьке підприємство електротранспорту здійснює електронний платіж безготівкових коштів у сумі 138 440 грн на рахунок ТОВ «Спектрум Україна». Засвідчивши платіжне доручення електронним підписом для проведення платежу, зловмисники передали його через систему електронних платежів «Приват24» до ВГРУ ПАТ КБ «Приват Банк», яке здійснило перерахування безготівкових коштів у сумі 138 440 грн з рахунка Луцького підприємства електротранспорту на рахунок заздалегідь створеного фіктивного ТОВ «Спектрум Україна». Ці гроші під виглядом законного переказу було переведено на картковий рахунок ТОВ «Спектрум Україна» в ПАТ «Укрсиббанк». З використанням корпоративної картки безготівкові кошти через банкомати було конвертовано в готівку й розділено між співучасниками. Дії організатора цієї злочинної схеми кваліфіковано за ч. 1 ст. 205; ч. 2 ст. 361; ч. 3 ст. 190; ч. 2 ст. 200; ч. 2 ст. 209. У межах досудового слідства також було встановлено вчинення цією особою іншого злочину в кіберпросторі, зокрема передбаченого ч. 2 і 3 ст. 301 КК України.*

Коли йдеться про діяльність транснаціональної мережевої злочинної групи, організатор злочину та сума загального збитку найчастіше залишаються невстановленими. Тому за матеріалами слідчо-судової практики такі злочини кваліфікують лише за сукупністю статей розділу XVI КК України. *Наприклад, у травні 2016 року група осіб вступила у злочинну змову з метою проведення несанкціонованих платіжних операцій з рахунків українських і зарубіжних користувачів через систему миттєвих інтернет-розрахунків «WebMoney Transfer» [27]. Гр. А., маючи спеціальні технічні знання у сфері програмування, в Херсонській області за допомогою невстановленого комп'ютера створив з метою використання й розповсюдження програмне забезпечення за назвою «grafon.apk» і файл «restricted» для мобільних комп'ютерів на базі операційної системи «Android», після чого передав логін і пароль доступу до панелі управління бот-мережею «SexDrugWokrug.apk» зазначеного програмного забезпечення гр. Б. У травні 2016 року за декількома електронними адресами, де знаходилися панелі управління зазначеної бот-мережі, гр. Б. використав і розповсюдив у мережі Інтернет через низку власних сайтів зазначений програмний засіб. Останній, за висновками комп'ютерно-технічної експертизи, є шкідливим програмним забезпеченням («троян»), що встановлюється як звичайна програма й надалі отримує права суперкористувача, працює таємно у фоновому режимі, перехоплює платіжні операції, а також збирає особисті дані користувача. Управління ним здійснюють з віддалених інтернет-серверів, а саме розміщується на вебсайтах вільного доступу. Останні мають ідентичний зміст про нібито додаток до АС «Android» за назвою «SexDrugWokrug.apk», який за описом призначений для пошуку друзів і спілкування, але насправді є шкідливим програмним засобом. Після завантаження на мобільний термінал потерпілого шкідливого програмного засобу «SexDrugWokrug.apk» цю програму встановлюють під виглядом системного процесу як SystemUpdate, а після першого запуску вона вимагає надання додаткових повноважень для доступу до системи. Отримавши*

повноваження, програма видаляє свою «іконку-ярлик» і переходить у фоновий режим, намагаючись з'єднатися із сервером та передати інформацію з електронного приладу жертви. Отримавши дані, програма перевіряє наявність встановленого мобільного банкінгу на телефоні жертви, надсилаючи смс-запити на запрограмовані спеціальні номери, і в разі позитивного результату намагається заволодіти грошовими коштами потерпілого шляхом здійснення несанкціонованих платежів через систему миттєвих інтернет-розрахунків «WebMoney Transfer» [158, с. 158–161].

2. Незаконні дії з платіжними картками. Практика роботи оперативних підрозділів свідчить про наявність декількох способів незаконних дій з платіжними картками. Водночас всім їм притаманні три типові фази вчинення злочину:

– отримання даних щодо платіжних карток різноманітними способами;

– сортування, класифікація та їх реалізація іншим кримінальним угрупованням;

– безпосередня конвертація коштів, які знаходяться на банківській картці, у готівку.

Водночас складність технологічного процесу вчинення таких злочинних дій зумовлює те, що їх завжди вчиняє група осіб, оскільки кожна зі стадій пов'язана з необхідністю наявності спеціальних знань, досвідом у відповідній сфері, посадовим становищем, доступом до апаратних засобів і програмного забезпечення.

Для розроблення ефективного алгоритму протидії злочинам означеної категорії слушно визначити на основі вивчення матеріалів кримінальних проваджень й оперативно-розшукових справ типові способи незаконного отримання даних стосовно пластикових платіжних карток:

– дистанційний неправомірний доступ до сервера, де зберігають чи обробляють такі дані, наприклад, сервера магазину чи банку (зрідка трапляється на практиці – 13 % випадків);

– доступ до даних із використанням посадового становища й недоліків у системі захисту підприємства (спосіб є поширеним, оскільки власники підприємств спрямовують посилену увагу на захист від зовнішніх загроз, нехтуючи внутрішньою інформаційною безпекою підприємства);

– перехоплення трафіку у випадку, коли дані картки передають у відкритому доступі (цей спосіб безпосередньо пов'язаний з віктимною поведінкою потерпілого);

– отримання даних банківських карток або знання дампу під час обслуговування клієнтів у закладах торгівлі й харчування (необхідний безпосередньо фізичний контакт із карткою);

– виманювання даних і PIN кодів за допомогою заходів фішингу;

– фізичне заволодіння карткою шляхом обману потерпілого.

Складнішими є способи безпосереднього отримання готівки з банківських платіжних карток. До найпоширеніших із них належать такі:

– речовий кардинг – придбання в інтернет-магазинах або реальних (фізичних) торговельних точках товарів з метою власного використання, на замовлення, для перепродажу;

– здійснення фіктивних придбань в інтернет-магазинах чи придбання послуг платних сайтів за попередньою домовленістю з їхніми власниками (за допомогою картки здійснюють оплату, після чого частину коштів повертає злочинцю власник сайту);

– гра в інтернет-казино (заздалегідь найняті особи реєструють в інтернет-казино чимало акаунтів на ім'я власника карти, вносять депозит з карти й розпочинають гру, а надалі виводять виграш на інші рахунки). Аналізуючи діяльність інтернет-казино, слід зазначити про певні аспекти, які ускладнюють використання цього способу кримінально протиправної діяльності на сучасному етапі. Доволі часто для виплати коштів казино вимагає підтвердження особи гравця, а також не використовує анонімні системи платежів. Від гравця, який прагне отримати виграш, можуть вимагати вислати скановану копію паспорта й документа, який підтверджує фактичне

місце проживання. В окремих випадках у гравця вимагають номер телефону для підтвердження його особи. Виплату надалі здійснюють на іменний банківський рахунок або за допомогою іменного чека, який відправляють поштою.

Водночас поява нових способів протидії злочинній діяльності змусила модифікуватися останню. У мережі можна знайти послугу виготовлення точних сканкопій паспортів й інших документів, телефонні номери в «благонадійних» країнах із переведенням дзвінків у будь-яку частину світу, банківські рахунки, що приймають кошти, адресовані будь-яким фізичним особам, тощо;

– використання інших інтернет-сервісів, де можливим є отримання коштів, наприклад, перегляд аматорського кіно;

– зняття готівки в банкоматах у випадку наявності PIN коду (виготовляють тверду копію картки – «білий пластик», з якої знімають максимально доступну суму за максимально стислий проміжок часу).

На нашу думку, окремого аналізу потребує характеристика криміногенного потенціалу платежів, які здійснюють через мережу Інтернет. Нині поряд з банківськими платіжними системами й методами, які врегульовані як внутрішнім законодавством України, так і міжнародно-правовими актами, значною є кількість платіжних систем, які не є банківськими й не контрольовані на належному рівні з боку державних органів. Детально не характеризуючи зміст функціонування таких систем, оскільки це питання розглянуто вище, слід зазначити, що всі вони пов’язані відповідною системою посередників, які надають можливість швидко конвертувати кошти й переводити їх з однієї системи до іншої, ускладнюючи тим самим відслідковування та блокування кримінальних транзакцій. Крім того, на підставі аналізу правоохоронної практики доходимо висновку, що є і система вторинних послуг – управління рахунками платіжних систем, введення та виведення коштів, зокрема й анонімно.

Значна кількість мережевих платіжних систем емітують, співпрацюючи з банками, власні пластикові картки, за допомогою яких можна переказувати кошти з подальшим зняттям у будь-якому банкоматі. Для випуску такої карти необхідно надати паспорт або його сканкопію, але перевірку особи здійснюють переважно формально, що дає змогу безперешкодно отримати картку на чуже ім'я. Нині можна впевнено стверджувати про появу ринку таких карток, які вільно продаються в мережі. Така опція надає злочинцям можливість використовувати рахунок «WebMoney» чи «E-gold» для отримання кримінальних платежів, наприклад, прибутків від кардерської діяльності. У такому випадку зараховану на гаманець суму швидко переводять через декілька рахунків на картковий рахунок, використовуючи вебінтерфейс управління рахунком, який забезпечує анонімність користувача. Поширеним стало використання децентралізованих віртуальних криптовалют: Bitcoin (BTC), Litecoin (LTC), Namecoin, Zerocoin, Quark, Megacoin, Namecoin, Peercoin, Worldcoin тощо. Темпи приросту капіталу їх власників становлять у певні дні 100 %, 200 % і навіть 1000 %. Криптовалюта стала одним із видів електронних платіжних засобів для оплати товарів і послуг у мережі Інтернет, її також можна обміняти на реальні гроші.

Моделі, які застосовують злочинці для приховування кримінально протиправної діяльності економічної спрямованості, що вчиняють із використанням кіберпростору, корелюють із рівнем кваліфікації злочинців. Особи, які мають високий рівень підготовки та компетенцій, використовують *універсальні способи* приховування кримінально протиправної діяльності, сутність яких полягає в приведенні відповідної інформаційної системи та середовища вчинення злочину до попереднього стану. Такими способами приховування послуговуються для злочинів, під час яких відбувається незаконне заволодіння незначними, порівняно з обігом фінансової установи, сумами коштів і спрямовуються на: а) суттєве відтермінування виявлення злочину, оскільки незаконне заволодіння такими сумами в разі продовження нормального функціонування інформаційної системи залишається

непомітним; б) забезпечення можливості в разі не виявлення факту вчинення злочину надалі вчинити новий злочин у цій інформаційній системі; в) фактичне знищення всіх слідів кримінально протиправної діяльності. Використання таких універсальних способів приховування кримінально протиправної діяльності економічної спрямованості супроводжується здебільшого застосуванням спеціалізованого програмного забезпечення – rootkit, яке можуть використовувати й на інших стадіях кримінально протиправної діяльності. Відмітною особливістю способів приховування (маскування) кримінально протиправної діяльності економічної спрямованості, яку вчиняють із застосуванням кіберпростору, є застосування електронного блокування, яке можуть використовувати й під час безпосереднього вчинення злочинних дій, його спрямовують на відволікання служб захисту інформації від основного задуманого кримінального правопорушення. Сутність таких дій полягає в одночасному блокуванні системи значною кількістю користувачів з різних місць, тому використання такого способу приховування та маскування характерне для кримінально протиправної діяльності, яку вчиняють в організованій формі.

У контексті цього слушною також видається позиція О. Тарасенка, що на заключній стадії кримінально протиправної діяльності використовують способи зачистки, до яких дослідник відносить: а) способи видалення змін у системі: використання програм віддаленого адміністрування комп'ютерної системи; використання виявлених під час підготовки та вчинення злочину «потайних ходів» у системі для доступу до необхідних ресурсів; б) способи руйнації комп'ютерної інформації: використання руйнівних програмних вірусів; використання програм форматування носіїв інформації [171].

Висновки до розділу 1

1. Розвиток інформаційних технологій зумовив докорінну трансформацію соціально-економічних процесів, зокрема цифровізацію економічних інституцій, що безпосередньо позначилося і на технологіях, структурі й динаміці кримінально протиправної діяльності економічної спрямованості.

Аналіз наукових підходів до сутності інформаційного суспільства засвідчує, що вчені акцентують увагу на трансформації економічних інституцій.

Наукові дослідження цієї проблематики мають певну специфіку, зокрема в частині необхідності їх постійного та безперервного проведення, що зумовлено такими чинниками: 1) постійне розширення переліку кримінальних правопорушень, які можуть бути вчинені за допомогою різних складових інформаційних технологій; 2) безперервна модифікація способів вчинення таких злочинів, що прямо корелює з механізмом слідоутворення і, як наслідок, організаційно-тактичними моделями проведення СРД і НСРД; 3) формування нових типів доказів – цифрових доказів, які постійно видозмінюються та потребують систематичного вивчення.

Розвиток наукового знання за такою траєкторією має логічне пояснення та зумовлений такими факторами: напрацюванням теоретичних моделей і практичних рішень щодо кримінально-правової оцінки та кваліфікації досліджуваної категорії злочинів; напрацюванням слідчої практики щодо розслідування таких злочинів, яка стала основою для наукового аналізу й формування типових моделей їх розслідування.

2. Ваємозв’язки між розвитком кіберпростору й окремими формами кримінально протиправної діяльності у сфері економіки виявляються в таких формах: криміналізація окремих діянь, зумовлена широкомасштабним упровадженням інформаційних технологій та їх структурної складової – кіберпростору у всі форми суспільного життя; якісна трансформація інфраструктури економічної злочинності, що зумовлена перетворенням кіберпростору на невід’ємну складову економічних відносин; трансформація

окремих способів вчинення економічних злочинів у складні технології кримінально протиправної діяльності; якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій; формування цифрових кримінальних ринків. Усі ці напрями знаходяться в системних зв'язках, проте, з огляду на особливості кожного з них, їх може бути досліджено відокремлено з подальшим узагальненням.

Розвиток кіберпростору перетворив його на самостійний елемент інфраструктури економічної злочинності. У переважній більшості випадків як інфраструктурний елемент використовують мережеві системи, створені із соціально корисною метою.

3. Типовими ознаками кримінально протиправної діяльності є: 1) наявність прямого умислу, попереднього задуму й повноструктурного способу (технології) досягнення злочинної мети; 2) вчинення на різних стадіях реалізації злочинного умислу дій, які утворюють самостійні склади злочинів; 3) систематичне вчинення конкретних дій для досягнення злочинного результату та їх відтворення в разі успіху; 4) наявність у суб'єкта стратегічної злочинної мети, на яку спрямована кримінально протиправна діяльність, наприклад, побудова кримінальної кар'єри та досягнення відповідного статусу в злочинному середовищі; 5) створення інфраструктури для забезпечення кримінально протиправної діяльності, зокрема встановлення корумпованих зв'язків тощо; 6) вчинення кримінально протиправної діяльності групою осіб.

РОЗДІЛ 2
ВИЯВЛЕННЯ ЗЛОЧИНІВ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ЯКІ ВЧИНЯЮТЬ З ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

2.1. Організація оперативного обслуговування кіберпростору як складова виявлення злочинів економічної спрямованості

Будь-які форми кримінально протиправної діяльності, які вчиняють з використання кіберпростору, оскільки мають специфічний і недостатньо вивчений механізм вчинення, криють у собі істотну небезпеку для суспільства. Тому, відповідно до п. 21 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», окремим напрямом функціонування кібербезпеки визначено здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення та розкриття злочинів проти миру й безпеки людства, які вчиняють з використанням кіберпростору, розслідування, переслідування, оперативне реагування та протидія кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності в кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях. Отже, перед правоохоронними органами поставлено завдання щодо постійного оперативно-розшукового моніторингу (контролю, оперативного обслуговування) кіберпростору. Це відображено в законах України «Про оперативно-розшукову діяльність», «Про Національну поліцію України» [145], «Про Службу безпеки України» [150], наказах НПУ [138], з цією метою передбачено створення спеціальних підрозділів ДКІБ СБУ та ДКП НПУ.

Підрозділи ДКП, згідно з п. 2.1 Положення про ДКП НПУ, уповноважені на протидію кримінальним правопорушенням, механізмам підготовки, учинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Цю сферу діяльності в Положенні визначено як

«протидія кіберзлочинності». В Україні правові засади боротьби з кіберзлочинами регламентовано насамперед Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП зобов'язані здійснювати ОРД властивими їм методами з метою протидії конвенційним злочинам (відповідальність за які фактично передбачено в ст. 163, 176, 185, 190, 200, 301, 361-1, 363-1 КК України).

Зауважимо, що НП України без деталізації її структурних одиниць, відповідно до §3 Стратегії кібербезпеки України, віднесена до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини й громадянина, інтересів суспільства та держави від злочинних посягань у кіберпросторі, здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Тому щодо протидії іншим, альтернативним Конвенції, злочинам, які вчиняють у кіберпросторі та підслідні слідчим НПУ, завдання ДКП визначено як «сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам НПУ в попередженні, виявленні та припиненні кримінальних правопорушень» [138, с. 9]. З огляду на те, що здійснення ОРД щодо альтернативних Конвенції злочинів згідно з окремими наказами НПУ [136–139] віднесено до компетенції або Департаменту карного розшуку, або Департаменту стратегічних розслідувань, або Департаменту протидії наркозлочинності, то ОРД співробітників структурних підрозділів ДКП обмежується щодо них застосуванням відповідних їх компетенції засобів і методів, спрямованих на своєчасне отримання інформації про злочини, що вчинені в кіберпросторі, або відповідні злочинні наміри. Процес, пов'язаний з організацією надходження такої інформації, визначають категорією «оперативне обслуговування кіберпростору».

На підставі зазначеного вище можна констатувати, що в Україні суб'єктами оперативного обслуговування кіберпростору є структурні підрозділи ДКІБ СБУ та ДКП НПУ.

Згідно з відомчими нормативними актами НПУ, положення щодо здійснення оперативного обслуговування об'єктів, які становлять

оперативний інтерес, містяться в нормах, що регламентують особливості роботи підрозділів за справами контрольно-спостережного провадження. Останні власне є документальною формою відтворення результатів діяльності щодо такого обслуговування, а конкретні умови їх провадження зумовлені оперативною обстановкою на об'єкті обслуговування, територіях або окремих напрямках (лініях) роботи оперативного підрозділу.

Зміст оперативної обстановки часто розглядають крізь призму кримінологічної характеристики злочинів, тобто отримання розгорнутих кримінологічних знань про стан, структуру, динаміку злочинів, їх причини й інші детерміністичні чинники [131]. На підставі такого аналізу визначають найвразливіші об'єкти й ділянки, території, складають прогностичні висновки про кількість, структуру й найімовірніші місця вчинення злочину [109]. Утім цей підхід не відображає спрямованості на визначення та виконання конкретних завдань щодо протидії злочинам, які вчинені в кіберпросторі, адже однією з особливостей глобальної мережі Інтернет як основного засобу створення кіберпростору є відсутність географічних і державних кордонів.

Первинним предметом посягання під час вчинення злочину в кіберпросторі є інформаційний продукт у вигляді інформації, що зафіксована в електронній формі, як результат задоволення потреб користувача. Під час документування ознак інформації як предмета злочину встановлюють осіб, які є власниками, розпорядниками або користувачами цієї інформації [26]. Це стосується і власників (розпорядників) та користувачів інформаційної системи (як сукупності телекомунікаційних мереж і засобів для накопичення, обробки, зберігання та передавання даних [151]), що зазнала кібератаки й була знаряддям вчинення злочину. Тож оперативну обстановку в кіберпросторі буде визначено за сукупністю відомостей про конкретних суб'єктів, діяльність яких пов'язана із захистом, регулюванням та обігом цифрової інформації в магістральних, регіональних чи локальних комп'ютерних мережах, окремих комп'ютерних системах.

Отже, сутність оперативного обслуговування кіберпростору полягає в процесі організації надходження інформації щодо конкретних суб'єктів, діяльність яких пов'язана із захистом, регулюванням та обігом цифрової інформації (у магістральних, регіональних чи локальних комп'ютерних мережах, окремих комп'ютерних системах), що становлять оперативний інтерес.

Дослідники О. Манжай та Є. Жицький на підставі аналізу терміна «оперативне обслуговування» виокремили його дев'ять головних ознак: 1) поєднання активних і пасивних заходів оперативно-розшукового характеру; 2) системність; 3) безперервність; 4) циклічність; 5) визначене коло об'єктів оперативної уваги; 6) пошуковий характер; 7) чітко визначена мета (стратегічна, тактична й оперативна), яка в загальному вигляді може бути представлена як виявлення, попередження злочинів, а також сприяння розслідуванню та відшкодуванню матеріальних збитків; 8) взаємодія суб'єктів – учасників оперативного обслуговування; 9) особливості щодо конкретних напрямів правоохоронної діяльності [104]. Не вдаючись до полеміки щодо сутності для «оперативного обслуговування» кожної з виокремлених авторами ознак, акцентуємо на важливості останньої з них з позицій як ОРД, так і криміналістичної науки.

Чимало вчених, які досліджували проблематику оперативно-розшукової протидії [5; 60; 121; 129] та закономірності виникнення доказів з криміналістичних позицій, обґрунтовували наявність характерних для певної сфери вчинення злочинів особливостей процесу здійснення оперативного обслуговування. Оскільки до предмета криміналістичної науки традиційно відносять закономірності виникнення інформації про злочин та його учасників, то організаційні аспекти отримання такої інформації мають окреме значення в криміналістичних дослідженнях у контексті організації виявлення злочину.

Зазначене дає змогу стверджувати, що фактично оперативне обслуговування кіберпростору є «відправною точкою» для виявлення

злочинів як оперативним підрозділом, так і слідчим з отриманих від оперативного підрозділу матеріалів. Сформована ж унаслідок цього мережа конфіденційних джерел отримання інформації надасть можливість уміло провадити не лише оперативно-розшукові заходи, а й згодом НСРД безпосередньо слідчим.

Як складова ОРД оперативне обслуговування містить елементи організаційного характеру [112; 119], традиційними є рівень оперативного обслуговування; види (принципи) оперативного обслуговування; аналіз стану оперативної обстановки; режим оперативного обслуговування; розстановка негласних працівників й організація функціонування інших джерел інформації. Розглянемо їх крізь призму оперативного обслуговування кіберпростору.

1. Рівень оперативного обслуговування кіберпростору. Його визначають через ієрархічну будову суб'єктів, які здійснюють відповідний процес. Вважаємо, що під час використання системно-структурного підходу до пізнання явища через категорію «рівень» остання повинна насамперед відображати систему, де підсистема вищого рівня має зв'язок із підсистемою нижчого рівня. Цей зв'язок стосовно ДКП відображено в п. 1.4 Положення про ДКП, згідно з яким до складу Департаменту як міжрегіонального територіального органу НПУ входять структурні підрозділи, які діють за міжрегіональним принципом за безпосереднього підпорядкування начальнику Департаменту [138].

На рівні центрального апарату в структурі Департаменту функціонують Сектор національного контактного пункту реагування на кіберзлочини і три управління (Управління протидії злочинам у сфері інтелектуальної власності та господарської діяльності; Управління протидії злочинам у сфері інформаційної безпеки; Управління інформаційних технологій та програмування), які структурно складаються з відділів [140].

На підставі аналізу структури служб, що здійснюють оперативне обслуговування кіберпростору, можна виокремити чотири *рівні обслуговування кіберпростору*:

1) центральний (92 %, п. 4 додатка Б), до якого залучено ДКП, ДКІБ;

2) регіональний (78 %, п. 4 додатка Б) – Управління інформаційних технологій та програмування кіберполіції в східному, південному та західному регіонах;

3) міжрегіональний (59 %, п. 4 додатка Б) – відділи протидії кіберзлочинам в областях, що діють за міжрегіональним принципом у структурі восьми управлінь кіберполіції (Донецьке, Карпатське, Київське, Подільське, Поліське, Слобожанське, Придніпровське, Причорноморське);

4) територіальний (69 %, п. 4 додатка Б) – Управління контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ в областях та його відділи.

2. Види (принципи) оперативного обслуговування кіберпростору. Аналіз матеріалів практичної діяльності оперативних підрозділів засвідчує, що види (принципи) здійснення оперативного обслуговування кіберпростору безпосередньо пов’язані з рівнями обслуговування.

Для центрального рівня оперативного обслуговування кіберпростору характерні об’єктово-галузевий та лінійно-об’єктовий види обслуговування.

Об’єктово-галузевий вид полягає в закріпленні за оперативним співробітником/оперативним підрозділом об’єктів чітко визначеної галузі (сфери) суспільства. Цей вид обслуговування властивий переважно ДКІБ СБУ. З огляду на зміст Стратегії кібербезпеки України та постанови Кабінету Міністрів України від 4 березня 2015 року № 83 «Про затвердження переліку об’єктів державної власності, що мають стратегічне значення для економіки і безпеки держави» [135], ДКІБ СБУ, здійснюючи кіберзахист об’єктів критичної інфраструктури, обслуговує сфери, що мають стратегічне значення для економіки й безпеки держави, зокрема це: оборонна галузь, паливно-енергетичний комплекс, транспортна галузь, агропромисловий комплекс,

сфера телекомунікацій та зв'язку, авіаційна та ракетно-космічна промисловість, машинобудівна промисловість, металургійний комплекс, хімічний комплекс, наукова діяльність, сфера стандартизації, метрології та сертифікації, гідрометеорологічна діяльність, промисловість будівельних матеріалів, фінансово-бюджетна сфера, харчова та легка промисловість, поліграфія, геологорозвідувальна галузь.

Лінійно-об'єктовий вид обслуговування пов'язаний з лінією роботи оперативного підрозділу з виявлення та розкриття конкретних видів злочинів. Термін «об'єктовий» відображає зв'язок виду злочину з конкретним об'єктом, мережеву інфраструктуру якого застосовують для підготовки або вчинення злочину. Цей вид характерний для здійснення оперативного обслуговування структурними підрозділами ДКП [140]. Експериментальним шляхом під час здійснення оперативного обслуговування кіберпростору кіберполіцейські запровадили чотири лінії обслуговування кіберпростору: 1) протиправний контент; 2) платіжні системи; 3) електронна комерція; 4) кібербезпека.

Для регіонального рівня оперативного обслуговування кіберпростору характерним є міжгалузевий вид обслуговування. Утім у кіберпросторі він не буде мати традиційний вигляд. Його зміст полягає в обслуговуванні з використанням комп'ютерних технологій єдиних технологічних ланцюгів діяльності об'єкта або групи об'єктів у кіберпросторі. Ланцюг, що становить оперативний інтерес, можуть утворювати різні об'єкти: конкретні фізичні особи, юридичні особи сфери телекомунікацій, надання різноманітних інтернет-послуг, банківських послуг або платіжні системи.

Міжрегіональному рівню обслуговування кіберпростору властиві як лінійно-об'єктовий, так і міжгалузевий види обслуговування.

По-перше, за оперативними працівниками відділів кіберполіції в областях повинні бути закріплені конкретні об'єкти інформаційно-телекомунікаційної інфраструктури. Інформаційно-телекомунікаційна інфраструктура – це територіально розподілені державні й корпоративні комп'ютерні мережі, телекомунікаційні мережі, системи спеціального

призначення та загального користування, мережі й канали передачі даних, засоби комутації та управління інформаційними потоками [58]. «Територіальна розподіленість», яка забезпечує доступ користувача до віддалених ресурсів і супроводження його діяльності суб'єктом надання телекомунікаційних або інтернет-послуг, зумовила необхідність об'єднання відділів кіберполіції в областях у міжрегіональні управління (Донецьке, Карпатське, Київське, Подільське, Поліське, Слобожанське, Придніпровське, Причорноморське).

По-друге, функції оперативних працівників підрозділу кіберполіції в межах області розподілено відповідно до специфіки діяльності управлінь центрального апарату. Тож для оперативного обслуговування за оперативним працівником відділення кіберполіції в області закріплено один з напрямів роботи в кіберпросторі, а саме: 1) протидія злочинам у сфері електронної комерції; 2) протидія злочинам у сфері обігу протиправного контенту й телекомунікацій; 3) протидія злочинам у сфері платіжних систем; 4) протидія злочинам у сфері інформаційної безпеки.

Територіальному рівню обслуговування властивий зональний (територіальний) вид обслуговування. Функціонування підрозділів СБУ за територіальним принципом надає можливість стверджувати стосовно них саме про цей вид оперативного обслуговування кіберпростору. Управління контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБУ в областях та його відділи здійснюють оперативне обслуговування конкретних об'єктів критичної інфраструктури, що мають стратегічне значення для економіки й безпеки держави та розташовані на чітко визначеній території (область, район).

3. Аналіз стану оперативної обстановки. З огляду на наявну правову базу [133; 141; 144], *інформацію, необхідну для аналізу оперативної обстановки, можна розподілити на три групи*: 1) детермінанти злочинів у кіберпросторі (31 %, п. 5 додатка Б); 2) відомості про власників (або розпорядників) систем (50 %, п. 5 додатка Б); 3) відомості про володільців

інформації в системі (97 %, п. 5 додатка Б); 4) наявні оперативні позиції на об’єкті оперативного обслуговування (99 %, п. 5 додатка Б).

1. Детермінанти злочинів у кіберпросторі. Вчинення злочинів у кіберпросторі детермінують об’єктивно наявні соціальні, технічні та географічні особливості кіберпростору, які злочинець використовує з метою досягнення злочинного результату. Утім акцентуємо увагу на особливостях організації національного сегмента кіберпростору.

У технічному аспекті магістральна мережа Інтернет об’єднує всю планету, пов’язуючи континенти, країни й окремі міста. Магістральні мережі, що передають трафік усередині України, між регіонами й за кордон, обслуговують великі оператори та провайдери. Отже, для передавання трафіка кожного абонента до точки обміну здебільшого використовують магістральні оптоволоконні мережі, будівництво й обслуговування яких потребує значних коштів. Тож великі оператори та провайдери мають інтернет-вузли магістральні лінії в Україні та за її межами; регіональні оператори та провайдери охоплюють своєю мережею регіон, декілька або одну область, більшість із них не мають власної магістральної мережі (наприклад, Воля, Тріолан, Ланет та інші); локальні оператори та провайдери – один або кілька населених пунктів.

Тож обсяги трафіка та кількість магістральних мереж спричиняють конкретні проблеми щодо протидії злочинам у кіберпросторі, зокрема: 1) недостатність людського ресурсу для здійснення оперативного обслуговування національного кіберпростору та забезпечення кібербезпеки національного сегмента інтернету; 2) складність в організації збереження цілісності транзитної інформації, що може містити ознаки вчинення конкретного злочину й відповідно є нетрадиційним слідом його вчинення.

2. Відомості про власників (або розпорядників) систем. На відповідному рівні оперативного обслуговування правоохоронним органам потрібно мати інформацію про володільців інформаційних систем, зокрема кількість і реєстраційні дані операторів та провайдерів, їх договірні й позадоговірні

умови співробітництва, надання доступу до мережевої інфраструктури, терміни дії ліцензій, наявність «сірих провайдерів», обсяги фінансово-господарської діяльності, знати карти покриття, наявність на території зареєстрованих у встановленому порядку організацій, представництв, українських офісів інтернет-сервісів; наявність точок обміну трафіком.

3. Відомості про володільців інформації в системі. Володілець інформації – це фізична або юридична особа, якій належать права на інформацію в інформаційній системі. У значенні інформації вона має форму інформаційного продукту або інформаційного ресурсу (сукупності продуктів, об'єднаних технологією зберігання або передачі даних). Таким ресурсом переважно є вебсайт та електронно-інформаційні системи різного призначення (платіжні системи, автоматизовані системи технологічного виробництва, інформаційно-пошукові, робочі автоматизовані місця тощо) [157]. Тому оператор, провайдер, організації, що надають послуги обміну трафіком або контент-сервісів, власник вебсайту, а також будь-який власник чи розпорядник електронно-інформаційної системи (банк, державні й недержавні установи, платіжні організації та оператори послуг платіжної інфраструктури, будь-які підприємства та організації) є володільцями інформації.

У контексті аналізу оперативної обстановки важливою є наявність в оперативного співробітника інформації щодо єдиного покажчика (Uniform Resource Locator, URL) популярних серед українців інтернет-ресурсів, що пов'язані з відповідними лініями обслуговування, зокрема:

1) ресурсів, призначених для поширення аудіо-, відеопродукції; ресурси порнографічної продукції; специфічні інтернет-спільноти (групи) в соціальних мережах (з метою забезпечення пошуку будь-якого протиправного контенту);

2) «топових» «інтернет-магазинів, інших суб'єктів електронної комерції та забезпечення роботи платіжних систем (що пов'язані зі здійсненням електронних платежів);

3) тематичні інтернет-спільноти/форуми (хакерів; жертв шахраїв, вимагачів; батьків і дітей, що описують «підозрілу» поведінку інших користувачів). *Єдиний покажчик ресурсу* (Uniform Resource Locator, URL) – це загальноприйнятий стандарт запису адреси та вказівки на розміщення ресурсу в інтернеті. З англійської мови його назва (Uniform Resource Locator) означає «універсальний локатор ресурсів». Доволі часто його пов'язують з доменом, адже переведення його у формат IP адрес здійснюють за допомогою системи DNS (Domain Name System). Слід зауважити, що алфавітно-цифрове позначення для вебсайту зручно запам'ятовувати та використовувати не лише користувачам конкретного вебсайту, а й під час моніторингу оперативним співробітником національного контенту інтернету.

4. Наявні оперативні позиції на об'єкті оперативного обслуговування. Насамперед ідеться про оперативні позиції в організаціях надання телекомунікаційних послуг; негласні контакти серед фахівців з організації захисту інформації, інженерів з експлуатації засобів захисту інформації; інспекторів з організації захисту секретної інформації; проєктувальників систем захисту інформації; прикладних і системних програмістів, проєктувальників комп'ютерних мереж й адміністраторів баз даних, що забезпечують агентурне перекриття кіберпростору. Також оперативні позиції в середовищі системних адміністраторів мережі створюють можливість завчасно отримати інформацію про вчинення злочину в кіберпросторі, адже вони є першою ланкою в ланцюгу поширення інформації про кіберінциденти, що відбулися в мережі.

Уваги потребують оперативні позиції серед осіб, відповідальних за безпеку організацій банківських і небанківських платіжних систем, операторів послуг платіжної інфраструктури в Україні. Національний банк України веде відкритий Реєстр щодо платіжних організацій, систем й операторів послуг платіжної інфраструктури в Україні [153]. У ст. 1 Закону України «Про платіжні системи та переказ коштів в Україні» платіжну організацію визначають як юридичну особу, що встановлює правила роботи платіжної

системи, а також виконує інші функції щодо забезпечення діяльності платіжної системи й несе відповідальність згідно із Законом і договором; оператор послуг платіжної інфраструктури – це клірингова установа, процесингова установа й інші особи, уповноважені надавати окремі види послуг у платіжній системі або здійснювати операційні, інформаційні та інші технологічні функції щодо переказу коштів [148]. Вони як власники інформації в системі володіють інформацією про її користувачів, які з позицій сумнівних операцій становлять надалі оперативний інтерес.

5. Режим оперативного обслуговування. Ураховуючи оперативну обстановку в кіберпросторі, вважаємо, що його оперативне обслуговування слід здійснювати в посиленому режимі, що полягає в обов'язковій наявності оперативних позицій на об'єктах, пов'язаних зі сферою телекомунікацій, платіжних систем і в різноманітних інтернет-спільнотах (групах, соціальних мережах, форумах).

6. Розстановка сформованих оперативних позицій та організація функціонування інших джерел інформації. З огляду на зазначену вище інформації щодо оперативної обстановки в кіберпросторі, вважаємо, що пріоритетними об'єктами для формування та розстановки оперативних позицій є: Державна служба спеціального зв'язку та захисту інформації України та підпорядковані їй регіональні органи (управління в областях); Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ); національні оператори зв'язку; національні оператори та провайдери телекомунікацій; регіональні оператори і провайдери телекомунікацій; локальні оператори та провайдери телекомунікацій; «точки обміну трафіком» (організацій, що надають послуги обміну трафіком); представництва, українські офіси глобальних інтернет-сервісів; власники й розпорядники національних інтернет-сервісів; банки (державні й комерційні; центральні, регіональні відділення та їхні філії); платіжні організації, які не є банківськими установами; оператори послуг платіжної інфраструктури; об'єкти критичної інфраструктури (включені до

переліку підприємств, що мають стратегічне значення для економіки й безпеки держави, об’єкти потенційно небезпечних технологій і виробництв); інтернет-ресурси (електронні дошки оголошень, вебсайти, соціальні мережі, форуми тощо).

Згідно з результатами аналізу матеріалів практики, агентурно-оперативна робота в організаційних структурах власників (або розпорядників) системи, володільців інформації дає змогу завчасно отримати інформацію: 1) про користувачів системи, місце й обладнання для здійснення доступу до інформації; 2) про злочини, які готують або вчинені; 3) про злочинні зв’язки особи-користувача; 4) про латентні злочини й осіб, що їх вчинили; 5) про створення та діяльність злочинних груп.

Також технічний персонал власників електронно-інформаційних систем володіє інформацією, що становить оперативний інтерес: 1) про розподілення меж і функцій між структурними підрозділами (відділами, дільницями, службами) з обслуговування точок доступу, окремих будівель, споруд і комунікацій; 2) про конкретних суб’єктів, які здійснювали загальне оперативно-технологічне керування об’єктом, штатне та нештатне обслуговування певного об’єкта; 3) про осіб, що зайняті на конкретному об’єкті, їх характеристики, поєднання не сумісних, з погляду забезпечення інформаційної безпеки, посад, причини звільнення окремих осіб; 4) про кіберінциденти.

Зауважимо, що в деяких випадках на рівнях оперативного забезпечення залучають негласний штатний працівник підрозділу кримінальної розвідки НПУ, який виконує довгострокові (стратегічні) завдання з боротьби зі злочинністю на засадах конспірації. Таку роль можуть виконувати співробітники управлінь інформаційних технологій та програмування ДКП НПУ.

Згідно з п. 1.1 положень про відповідні управління інформаційних технологій та програмування, затверджених наказом Департаменту кіберполіції НПУ від 15 грудня 2015 року № 15 «Про затвердження

Положення про Управління кіберполіції Департаменту», такі управління (у східному, південному та західному регіонах) здійснюють ОРД і надають інформаційно-технологічну допомогу практичним та слідчим підрозділам НПУ й тим, що розташовані на території їх обслуговування. Відповідно до численних наказів про штатні зміни в таких підрозділах, посада співробітника управління визначається як «інспектор кіберполіції (з функціями спецагента)». Їхня діяльність полягає в проведенні заходів, спрямованих на виявлення, фіксацію та аналіз цифрових доказів вчинення кримінальних правопорушень; наданні інформаційно-технологічної допомоги органам досудового розслідування; проєктуванні, розробленні та впровадженні програмних і програмно-апаратних комплексів; накопиченні, аналізі й упровадженні позитивного закордонного та вітчизняного досвіду протидії кіберзлочинам [74]. У структурі такого Управління як на центральному, так і на територіальному рівнях функціонують два відділи (№ 1 та № 2).

Діяльність інспекторів з відділу № 1 спрямована на забезпечення здійснення досудового розслідування, виконання доручень слідчого, пов’язаних з отриманням цифрових доказів.

Інспектори відділу № 2 вживають передбачені законодавством заходи зі збирання й узагальнення інформації стосовно об’єктів, що становлять оперативний інтерес, зокрема сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень. Неофіційно відділ № 2 називають «підрозділом кіберрозвідки». Зазначене пов’язано з тим, що ще за часів функціонування Управління по боротьбі з кіберзлочинністю ДБКТЛ МВС України в його структурі діяв відділ комп’ютерно-технічної розвідки. Відповідно до Положення про Управління по боротьбі з кіберзлочинністю ДБКТЛ МВС України, до основних завдань цього відділу було віднесено організаційне та практичне забезпечення проведення судових експертиз і комп’ютерної розвідки.

У чинних положеннях про управління інформаційних технологій та програмування в східному, південному та західному регіонах не використано термін «розвідка», також немає конкретики щодо функцій, завдань або засобів діяльності відділу № 2. Досі не розроблено положення про управління, що належать до складу Департаменту кіберполіції як центрального апарату поліції. З цих позицій питання співвідношення оперативного обслуговування кіберпростору з «комп'ютерною розвідкою» [109], «кримінальною розвідкою у кіберсфері» [20] або «кіберрозвідкою» потребує конкретизації.

У публікаціях із цієї тематики спостерігається тенденція до ототожнення цих форм діяльності [12]. М. Грібов зазначає, що розвідувальні заходи є інструментальними засобами здійснення як розвідувальної, так й оперативно-розшукової діяльності [42]. І. Козаченко під час визначення оперативного обслуговування посилається на систему контррозвідувальних та інших заходів, що здійснюють оперативні підрозділи (спеціальні служби) для забезпечення захищеності життєво важливих інтересів суспільства від внутрішніх і зовнішніх загроз [70]. О. Манжай та О. Богінський зазначають про так звану подібність, але не тотожність цих інститутів [103]. На їхню думку, діяльність із кримінальної розвідки, яку здійснюють у західних державах, цілком узгоджується з вітчизняним інститутом оперативного обслуговування. Такий висновок вони обґрунтовують наявними особливостями «організації діяльності поліції на основі розвідувальних даних» і різних «моделей поліцейської діяльності» в європейських країнах.

Вважаємо, що впровадження терміна «кіберрозвідка» в Законі України «Про основні засади забезпечення кібербезпеки України» нівелювало такі терміни, як «комп'ютерна розвідка» або «кримінальна розвідка у кіберсфері». У п. 12 ч. 1 ст. 1 цього Закону кіберрозвідку визначено як діяльність, яку здійснюють розвідувальні органи в кіберпросторі або з його використанням. З огляду на те, що в ст. 6 Закону України «Про розвідувальні органи України» [149] немає прямої вказівки на віднесення підрозділів НПУ та СБУ до суб'єктів розвідувальної діяльності, немає правових підстав для використання

терміна «кіберрозвідка» для позначення процесу організації підрозділами НПУ та СБУ надходження інформації про стан оперативної обстановки в кіберпросторі й організації ними негласної роботи.

Фактично спецагентів управлінь інформаційних технологій та програмування ДКП НПУ та співробітників підрозділів аналогічного спрямування в СБУ задіюють для виконання тактичних завдань із зашифруванням приналежності до оперативних підрозділів. Вони впроваджуються в злочинні групи, організовані групи або злочинні організації, де, виконуючи функцію поліцейського «під прикриттям», здійснюють пошук інформації, що становить оперативний інтерес та сприяє викриттю групи осіб/організованої групи, що вчиняють або мають намір вчинити злочин у кіберпросторі.

У теорії ОРД оперативний (ініціативний) пошук є самостійною організаційно-тактичною формою негласної роботи [3]. Заходи оперативного (ініціативного) пошуку – це комплекс конспіративних заходів, що не порушують права та свободи громадян, їх здійснює оперативний працівник (підрозділ) кримінальної або спеціальної поліції НПУ, спрямований на виявлення, запобігання та припинення кримінальних правопорушень, установлення місцезнаходження розшукуваних осіб, відповідно до чинного законодавства.

З метою протидії злочинам, вчиненим у кіберпросторі, традиційним є застосування таких заходів оперативного пошуку: інформаційно-аналітичне прогнозування; розвідувальне опитування (технічного та банківського персоналу; осіб – учасників загального діалогу в інтернеті («чату») у формі «прихованого діалогу»); оперативне ототожнення осіб, предметів і речовин (за фото-, відео, що розміщені в мережі); особистий пошук й оперативний огляд публічно доступного місця (у формі радіотехнічного обстеження).

Акцентуємо увагу на інформаційно-аналітичному прогнозуванні. Такий захід полягає в цілеспрямованому пошуку й отриманні інформації загального користування з телекомунікаційних мереж та інформаційних систем, інших

джерел з метою виявлення негативних тенденцій щодо рівня злочинності та відомостей криміногенного, кримінального характеру. Зокрема, присутність у ролі звичайного користувача працівника кіберполіції в тематичних інтернет-спільнотах (групах) і користування певними інтернет-ресурсами дають змогу виявити осіб та факти, які становлять оперативний інтерес. Такі інтернет-ресурси та спільноти/форуми можуть бути різної тематики («хакерство»; «наркозалежність»; «глядачі порнопродукції»; «жертви шахраїв і вимагачів»; «групи батьків і дітей, що описують «підозрілу» поведінку інших користувачів тощо); електронна комерція (інтернет-магазини, «дошки оголошень», поширення аудіо-, відеопродукції, порнопродукції); «соціальні комунікації» («топові» в Україні та на рівні регіонів соціальні мережі); «сепаратизм», «національні меншини» тощо.

Після виявлення інформації, що становить оперативний інтерес, слід визначити ідентифікуючі відомості джерела цієї інформації, зокрема IP адресу. Якщо для визначення постійної IP адреси є інтернет-сервіси (наприклад «https://2ip.ua/ru/») або програми («Magic Net Trace»), які дають змогу визначити її без спеціальних знань, то визначення динамічної адреси часто потребує застосування спеціальних технічних методів: через передачу файлу; застосування онлайн програми «сніффер» (web sniffer (eng) і методів соціальної інженерії, складніших технічних (кібернетичних) методів. Для автоматизації процесу аналізу одержаного переліку IP адрес також послуговуються спеціалізованим програмним забезпеченням і сервісами [103]. Деякі науковці акцентують на можливості використання шкідливих програмних засобів. Наприклад, Ю. Нізовцев зауважує про недостатній рівень регламентації процедури використання таких засобів і подальшої легалізації отриманої в такий спосіб інформації. Для підтвердження достовірності отриманих таким шляхом відомостей науковець пропонує документувати весь процес роботи засобу та його оператора (оперативного співробітника) з подальшим підписанням зазначеної інформації та здобутих даних за допомогою електронного цифрового підпису [114]. Цю пропозицію поки що

не реалізовано. Ми змушені визнати, що фактичні дані, які вказують на наявність ознак вчинення або готування кримінального правопорушення з використанням обстановки кіберпростору, здобуті внаслідок застосування технічних методів оперативного обслуговування кіберпростору, є достовірними лише з позицій носія спеціальних знань у сфері комп'ютерних технологій. Цю тезу підтвердили 90 % анкетованих співробітників кіберполіції.

В умовах браку уваги держави до проблеми забезпечення слідчих підрозділів спеціалізованими для розслідування кіберзлочинів кадрами, інспектори ДКП формально оформлюють достовірно відому оперативну інформацію про вчинений злочин (що була отримана під час негласної роботи в процесі здійснення оперативного обслуговування технологічних ланцюгів діяльності об'єкта/ів у кіберпросторі) як матеріали попередньої перевірки. Або ж формально ініціюють безальтернативну форму початку провадження, тобто через звернення осіб, з якими встановлено конфіденційне співробітництво, з повідомленням про вчинений злочин. Останній у кримінальному провадженні «відходить на другий план», що працює на користь сторони захисту. Якщо ж оперативний підрозділ намагається ініціювати звернення до слідчого з боку потерпілого, то з різних причин цей суб'єкт може намагатися приховати інформацію з приводу своєї ролі в події злочину, що унеможливлює встановлення всього комплексу злочинів у злочинній діяльності конкретної особи.

Вважаємо, що з метою оптимізації виявлення системної кримінально протиправної діяльності в кіберпросторі для подальшого розслідування нетяжких і середньої тяжкості таких злочинів можна рекомендувати слідчому під час отримання ініціативного рапорту структурних підрозділів ДКП НПУ про безпосередньо виявлений ними під час оперативного обслуговування кіберпростору факт вчинення злочину, відмовитися від «альтернативної» форми початку кримінального провадження і застосувати «безальтернативну» форму, тобто внести відповідну оперативну інформацію до ЄРДР або, за

умови наявності обґрунтованих перешкод для початку провадження (наприклад, за небажання потерпілого звертатися до правоохоронного органу або за відсутності фактичного повідомлення про злочин), максимально сприяти реалізації матеріалів перевірки підрозділами ДКП НПУ.

Також акцентуємо увагу, що отримана під час роботи оперативних позицій інформація є не єдиною складовою загального масиву оперативно-розшукової інформації, окремого значення набувають і гласні її джерела. Однак, з огляду на те, що оперативне обслуговування кіберпростору співробітниками ДКП НПУ та ДКІБ СБУ є важливою умовою надходження первинної інформації про злочин або злочинні наміри особи, що діє в кіберпросторі, вважаємо за доцільне розглянути гласні джерела інформації в контексті попередньої перевірки інформації про вчинення кримінального правопорушення або підготовку до його вчинення в кіберпросторі.

2.2. Організація і тактика оперативного (ініціативного) пошуку ознак кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору

Одним із ключових завдань оперативних підрозділів, незалежно від їх функціональної спрямованості, є своєчасне виявлення та документування фактів кримінально протиправної діяльності з метою подальшої реалізації таких матеріалів у формі початку кримінального провадження. Вивчення матеріалів практики засвідчує, що понад 75 % кримінальних проваджень щодо кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, розпочинаються за матеріалами оперативних підрозділів. Проведене нами дослідження на базі діяльності підрозділів кіберполіції дає підстави стверджувати про наявність двох моделей реалізації оперативної інформації про кримінально протиправну діяльність економічної спрямованості, яку вчиняють з використанням

кіберпростору: *по-перше*, виявлення та документування такої кримінально протиправної діяльності працівником оперативного підрозділу з подальшим поданням рапорту з відповідними матеріалами керівнику слідчого підрозділу (100 %, п. 6 додатка Б); *по-друге*, документування такої кримінально протиправної діяльності в межах оперативної розробки із залученням слідчого для надання методичної допомоги (99 %, п. 6 додатка Б). У контексті цього необхідно зауважити, що відсутність у системі НПУ достатньої кількості слідчих, які є фахівцями з розслідування кіберзлочинів, а також надмірна завантаженість працівників слідчих підрозділів призводять до того, що другу модель використовують здебільшого в таких випадках: а) документування багатоепізодних злочинів економічної спрямованості, які вчиняють з використанням кіберпростору; б) документування кримінально протиправної діяльності злочинних угруповань, які здійснюють таку злочинну діяльність.

З огляду на викладене, можна констатувати, що ініціативна робота працівників оперативних підрозділів є ключовою формою виявлення злочинів цієї категорії, яка відповідає принципу наступальності як одному із центральних спеціальних принципів ОРД. Зазначене актуалізує необхідність у межах нашого дослідження детальніше проаналізувати організацію і тактику оперативного (ініціативного) пошуку кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, як самостійної організаційно-тактичної форми ОРД.

В умовах сьогодення пошук є одним з основних напрямів діяльності оперативних підрозділів кіберполіції в протидії злочинній діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору. Означене випливає з аналізу Закону України «Про оперативно-розшукову діяльність», ст. 1 якого визначає, що основним завданням ОРД є пошук і фіксація фактичних даних про протиправну діяльність окремих осіб чи груп. Ця норма має бланкетний характер і для конкретизації завдань ОРД відсилає до інших нормативно-правових актів. Однак аналіз її дає достатні підстави вважати, що серед головних завдань ОРД законодавець виокремлює пошук і

фіксацію фактичних даних. Тож слушною є думка науковців, які зазначають, що ОРД правоохоронних органів України має розвідувально-пошуковий характер, оскільки особи, стосовно яких її здійснюють, вдаються до хитрощів, щоб зберегти в таємниці підготовчий характер своїх неправомірних дій, приховати його сліди та врешті-решт приховати факт вчиненого злочину з метою уникнення кримінального покарання. Цією обставиною і зумовлена різноманітність сил, засобів і методів, за допомогою яких проводять конкретні дії в боротьбі зі злочинністю [113, с. 16–17]. Для реалізації основних завдань щодо протидії злочинності теорія та практика ОРД розробила й апробувала конкретні організаційно-тактичні форми: оперативний пошук, оперативну розробку та оперативно-розшукову профілактику. Зазначені організаційно-тактичні форми різняться за змістом і завданнями, а також тактикою застосування сил, засобів та методів ОРД.

Принагідно зауважимо, що в межах теорії ОРД сутність і зміст оперативного (ініціативного) пошуку досліджували чимало науковців [16; 17; 31; 32; 166; 167; 196]. Зважаючи на викладене, у межах нашого дослідження ми не акцентуємо увагу на характеристиці оперативного пошуку як самостійної організаційно-тактичної форми ОРД, а проаналізуємо лише окремі теоретичні положення.

У гносеологічному розумінні пошук, про що цілком слушно зазначає В. Німчик, – це початкова стадія пізнавального процесу знайдення істинного об’єкта [116].

Оперативний пошук передбачає отримання та перевірку первинної інформації про осіб і факти, що становлять оперативний інтерес, поза зв’язками з конкретною особою чи фактом з подальшим виокремленням їх із загальної маси. Таку форму використовують для розкриття та попередження злочинів за принципом «від злочинця до злочину». У цьому полягає одна з головних відмінностей оперативного пошуку від заходів за матеріалами оперативної розробки, які завжди проводять за конкретними фактами чи стосовно конкретних осіб.

Аналіз наявних наукових підходів дає підстави виокремити основні ознаки оперативного (ініціативного) пошуку:

– оперативний пошук передує оперативній профілактиці й оперативній розробці (87 %, п. 7 додатка Б);

– об’єктами оперативного пошуку є особи, предмети та події (факти), які є джерелами оперативної інформації (71 %, п. 7 додатка Б);

– основним критерієм віднесення особи, події та предмета до об’єктів оперативного пошуку є те, що вони становлять оперативний інтерес для оперативних підрозділів правоохоронних органів, а первинна інформація про них є оперативно значущою для цих підрозділів (69 %, п. 7 додатка Б);

– оперативний пошук здійснюють поза зв’язком з конкретною особою або фактом, конкретною справою оперативного обліку, виконанням окремих завдань, виявленням і розслідуванням окремих злочинів уже відомими фактами й особами (99 %, п. 7 додатка Б);

– здійснення оперативного пошуку ґрунтується на потенційній можливості розпізнання об’єкта пошуку за попередньо відомими ознаками, що властиві саме цим, ще не відомим об’єктам пошуку, які підлягають встановленню в процесі його здійснення (90 %, п. 7 додатка Б);

– основними завданнями оперативного пошуку є отримання первинної інформації про осіб, предмети, події (факти), які становлять оперативний інтерес, а також перевірка цієї інформації для встановлення ознак злочину чи спростування інформації про нього (98 %, п. 7 додатка Б);

– зміст оперативного пошуку становить постійна, активна, цілеспрямована пошукова робота, яка є системою розвідувально-пошукових заходів, що здійснюють як особисто суб’єкти пошуку (особистий пошук), так і з залученням до нього відповідних сил і засобів, зокрема інформаційних систем (66 %, п. 7 додатка Б);

– підставою для початку пошуку первинної оперативно значущої інформації слугує законодавчий припис (69 %, п. 7 додатка Б);

– для проведення розвідувально-пошукових заходів достатньо лише припущення щодо підготовки або вчинення злочину за наявністю окремих ознак, що вказують на такі діяння або на осіб, які готують, вчиняють чи вчинили злочин, причому таке припущення може мати характер версії, що ґрунтується на певних фактах (86 %, п. 7 додатка Б);

– оперативний пошук здійснюють у місцях найімовірнішого виявлення об’єктів пошуку, а саме: там, де криміногенні процеси мають тенденцію до повторюваності, регулярності виявів у часі та просторі, де ймовірною є поява осіб, які готують, вчиняють чи вже вчинили злочин, і спостерігається концентрація кримінального контингенту; час і місце оперативного пошуку залежно від обставин визначають суб’єкти пошуку й відповідні приписи (функціональні обов’язки, вказівки, плани тощо) (51 %, п. 7 додатка Б).

Не заперечуючи наявних у наукових джерелах підходів до цієї проблематики, вважаємо, що оперативний пошук є ініціативною діяльністю оперативного підрозділу чи його працівника з виявлення осіб і фактів, які становлять оперативний інтерес, поза межами конкретної оперативно-розшукової справи і має пошуково-розвідувальний характер. Проте на сучасному етапі актуальності набуває не лише виявлення осіб і фактів, що становлять оперативний інтерес, а й отримання різнопланової інформації, аналіз і структурування якої дасть змогу визначити тенденції розвитку криміногенних процесів у певних сферах суспільного життя, оскільки відповідні підрозділи, що здійснюють ОРД, зобов’язані вживати всіх необхідних оперативно-розшукових заходів щодо попередження, своєчасного виявлення, припинення та документування злочинів, викриття причин та умов, що сприяють їх вчиненню, здійснювати профілактику правопорушень.

Оперативний пошук передбачає декілька самостійних етапів, які знаходяться у відповідних взаємозв’язках, але мають відповідний рівень завершеності:

– постановка завдання та формування (інформаційної) моделі об’єкта пошуку, що містить загальні відомості про риси та властивості об’єктів

пошуку (ознаки розпізнання), їх вияви в зовнішньому середовищі (пошукові ознаки) (92 %, п. 8 додатка Б);

– здійснення конкретного комплексу пошуково-розвідувальних заходів з метою виявлення конкретного об’єкта, що становить оперативний інтерес (59 %, п. 8 додатка Б);

– перевірка й оцінювання отриманої первинної інформації про об’єкт, що становить оперативний інтерес, а також прийняття відповідного рішення за результатами перевірки (100 %, п. 8 додатка Б).

Аналізуючи особливості оперативного (ініціативного) пошуку ознак кримінально протиправної діяльності, яку здійснюють з використанням кіберпростору, необхідно зауважити, що це складна системна діяльність, здійснювана належним суб’єктом у взаємодії з іншими офіційними та неофіційними суб’єктами в межах законодавства України, що спрямована на пошук фактичних даних про протиправні діяння, відповідальність за які передбачена КК України. Оскільки виявлення інноваційних форм кримінально протиправної діяльності у сфері економіки потребує використання інноваційних знарядь і засобів, слід переосмислити організаційні принципи їх функціонування. Зокрема, постає необхідність теоретичного й науково-методичного розроблення питань організації і тактики оперативного пошуку ознак вчинення злочинів у сфері інформаційних технологій, визначення пріоритетних напрямів пошукової роботи оперативних підрозділів, необхідність окреслення кола цифрових об’єктів оперативного пошуку в національному сегменті мережі Інтернет.

Попри наявні проблеми, зазначає М. Літвінов, перед оперативними підрозділами завжди постає завдання з виявлення, попередження та розкриття злочинів, які дедалі ускладнюються, якщо робота пов’язана з новими видами злочинів, зокрема з використанням комп’ютерної техніки. Остання стала необхідністю повсякденного життя та встановлює власні правила щодо роботи, взаємодії людей та їх поведінки [95, с. 86–87]. Крім того, у боротьбі з інноваційними формами кримінально протиправної діяльності не завжди

спрацьовує традиційна тактика, зокрема пошук за способом вчинення злочину, прикметами злочинця та предметами, які вилучені під час огляду місця події. Досліджуючи окремі форми кримінально протиправної діяльності, які супроводжуються використанням кіберпростору, можна виокремити значну кількість чинників, які ускладнюють оперативний пошук у цій сфері: *по-перше,* з упровадженням у суспільне життя комп'ютерних технологій до сфери кримінально протиправної діяльності залучають об'єкти нетрадиційної природи; *по-друге,* кримінально протиправна діяльність у сфері комп'ютерних технологій виявляється в нових, не звичних для правоохоронної практики формах, способах тощо (вчинення кримінальних правопорушень із використанням інформаційних ресурсів, які територіально розміщені в різних країнах, що ускладнює проведення оперативно-розшукових заходів; неможливим є виявлення та фіксування слідів кримінально протиправної діяльності без використання спеціальних знань і відповідних програмно-технічних засобів); *по-третє*, працівник оперативного підрозділу не завжди володіє спеціальними знаннями щодо того, як ознаки шахрайських дій у сфері комп'ютерних технологій можуть відображатися в електронному середовищі (вияви високотехнологічної злочинності та її характер створюють ситуацію, коли працівник оперативного підрозділу самостійно не може виконати низку завдань, що виникають під час виявлення та фіксації інформації; постає необхідність використання можливостей операторів і провайдерів, що здійснюють системний моніторинг параметрів функціонування інформаційних та телекомунікаційних мереж, процесингових центрів, що забезпечують контроль за операціями на персональних комп'ютерах); *по-четверте*, у частині випадків оперативний пошук здійснюють за принципом «від факту злочину до особи», а в інших випадках – за схемою, яка є характерною для виявлення економічних злочинів «від конкретної особи до вчиненого злочину».

Зі всіх можливих дій оперативного працівника, зумовлених конкретним злочином й оперативно-тактичною ситуацією, що склалася на початковому

етапі, оптимальним є лише певний перелік дій, який варіює в незначних межах. Кожен оперативний працівник має в певному випадку виконати чіткий набір схожих дій, перелік яких є об'єктивно зумовленим і не залежить від конкретних суб'єктивних чинників. У них має бути мінімальна кількість суб'єктивного, оскільки зумовлені вони об'єктивними передумовами – обставинами вчинення конкретного злочину й оперативно-тактичною ситуацією, що склалася. Виявлення злочинів як специфічний вид діяльності передбачає організацію та проведення цілеспрямованих комплексів оперативно-розшукових заходів, успішна реалізація яких має забезпечити досягнення необхідного результату, тобто реалізацію завдань, що виникають. У зв'язку із цим виявлення кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, потребує розроблення чіткого алгоритму дій працівників оперативних підрозділів, що ґрунтуються, зокрема, на використанні апаратних засобів і програмного забезпечення.

Формування конкретних алгоритмів, які використовують у боротьбі зі злочинністю, було започатковано в межах криміналістичної науки й ОРД. Працівник оперативного підрозділу, зазначає С. Ніколаюк, щоразу розробляє певний порядок дій, який формально можна визначити як алгоритм. Тож теорія ОРД має науково обґрунтувати максимальну кількість алгоритмів для забезпечення перекриття всіх можливих оперативно-тактичних ситуацій [115]. Слід зосередити увагу на органічний взаємозв'язок таких проблем, як індивідуалізація і типізація діяльності оперативного працівника у відповідній оперативно-тактичній ситуації. Ми поділяємо позицію Д. Цехана, який зазначає, що *алгоритмізація оперативно-розшукової діяльності* передбачає розробку відповідних алгоритмів. У ширшому значенні – це підхід до виявлення та документування кримінально протиправної діяльності, ґрунтований на автоматичній пропозиції працівнику оперативного підрозділу оптимального варіанту, залежно від оперативно-тактичної ситуації, рішень переважної більшості питань, що перед ним постають. Важливо враховувати

ключову функціональну особливість оперативно-розшукового алгоритму – він обов'язково має залежати від вихідних даних, які, власне, і становлять сутність оперативно-тактичної ситуації [186, с. 77–78].

Безпосередньо аналізуючи алгоритми оперативного пошуку ознак кримінально протиправної діяльності, яку здійснюють з використанням кіберпростору, на нашу думку, такий аналіз необхідно проводити в розрізі їх конкретних форм.

Насамперед зауважимо, що, розпочинаючи пошукову роботу з виявлення ознак кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, працівнику оперативного підрозділу необхідно чітко окреслити сфери пошуку, якими здебільшого є: конкретні ЕОМ, комп'ютерні системи й мережі, глобальні інформаційні мережі, суб'єкти господарської діяльності, які надають інтернет-послуги, тощо. Крім того, вагоме значення на початковому етапі реалізації будь-якого алгоритму мають попередній збір і накопичення інформації, а така її систематизація про осіб, які становлять оперативний інтерес (відрізняються окремими видами девіантної поведінки), і фактичних даних, що вказують на різноманітні ознаки таємної, з елементами маскування, їхньої протиправної діяльності.

Щодо злочинів досліджуваної категорії первинними сигналами про протиправну діяльність можуть бути: а) скарги користувачів мережі Інтернет на протиправні дії інших (71 %, п. 9 додатка Б); б) стрімке збагачення програмістів-професіоналів, які знаходяться в полі оперативної уваги працівників оперативних підрозділів (38 %, п. 9 додатка Б); в) сигнали про пошуки в інтернет-середовищі незаконних шляхів для розвитку торгової діяльності від е-комерції (41 %, п. 9 додатка Б); г) пропозиції щодо вчинення злочинних угод, фінансових афер (16 %, п. 9 додатка Б); д) замовлення на розробку спеціального програмного забезпечення, інформацію про реквізити (дані) банківських платіжних систем (72 %, п. 9 додатка Б).

Постійний моніторинг таких ознак необхідний для визначення криміногенного потенціалу цієї сфери господарської діяльності та національного сегменту мережі Інтернет.

Алгоритм оперативного пошуку ознак кримінально протиправної діяльності інтернет-магазинів. Головним завданням першого етапу є збір первинної інформації щодо функціонування інтернет-магазину, що свідчить про незаконну господарську діяльність чи вчинення шахрайських дій у кіберпросторі. Початковою стадією цього етапу є оцінка оперативної обстановки та виявлення найбільш криміногенних секторів функціонування інтернет-магазинів з відповідною класифікацією за такими ознаками: 1) фізичне розташування інтернет-магазину; 2) група товарів, які реалізують через магазин; 3) форми оплати товару; 4) спосіб доставки товару й отримання коштів. На цьому етапі, на нашу думку, слушним є використання оперативно-розшукової діагностики, яка, на думку вчених, виконуючи роль спеціального методу пізнання, дає змогу виявляти ознаки та сліди об'єктивної сторони складу злочину. Її можна ефективно здійснювати на основі економічної інформації, яка після її сприйняття суб'єктом ОРД, а саме аналізу, осмислення та виявлення в ній ознак кримінально протиправної діяльності, може трансформуватися в оперативно-розшукову [45, с. 150].

Отримання такої первинної інформації потребує організації оперативними підрозділами оперативного обслуговування національного сегменту мережі Інтернет, зокрема з використанням статичних об'єктів постійного збирання інформації та моніторингу оперативної обстановки. З цією метою може бути використано таке програмне забезпечення: i2 Limited, Lexis Nexis, Microsoft, MicroStrategy, Visual Analytics та Xanalys. Попри те, що означені програмні продукти істотно різняться архітектурою, водночас вони мають зрозумілий інтерфейс і працюють за принципом «об'єкт–зв'язок», функціонально призначені для виконання тотожних завдань. Деякі програмні продукти, зокрема Analyst's Notebook, рекомендовані Інтерполом як стандарт у галузі кримінального аналізу й можуть виконувати такі завдання: 1) фіксація,

узагальнення або структуризація оперативно-розшукової інформації (візуалізація даних незалежно від обсягу та формату); 2) класифікація джерел оперативно-розшукової інформації; ефективна групова робота за обраним напрямом діяльності; 3) створення схем послідовності подій; 4) виявлення прихованих зв'язків між об'єктами та подіями, що становлять оперативний інтерес; 5) обмін фіксованими результатами аналізу між оперативними підрозділами (зокрема обмін даними з відкритою категорією доступу під час взаємодії із зарубіжними поліцейськими структурами).

Наступним сегментом реалізації алгоритму є аналітичне опрацювання отриманої інформації, що має ключове значення, оскільки без виокремлення відповідних ознак, які характеризують певний об'єкт, будь-яка інформація про нього не становитиме жодного інтересу, вона буде «мертвою». Ознаки є засобом взаємодії між суб'єктом та об'єктом аналітичної діяльності. Вони дають змогу розпізнати відповідний об'єкт і належно дослідити його. Вивчення та узагальнення матеріалів практичної діяльності оперативних підрозділів кіберполіції та проведене дослідження засвідчують, що традиційно аналіз отриманої інформації здійснюють за трьома напрямами: 1) аналіз суб'єкта господарської діяльності (інтернет-магазину); 2) аналіз контрагентів (ключових партнерів у бізнесі); 3) аналіз особливостей руху товарно-матеріальних цінностей.

Під час реалізації ***першого напряму*** з'ясовують:

– наявність у власника установчих та інших документів, що регламентують роботу інтернет-магазину;

– компаративістський аналіз цінової політики магазину як у національному сегменті мережі, так і в іноземних сегментах;

– визначення пріоритетної товарної групи, яку реалізують у магазині;

– визначення та аналіз основних постачальників товару;

– ідентифікація інтернет-магазину та його контрагентів (визначення статусу юридичної або фізичної особи, адреси, контактних телефонів, посадових осіб і засновників, фінансово-майнового становища фізичних осіб,

участі в інших АПД, притягнення до відповідальності, 1-ДФ фізичних та юридичних осіб, банку, що здійснює обслуговування).

У межах ***другого напряму*** реалізують такі завдання:

– визначення та відпрацювання ризикових операцій (контрагентів);

– аналіз зовнішньоекономічної діяльності підприємств (юридичних і фізичних осіб), задіяних у схемі роботи інтернет-магазину;

– аналіз руху товарів за допомогою бази реєстру податкових накладних;

– схема товарно-грошових потоків інтернет-магазину;

– визначення та аналіз основних постачальників товару;

– визначення та аналіз основних покупців товарів;

– серед основних контрагентів визначення складів і перевізників (вибір за КВЕДом).

Третій напрям передбачає реалізацію таких завдань:

– аналіз ціни (від митниці через гуртових покупців і дистриб'юторів до інтернет-магазину, визначення реальної маржі, яку отримує інтернет-магазин);

– ідентифікація товару – обсяг, країна, сертифікація.

Також необхідно використовувати алгоритм відпрацювання імпортерів і суб'єктів господарювання з ознаками фіктивності, які задіяні в схемах реалізації товарно-матеріальних цінностей через інтернет-магазини, з метою протидії незаконному використанню податку на додану вартість.

Водночас аналіз практики протидії злочинній діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, на нашу думку, потребує включення до запропонованого алгоритму інших напрямів, серед яких:

– аналіз програмно-технічної інфраструктури функціонування інтернет-магазину для з'ясування:

– конкретний провайдер, який надає відповідні послуги інтернет-магазину (територіальне розташування, можливість отримання інформації,

визначення наявних агентурних можливостей серед працівників компанії, практика співпраці провайдера з правоохоронними органами тощо);

– програмні продукти, які використовують для роботи інтернет-магазину (особливість конкретних програмних продуктів, зумовлює вибір засобів оперативно-технічного документування кримінально протиправної діяльності інтернет-магазину);

– вид і характеристика платіжних систем, які використовують під час розрахунків, що також дасть змогу розробити ефективну модель подальшого документування кримінально протиправної діяльності;

– визначення програмних комплексів і технічних засобів, які необхідні для подальшого документування кримінально протиправної діяльності інтернет-магазину;

– з'ясування необхідності залучення додаткових сил для подальшого документування діяльності інтернет-магазину (спеціалістів у сфері інформаційних технологій, бухгалтерів, агентів-консультантів тощо).

Поряд із цим, на нашу думку, під час оперативного пошуку ознак кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, необхідним є створення ***організаційної моделі подальшого документування кримінально протиправної діяльності***. Виконання такого завдання також потребує алгоритмізованої аналітичної роботи, оцінки та вирішення таких питань:

– чи достатньо власних сил і засобів для документування кримінально протиправної діяльності;

– якщо власних сил і засобів недостатньо, то які внутрішні допоміжні підрозділи необхідно залучити, а також потенційних суб'єктів зовнішньої взаємодії, наприклад, підрозділів СБУ чи Департаменту стратегічних розслідувань НПУ;

– створення оптимальної схеми агентурно-оперативного перекриття інтернет-магазину й інфраструктури його функціонування;

– за необхідності залучення до документування декількох оперативних підрозділів різного рівня та підпорядкування визначити, який з них буде виконувати координаційну функцію.

Водночас проведене опитування працівників оперативних підрозділів засвідчує, що під час реалізації цих етапів виявлення ознак кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, необхідну інформацію для подальшого ефективного документування вдається отримати лише в 47 % випадків. З огляду на це, у практичній діяльності постає необхідність практичного відпрацювання інтернет-магазину для отримання додаткової інформації шляхом проведення перевірочної закупівлі з метою:

– ознайомлення з фактичним рухом товару від складу до покупця (84 %, п. 11 додатка Б);

– встановлення порядку та форми розрахунку за товар (54 %, п. 11 додатка Б);

– ознайомлення з документами, які надають продавці (64 %, п. 11 додатка Б);

– у разі застосування приватної кур’єрської служби, а не служби інтернет-магазину, визначають підприємців, які здійснюють таку діяльність (59 %, п. 11 додатка Б);

– отримання інформації про кур’єра (на яких умовах здійснюють працевлаштування, на яких складах здійснюють отримання товару) (76 %, п. 11 додатка Б);

– визначення умов, за яких здійснюють повернення товару, після чого встановлюють коло суб’єктів господарської діяльності, які задіяні під час повернення товару (який документ видають) (71 %, п. 11 додатка Б);

– визначення обігу готівкових коштів (92 %, п. 11 додатка Б).

Алгоритм пошуку ознак кримінально протиправної діяльності, пов’язаної з використанням електронних грошей. Аналітичне опрацювання

оперативно-розшукових справ дає змогу визначити декілька типових схем використання електронних грошей з протиправною метою:

– ***незаконний обмін, конвертація валюти й виведення валюти за кордон***. Будь-який користувач мережі Інтернет має можливість зареєструвати на власне ім'я «електронний гаманець» у будь-якій валюті, далі – за допомогою оператора, що здійснює прийняття грошових коштів і подальший їх переказ. Оператор може здійснити як поповнення електронного рахунку, так і зняття готівки з нього, також оператор може провести валютно-обмінні операції, тобто отримати гривні, а на рахунок переказати іншу валюту. За виконання зазначених послуг оператор отримує комісію в розмірі 1,5–6 % від суми операції, залежно від обсягу наданих до переказу коштів.

Тобто відбувається виведення валюти за кордон, від звичайних споживчих покупок на міжнародних сайтах торгівлі (наприклад E-bay) до масштабного виведення валютних цінностей за кордон компаній, що виводять отримані прибутки чи здійснюють закупівлю товарів, які надалі надходять до України контрабандним шляхом;

– використання електронних грошей для розрахунку з інтернет-магазинами та компаніями, які надають послуги за допомогою мережі Інтернет. Працівники кіберполіції встановлюють факти торгівлі товарами та послугами в мережі Інтернет, оплата за які відбувається на електронні гаманці, відкриті на підставних осіб у платіжних системах, що не мають відповідних ліцензій на здійснення діяльності на території України. Ці грошові кошти, що надходять від покупця до продавця, оминають банківські рахунки, що унеможливлює контроль за їх переміщенням, проведенням відповідного фінансового моніторингу та надає можливість підприємствам отримувати великі суми неконтрольованого з боку держави прибутку. З метою руйнування схем мінімізації податкових зобов'язань, які виникають унаслідок торгових операцій в мережі Інтернет, проводять заходи з відпрацювання одного з товариств – інтегратора платежів, процесингової компанії. Власники цього сервісу надають послуги з отримання електронних грошових коштів від

покупців і подальшої їх передачі замовникам у безготівковому вигляді або ж у вигляді готівки (навіть валюти). За ці операції підприємство отримує винагороду у вигляді комісії в розмірі 3 % від суми переведених коштів. Така схема є аналогом схеми конвертації грошових коштів через банківські рахунки. Відмінність полягає в бездокументальному оформленні проведених операцій, проте замовникам послуг документи не потрібні через повну тінізацію їх операцій, як купівлі товару, так і його продажу. Наприклад, *ГУПМ ДПС України зібрано матеріали щодо кредитної спілки «Кредит Інвест», яка виконує роль інструменту незаконної конвертації безготівкових грошових коштів у готівку та є учасником діяльності «конвертаційного центру».*

Суб'єкти господарської діяльності реального сектору економіки перераховують безготівкові грошові кошти на кредитну спілку «Кредит Інвест» як поповнення депозитного рахунку, своєю чергою фізичні особи отримують кредити, заставою за які оформлено титульні знаки Web-Money Trasfer (електронні гроші). Такі кредити не повертають, а отримані готівкові кошти передають зазначеним суб'єктам господарської діяльності за вирахуванням обумовленого відсотка. За період діяльності схеми незаконно переведено в готівку близько 200 млн грн.

На нашу думку, незалежно від виду кримінально протиправної діяльності, яку вчиняють за допомогою електронних грошей, ***початковий етап алгоритму виявлення ознак кримінально протиправної діяльності передбачає визначення системи електронних грошей, що використовують у злочинній діяльності.*** Вивчення системи електронних грошей дає змогу сформувати декілька класифікацій, на які має орієнтуватися працівник оперативного підрозділу під час виявлення пошукових ознак кримінально протиправної діяльності.

За типом носія (69 %, п. 12 додатка Б):

1. На базі фізичного пристрою: електронні гроші зберігають на спеціальному пристрої (наприклад, на чипі, вбудованому в смарткартку), що одночасно використовують для здійснення платежів. Під час використання

такого типу платіжних інструментів транзакція між платником й отримувачем платежу іноді може бути виконана без додаткового під'єднання смарткартки до мережі.

2. На базі програмного забезпечення (онлайн гроші): електронні гроші зберігають на накопичувачах інформації у формі файлів бази даних/масиву інформації. У цьому випадку під час здійснення транзакції запит до оператора електронних грошей є обов'язковим для завершення операції.

За типом технології зберігання (94 %, п. 12 додатка Б):

1. Із централізованим веденням розрахунків: усі транзакції записують та авторизують через централізовану систему рахунків, управління якою здійснює система електронних грошей.

2. З використанням електронних записів/символів: транзакція не потребує авторизації, електронні гроші існують у формі електронних символів, які обертаються всередині комп'ютерної чи телекомунікаційної мережі, або шляхом прямого під'єднання до такої мережі електронних пристроїв.

За ступенем анонімності (30 %, п. 12 додатка Б):

1. Цілком анонімні системи електронних грошей: ідентифікації користувача не вимагають ані під час придбання електронних грошей, ані під час здійснення ним транзакцій, а отже, ідентифікація та відстеження здійснених операцій між платником й отримувачем платежу є неможливою.

2. Системи, які вимагають ідентифікації: платник та отримувач платежу, здійсненого за допомогою електронних грошей, мають ідентифікувати себе, надаючи можливість системі електронних грошей відслідковувати транзакції.

3. Системи, які вимагають часткової ідентифікації: вимоги щодо часткової ідентифікації клієнтів можуть бути встановлені на законодавчому рівні й передбачати мінімальну ідентифікацію клієнтів (наприклад, за паспортними даними). Проте доступ до інформації щодо ідентифікації клієнтів та здійснення ними угоди можуть мати чітко встановлені державні інституції.

За розміром платежу (41 %, п. 12 додатка Б):

1. Система пікоплатежів: можуть здійснювати платежі розміром від менше ніж 1 євроцент до 1 євро.

2. Системи мікроплатежів: можуть здійснювати платежі від 1 євро до 10 євро. Здійснення платежів такого розміру з використанням чеків чи платіжних карт часто не є економічно вигідним.

3. Системи макроплатежів: можуть здійснювати транзакції більшого розміру.

Надалі обов'язковою складовою є ***визначення категорії емітента електронних грошей, які використані в злочинній діяльності.*** Відповідно до п. 1 ст. 4 Директиви 2006/48/ЄС про кредитні інституції, передбачено такі категорії установ, які мають право емітувати електронні гроші:

– кредитні установи з обмеженнями;

– спеціалізовані установи – емітенти електронних грошей;

– поштові установи;

– Європейський центральний банк і національні центральні банки, якщо вони не виконують роль кредитно-грошової установи;

– держави – члени ЄС або їхні органи регіональної та місцевої влади.

Усім іншим фізичним і юридичним особам, крім тих, які визначені вище, емісію електронних грошей заборонено.

Після визначення категорії емітента грошових коштів працівнику оперативного підрозділу необхідно встановити, які види платіжних послуг, що не підлягають обов'язковому регулюванню, може здійснювати відповідний суб'єкт, зокрема:

1. Послуги, що передбачають внесення/зняття коштів з платіжного рахунку, а також операції, необхідні для функціонування такого режиму.

2. Виконання платіжних транзакцій, зокрема переказу коштів на платіжний рахунок, що обслуговується як постачальником платіжних послуг споживача, так й іншим постачальником, а також виконання платіжних

транзакцій, які забезпечує кредитна лінія для споживача платіжних послуг, а саме:

– виконання прямого переказу коштів, включаючи одноразові операції;

– виконання платіжних транзакцій через платіжну картку або схожий пристрій;

– виконання кредитних переказів, включаючи постійні доручення.

3. Випуск/придбання платіжних інструментів.

4. Грошові перекази.

5. Виконання платіжних транзакцій, коли згоду платник надає за допомогою будь-якого телекомунікаційного, цифрового чи ІТ пристрою і платіж здійснюється через телекомунікаційного, ІТ чи мережевого оператора, що діє лише як посередник між користувачем платіжної послуги чи постачальником товарів/послуг.

Наступним етапом ***є визначення моделі, яку використовують системи електронних розрахунків залежно від конкретних технологічних рішень:***

1. *Використання платіжних карт та інших пристроїв із вбудованим електронно-запам'ятовувальним пристроєм.* Нині до таких систем належать НСМЕП, МАКСІ тощо. Загальною рисою такої технологічної схеми є наявність платіжної карти чи іншого пристрою, що містить власний електронно-запам'ятовувальний елемент, який дає змогу зберігати інформацію про стан рахунку користувача та здійснювані ним операції безпосередньо на платіжному пристрої. Оновлення інформації на такому мікрочипі та в платіжній системі проходить щоразу, коли користувач виконує операцію (поповнення/переказу/оплати тощо), підключаючись до платіжної системи. Перевагою такої схеми є надзвичайно високий рівень захисту інформації, проте серед наявних платіжних засобів використання такої моделі є найдорожчою, оскільки потребує розвертання великого сегменту спеціальної інфраструктури, що уможливлює її поширення на ринку лише за наявності потужних інвестицій та координації зусиль різних учасників системи (емітентів, банків, еквайрів, торговців та ін.).

2. Використання онлайнових схем електронних грошей та платіжних технологій. Перевагою онлайн схем електронних грошей є їх простота, дешевизна й можливість швидкого проведення операцій, що часто не вимагають дотримання обтяжливих процедур ідентифікації користувача та відкриття рахунку. Крім того, коли оператори електронних грошей тісно інтегровані з комерційним банком, що володіє значною кількістю відділень/терміналів, значною кількістю емітованих кредитних карток, обіг електронних грошей може відбуватися в межах розвиненої інформаційно-телекомунікаційної інфраструктури. Це дає змогу оптимізувати витрати під час проведення розрахунків. Серед ключових недоліків таких схем – недостатній рівень захисту таких транзакцій від шахрайських дій, оскільки їх безпеку забезпечують лише на програмному рівні.

Висновки до розділу 2

1. Суб’єктами оперативного обслуговування кіберпростору є структурні підрозділи ДКІБ СБУ та ДКП НПУ.

Сутність оперативного обслуговування кіберпростору полягає в процесі організації надходження інформації щодо конкретних суб’єктів, діяльність яких пов’язана із захистом, регулюванням та обігом цифрової інформації (у магістральних, регіональних чи локальних комп’ютерних мережах, окремих комп’ютерних системах), що становлять оперативний інтерес.

Як складова оперативно-розшукової діяльності оперативне обслуговування містить елементи організаційного характеру, традиційними є рівень оперативного обслуговування; види (принципи) оперативного обслуговування; аналіз стану оперативної обстановки; режим оперативного обслуговування; розстановка негласних працівників й організація функціонування інших джерел інформації.

Агентурно-оперативна робота в організаційних структурах власників (або розпорядників) системи, володільців інформації дає змогу завчасно отримати інформацію: 1) про користувачів системи та місце й обладнання для здійснення доступу до інформації; 2) про злочини, які готують або вчинені; 3) про злочинні зв'язки особи-користувача; 4) про латентні злочини й осіб, що їх вчинили; 5) про створення та діяльність злочинних груп.

Отримана під час роботи оперативних підрозділів інформація є не єдиною складовою загального масиву оперативно-розшукової інформації, окремого значення набувають і гласні її джерела. Однак, з огляду на те, що оперативне обслуговування кіберпростору співробітниками ДКП НПУ та ДКІБ СБУ є важливою умовою надходження первинної інформації про злочин або злочинні наміри особи, що діє в кіберпросторі, доцільно спрямувати увагу на гласні джерела інформації в контексті попередньої перевірки інформації про вчинення кримінального правопорушення або підготовку до його вчинення в кіберпросторі.

2. Ініціативна робота працівників оперативних підрозділів є ключовою формою виявлення злочинів цієї категорії, що відповідає принципу наступальності як одному із центральних спеціальних принципів ОРД.

На підставі результатів аналізу наявних наукових підходів виокремлено основні ознаки оперативного (ініціативного) пошуку: оперативний пошук передує оперативній профілактиці й оперативній розробці; об'єктами оперативного пошуку є особи, предмети та події (факти), які є джерелами оперативної інформації.

Проаналізовано дві моделі реалізації оперативної інформації про злочини економічної спрямованості, які вчиняють з використанням кіберпростору: 1) виявлення та документування такої кримінально протиправної діяльності працівником оперативного підрозділу з подальшим поданням рапорту з відповідними матеріалами керівнику слідчого підрозділу; 2) документування такої кримінально протиправної діяльності в межах

оперативної розробки із залученням слідчого для надання методичної допомоги.

РОЗДІЛ 3
ОРГАНІЗАЦІЙНО-ТАКТИЧНІ ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ ЕКОНОМІЧНОЇ СПРЯМОВАНОСТІ, ЯКІ ВЧИНЯЮТЬ З ВИКОРИСТАННЯМ КІБЕРПРОСТОРУ

3.1. Формування та реалізація тактичних операцій на початковому етапі розслідування

Вивчення матеріалів оперативно-розшукових справ, кримінальних проваджень й аналітичних матеріалів підрозділів кіберполіції дає підстави стверджувати, що протиправна діяльність у сфері економіки, яку здійснюють з використанням кіберпростору, є складною та доволі структурованою формою протиправної соціальної практики. Фактично йдеться про злочинну діяльність, і ми про це зазначали вище. Водночас слушно зауважити, що, досліджуючи проблему злочинності в кіберпросторі, науковці визначають її як сукупність одиничних злочинів, що зумовлює вибір відповідної методології наукового пізнання проблеми та структуру практичних рекомендацій. Водночас, на нашу думку, аналізуючи це явище крізь призму категорії «кримінально протиправна діяльність», можна використати комплексні та складніші теоретико-методологічні конструкції, спрямовані на оптимізацію слідчої діяльності щодо розслідування таких злочинів.

Зважаючи на викладене, вважаємо, що нині постала теоретико-методологічна необхідність обґрунтування відповідних криміналістичних комплексів, які спрямовані на виконання комплексних завдань розслідування на відповідних етапах. Слушно зауважити, що проблема формування тактичних операцій загалом не є новою для криміналістичної науки. Її розвиток безпосередньо пов’язаний з ускладненням кримінально протиправної діяльності, як наслідок – складністю досудового розслідування окремих категорій кримінальних проваджень. Зокрема, протягом тривалого часу в структурі методики розслідування виокремлювали стратегічні й

тактичні завдання, які реалізували відповідними засобами: стратегічні завдання – шляхом проведення тактичних операцій; тактичні завдання – шляхом проведення слідчих дій та оперативно-розшукових заходів, а також застосування окремих тактичних прийомів.

Такі криміналістичні комплекси безпосередньо залежать від: по-перше, підстав для початку кримінального провадження; по-друге, типової слідчої ситуації, яка склалася на відповідному етапі розслідування кримінально протиправної діяльності економічної спрямованості, вчиненої з використанням кіберпростору.

Аналізуючи структуру та функціональне призначення таких криміналістичних комплексів, насамперед необхідно зосередити увагу на підставах початку кримінальних проваджень щодо злочинів економічної спрямованості, які вчиняють з використанням кіберпростору. Досліджуючи проблематику підстав і моменту початку досудового розслідування, Л. Лобойко зазначає, що: перевірку первинних джерел інформації здійснюють лише логічними (нематематичними) засобами пізнання; підставами для початку досудового розслідування є мінімально необхідна сукупність ознак кримінального правопорушення та ознак складу кримінального правопорушення в діянні, щодо якого отримано інформацію; норми КПК України починають дію тоді, коли є підстави для досудового розслідування [96]. Водночас, поряд із підставами й моментом початку досудового розслідування, слушно спрямувати увагу й на форми початку досудового розслідування, які детермінують застосування певних криміналістичних комплексів. Досліджуючи це питання в контексті формування комплексної криміналістичної методики розслідування кіберзлочинів, О. Самойленко цілком обґрунтовано виокремила чотири організаційні форми початку кримінальних проваджень щодо кіберзлочинів, а саме: 1) кримінальне провадження розпочинається на підставі отримання заяви потерпілого чи повідомлення особи про вчинення кримінального правопорушення; 2) кримінальне провадження розпочинають за результатами ознайомлення з

матеріалами оперативного підрозділу щодо перевірки оперативної інформації; 3) кримінальне провадження розпочинається внаслідок реалізації матеріалів оперативно-розшукової справи; 4) кримінальне провадження розпочинають унаслідок безпосереднього виявлення слідчим іншого кримінального правопорушення під час досудового розслідування конкретного кримінального провадження [158, с. 178–179].

Вивчення практики роботи підрозділів кіберполіції засвідчує, що кримінальні провадження щодо кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, у переважній більшості випадків розпочинається за матеріалами оперативних підрозділів, які здійснювали попереднє документування кримінально протиправної діяльності, а якість таких матеріалів безпосередньо залежить від того, чи залучали на етапі роботи за оперативно-розшуковою справою слідчого для надання методичної допомоги. Відповідно до положень відомчих нормативно-правових актів, які регулюють питання організації і тактики ОРД під час провадження за оперативно-розшуковою справою, яку заведено стосовно осіб, про яких є дані щодо участі в підготовці до вчинення злочину, начальник оперативного підрозділу може звернутися до начальника слідчого підрозділу про закріплення за цією оперативно-розшуковою справою слідчого для забезпечення методичного супроводження її реалізації та надання практичної допомоги оперативному підрозділу. Начальник оперативного підрозділу через режимно-секретний орган надає слідчому необхідні матеріали справи для вивчення та надання в разі потреби рекомендацій щодо фіксації додаткових фактичних даних про можливі протиправні діяння осіб і груп, що засвідчують наявність у їхніх діях ознак злочину. Одночасно розробляють план заходів з реалізації матеріалів оперативно-розшукової справи, який затверджує начальник оперативного підрозділу й органу досудового розслідування. Однак проведене нами дослідження дає підстави стверджувати, що через надмірну завантаженість слідчих підрозділів слідчих лише в деяких випадках залучають до супроводження та надання методичної

допомоги за оперативно-розшуковою справою, а в більшості випадків таке залучення слідчого є формальним, що істотно знижує якість зібраних оперативним підрозділом матеріалів.

Загалом необхідно зауважити, що за наявності такої форми початку кримінального провадження перед слідчим постає завдання щодо реалізації певної групи тактичних операцій, які, з одного боку, є системою завершених дій, а з другого – знаходяться у відповідних взаємозв'язках між собою.

Така наукова категорія, як тактична операція, завжди була предметом наукових дискусій. Відповідно до визначення, запропонованого колективом авторів Національної академії внутрішніх справ, тактична операція – це комплекс слідчих і негласних тактичних операцій СРД, інших процесуальних дій, оперативних-розшукових, організаційно-технічних та інших заходів, які проводять за узгодженим планом і спрямовані на виконання конкретного практичного завдання під час розслідування кримінального правопорушення [80, с. 385]. Перелік тактичних операцій та вибір конкретної з них залежить від обставин вчинення кримінального правопорушення.

Першою тактичною операцією є *«Аналітичне опрацювання та оцінка отриманих матеріалів»*. Попри те, що під час такої діяльності слідчий не проводить відповідну систему СРД і НСРД, водночас використовують тактичні прийоми й аналітичні методи, спрямовані на оцінку отриманих матеріалів, прийняття первинних тактичних рішень і визначення загальної стратегії розслідування кримінального провадження. Саме тому, на нашу думку, цей організаційно-тактичний блок діяльності слідчого можна визначити як самостійний криміналістичний комплекс. Необхідно зауважити, що, попри зростання ролі комплексної роботи з інформацією під час здійснення досудового розслідування, питання аналітичної роботи слідчого залишається майже недослідженим у межах вітчизняної криміналістичної науки, його аналізують переважно крізь призму інформаційно-аналітичного забезпечення розслідування загалом і використання інформаційних систем

правоохоронних органів під час досудового розслідування кримінальних правопорушень.

Продовжуючи, слушно, на нашу думку, виокремити основні блоки завдань, які виконує слідчий під час реалізації зазначеної тактичної операції, зокрема:

по-перше, визначення сутності кримінально релевантної події, яку схарактеризовано в матеріалах оперативного підрозділу (87 %, п. 13 додатка Б). Аналіз практики роботи підрозділів кіберполіції засвідчує, що у 87 % випадків, направляючи матеріали слідчому, працівник оперативного підрозділу вказує відповідну норму кримінального закону та кримінальне правопорушення, задокументоване ним. Водночас слідчому з метою належної попередньої кваліфікації злочину як такого, що вчинений з використанням кіберпростору, слушно проаналізувати наявні матеріали з метою визначення: а) технології кримінально протиправної діяльності; б) обстановки вчинення злочину; в) знарядь і засобів, які використовували для здійснення кримінально протиправної діяльності. З огляду на складність досліджуваної нами категорії кримінально протиправної діяльності, здійснюючи попередню діагностику сутності події, слідчому поряд з нормами закону про кримінальну відповідальність слушно працювати й з іншими джерелами правової та іншої інформації з використанням аналітичної методології, яка охоплює використання таких методів, як: порівняння, екстраполяція, аналіз, синтез тощо, а додатковими інформаційними джерелами для аналітичного опрацювання є: матеріали архівних і поточних кримінальних проваджень щодо злочинів цієї категорії, а також судова практика в частині кваліфікації різних форм кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору;

по-друге, встановлення якості попереднього документування кримінально протиправної діяльності (64 %, п. 13 додатка Б). Згідно з положеннями відомчих нормативно-правових актів, у процесі оперативної розробки забезпечують збір інформації про причетність особи або групи осіб,

зокрема невстановлених, до підготовки вчинення злочину, інші обставини й відомості, що мають значення для попередження та припинення злочину. Також підлягають документуванню виявлені під час оперативної розробки інші злочини, водночас, крім причетності до його вчинення конкретної особи або групи осіб, фіксують: по-перше, час, місце, спосіб учинення злочину; по-друге, місцезнаходження знарядь злочину, здобутого злочинним шляхом майна, товарно-матеріальних цінностей, грошей тощо; по-третє, місця приховування викрадених документів, майна, предметів, речовин тощо; по-четверте, розмір шкоди, заподіяної злочином; по-п’яте, інші обставини (спосіб приховування слідів злочину, мотив тощо).

Науковці, аналізуючи особливості оперативної розробки й документування злочинів у сфері економіки, зазначають, що правопорушення цієї категорії вирізняються значною складністю розкриття, тому що в процесі документування необхідно встановлювати: а) способи вчинення злочинів; б) коло причетних до вчинення злочину осіб, які беруть участь в економічних операціях; в) зв’язок із працівниками фінансово-банківських структур, співробітниками з інших галузей господарювання; г) місце приховування цінностей, коштів, які нажиті злочинним шляхом, забезпечення їх вилучення з метою відшкодування збитків. До основних напрямів документування науковці відносять: а) виявлення предметів і документів, які після проведення в майбутньому процесуальних дій будуть джерелами доказів і забезпечення їх зберігання до моменту початку кримінального провадження; б) встановлення осіб, які мають відомості про протиправні дії розроблюваних і можуть бути допитані як свідки в кримінальному провадженні; в) фіксація протиправних і злочинних дій розроблюваних у процесі їхньої діяльності [56]. Поділяючи такий підхід, зауважимо, що під час виконання цього завдання слідчий з’ясовує рівень попереднього документування відповідної системи обставин, які підлягають встановленню під час розслідування цього виду кримінально протиправної діяльності. Аналізуючи якість попереднього документування кримінально протиправної діяльності економічної спрямованості, яку

вчиняють з використанням кіберпростору, з метою якісного подальшого планування розслідування слідчий має акцентувати увагу на таких аспектах: а) документуванні всього механізму кримінально протиправної діяльності; б) встановленні під час документування конкретного різновиду апаратних засобів і програмного забезпечення, яке використовували для кримінально протиправної діяльності. Вагоме значення встановлення таких даних має в разі документування фактів протиправної діяльності невстановленої особи (групи осіб);

по-третє, виокремлення обставин кримінально протиправної діяльності, які потребують першочергової фіксації за допомогою проведення СРД і НСРД (74 %, п. 13 додатка Б). У контексті цього слід зауважити, що під час такого аналізу та планування основну увагу слідчий акцентує на якнайшвидшій фіксації цифрових слідів кримінально протиправної діяльності, що зумовлено специфічною природою цифрової інформації та можливістю її остаточної втрати в разі початку протидії досудовому розслідуванню з боку злочинців та/або їх зв'язків.

Іншою тактичною операцією є *«Встановлення особи злочинця»*, реалізація якої слідчим розпочинається після внесення відомостей до ЄРДР та початку кримінального провадження. Практика роботи підрозділів кіберполіції, які також керуються відповідним спеціальним принципом ОРД – наступальності, дає підстави стверджувати, що й до початку кримінального провадження оперативні підрозділи реалізують відповідні оперативно-тактичні комплекси, спрямовані на встановлення осіб, причетних до кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору. Такі оперативно-тактичні комплекси охоплюють систему агентурно-оперативних й оперативно-технічних заходів, які можуть здійснювати оперативні підрозділи до початку кримінального провадження.

Водночас опрацювання матеріалів кримінальних проваджень засвідчує, що на початковому етапі розслідування правоохоронні органи не мають

точних установчих даних осіб, які причетні до такої кримінально протиправної діяльності, їм відомі лише нікнейми, які особи використовують для самоідентифікації в кіберпросторі.

Слушно зауважити, що розробленню слідчим внутрішньої структури такої тактичної операції передує аналітична робота щодо встановлення можливих кореляційних залежностей між: а) механізмом кримінально протиправної діяльності – особою злочинця; б) предметом злочинного посягання – особою злочинця; в) знаряддями та засобами кримінально протиправної діяльності – особою злочинця. Проведення такої аналітичної роботи виконує декілька завдань на початковому етапі розслідування, зокрема:

по-перше, формування типового портрета (моделі) особи (групи осіб), які могли вчинити таке кримінальне правопорушення. Моделювання властивостей невідомого злочинця або складання психологічного портрета, зазначає Н. Жерж, здійснюють в умовах гострого дефіциту інформації, на підставі поведінкового аналізу наявних слідів і відомих обставин вчинення злочину. Такі моделі дають змогу також на основі відомих взаємозв’язків і кореляційних залежностей прогнозувати не встановлені властивості й особливості розшукуваних злочинців для того, щоб деталізувати портрет. Деякі науковці, що досліджували проблему розроблення типових моделей створення пошукового портрета злочинця, окреслюють відомості про його структуру й елементний склад. Структура запропонованих моделей може мати незначні відмінності, але практично всі дослідники цього питання виокремлюють ознаки, що характеризують біологічні, психічні та соціальні складові розшукуваної особи [54];

по-друге, звуження кола осіб, серед яких необхідно здійснювати пошукові заходи та слідчі (розшукові) дії;

по-третє, прогнозування можливих моделей протидії досудовому розслідуванню, зокрема: а) приховування невстановлених епізодів

кримінально протиправної діяльності; б) знищення елементів слідової картини встановлених фактів кримінально протиправної діяльності.

Опрацювання матеріалів кримінальних проваджень щодо кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору, дає змогу констатувати, що ця тактична операція поєднує відповідну систему таких процесуальних дій, як: а) допит; б) огляд; в) тимчасовий доступ до речей та документів; г) зняття інформації з електронних інформаційних систем. Під час характеристики структури тактичних операцій ми не акцентуємо увагу на організаційно-тактичних особливостях проведення цих СРД, оскільки їх буде проаналізовано в подальших підрозділах дослідження.

Логіка системного розслідування кримінальних проваджень щодо кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, засвідчує, що поряд із описаним вище криміналістичним комплексом на початковому етапі розслідування першочерговій реалізації підлягає тактична операція *«Фіксація цифрових слідів і формування цифрових доказів»*. Учені недостатньо уваги спрямовують на аналіз сутності цифрових слідів і цифрових доказів, тому, на нашу думку, перед визначенням структури й особливостей реалізації такої тактичної операції доцільно розглянути наявні наукові та практичні підходи щодо сутності цифрових слідів і цифрових доказів. У контексті цієї проблематики необхідно зауважити, що в межах криміналістики не досягнуто доктринальної єдності щодо вибору термінологічної конструкції для позначення специфічних слідів, які утворюються під час кримінально протиправної діяльності в кіберпросторі, зокрема, в наукових виданнях для позначення цієї категорії використовують такі термінологічні конструкції, які позначають один і той самий об’єкт: «віртуальні сліди», «цифрові сліди», «електроні сліди» тощо. Дослідники зазначають, що кіберзлочини вирізняються специфічною картиною слідів. На місці події одночасно зі звичайними слідами мають бути віртуальні сліди, що залишаються в пам’яті електронних

пристроїв. Віртуальні сліди є слідами вчинення будь-яких дій в інформаційному просторі комп'ютерних та інших цифрових пристроїв, їх систем і мереж. У теорії криміналістики є різні думки про те, як слід тлумачити поняття «віртуальні сліди»: 1) як зміна автоматизованої інформаційної системи; 2) з позицій фізичної та квантової теорії; 3) як результат фізичних і логічних операцій з двійковим кодом тощо [111]. Своєю чергою Н. Ахтирська зазначає, що сліди вчинення кіберзлочинів можуть знаходитися не лише безпосередньо в комп'ютерній техніці, на флешносіях, а й у кіберпросторі – середовищі (віртуальному просторі), яке надає можливості для здійснення комунікації та реалізації соціальних відносин, комунікаційних систем і забезпечення електронної комунікації з використанням мережі Інтернет або інших глобальних мереж передачі даних [9].

На переконання вчених, електронні сліди – це матеріальні, невидимі сліди, що можуть бути виявлені, зафіксовані та вивчені за допомогою цифрових електронних пристроїв і які містять будь-яку криміналістично значущу інформацію (відомості, дані), зафіксовану в електронній цифровій формі на матеріальних носіях. Специфічними властивостями електронних слідів є: а) відсутність нерозривного зв'язку з матеріальним носієм; б) динамічність, можливість миттєвого перенесення в просторі; в) можливість зміни та знищення інформації будь-якого обсягу в стислі проміжки часу (також за допомогою віддаленого доступу); г) ідентичність оригіналу інформації та всіх її копій незалежно від виду носія [1].

На думку О. Метелева, цифровий слід може охоплювати значну кількість окремих інформаційних компонентів, записаних на одному чи кількох машинних носіях (локальних або мережевих), тобто він не має фізично цілісної структури. Також його відображення в кожний конкретний проміжок часу залежить від технічних характеристик пристрою (його апаратного наповнення, операційної та файлової систем тощо), за допомогою якого цей цифровий слід інтерпретується в прийнятний для людини вигляд. Цифрові сліди не належать до матеріальних слідів, адже не мають фізичних

властивостей і не охоплюються поняттям ідеальних слідів, адже вони існують не у свідомості людини, а на певних матеріальних носіях, які можна дослідити тільки за допомогою спеціальних апаратно-програмних комплексів. Отже, цифровий слід суттєво відрізняється від традиційних матеріальних слідів, насамперед через свій багатокомпонентний характер. У процесі електронно-цифрового відображення механізм формування цифрового сліду охоплює дві основні групи компонентів: діяльність людини або обчислювального процесу й апаратно-програмного середовища. Крім того, у цифрових слідах немає фізично цілісної структури, вони мають складну інформаційну будову, специфічний механізм слідоутворення, а також сталий зв'язок з матеріальним носієм, на якому містяться. Отже, цілком доцільно було б розглядати цифрові сліди як окрему категорію [106].

Зауважимо, що ми поділяємо підхід щодо необхідності виокремлення цифрових слідів у самостійну категорію поряд з матеріальними й ідеальними слідами, які ґрунтовно досліджено в межах криміналістичної науки. Водночас у цьому дослідженні ми не акцентуємо увагу на обґрунтуванні їх сутності, визначенні ознак та розробленні відповідної класифікаційної системи, оскільки це виходить за межі предмета наукової роботи.

Поширеність кіберзлочинів, а також розуміння вченими та практиками відповідної специфіки слідоутворення під час такої кримінально протиправної діяльності актуалізували відповідну дискусію серед учених-процесуалістів щодо необхідності нормативного закріплення самостійного різновиду доказів, які утворюються в кіберпросторі та як результат роботи із цифровою інформацією. У наукових дослідженнях такий вид доказів визначають як «цифрові» або «електронні» докази. На думку Н. Ахтирської, «електронними доказами» є дані, які підтверджують факти, інформацію або концепцію у формі, придатній для обробки за допомогою комп'ютерних систем, зокрема програми виконання комп'ютерною системою та інших дій. Джерелами електронних доказів є: комп'ютери, периферійні пристрої, комп'ютерні мережі, мобільні телефони, цифрові камери й інші портативні пристрої,

мережа Інтернет [10]. Досліджуючи аналогічну проблематику, І. Крицька цифровими джерелами доказової інформації вважає програми (програмне забезпечення), файли та бази даних, аудіо-, відеозаписи тощо, джерелом яких, а отже, і формою існування, є пристрої, постійні запам'ятовувальні пристрої, накопичувачі на жорстких магнітних дисках, мобільні машинні носії тощо [85].

На переконання Д. Цехана, цифровими доказами є фактичні дані, представлені в цифровій (дискретній) формі та зафіксовані на будь-якому типі носія, що стають доступними для сприйняття людиною після обробки ЕОМ та можуть бути засобами для розкриття злочину та виявлення винних або для спростування обвинувачення чи пом'якшення відповідальності [186, с. 130]. Продовжуючи аналіз цієї проблеми в іншій науковій роботі, вчений зауважує, що в кожній ситуації необхідним є висунення відповідних вимог до коректності фіксації інформації. Будь-яке програмне забезпечення може містити помилки, які можна розділити на систематичні та спорадичні, тобто епізодичні й нерегулярні. Аналіз роботи окремих видів програмного забезпечення засвідчує, що ймовірність помилки в програмному забезпеченні залежить від її виробника, саме тому необхідним є використання програмного забезпечення, яке сертифіковане, хоча це також не виключає можливість помилки. Проте ймовірна можливість помилки програмного забезпечення не може апріорно слугувати фактором, що спростовує зафіксовану за його допомогою цифрову інформацію.

Виявлена помилка повинна відповідати трьом ключовим умовам: *по-перше,* бути підтвердженою службою технічної підтримки виробника програмного забезпечення, його уповноваженим представником або компетентною організацією, яка вивчає та узагальнює помилки й недоліки програмного забезпечення; *по-друге*, помилка повинна безпосередньо стосуватися фіксації інформації , тому й могла призвести до її модифікації, що підтверджують висновки експерта; *по-третє,* вона модифікувала під час

фіксації саме ту інформацію, що має значення для доказування, що підтверджують висновком експерта.

Частково інші вимоги до коректності фіксації інформації ставлять у випадку покрокової фіксації необхідної інформації слідчим, зокрема з використання відповідних програмних продуктів. Для закріплення як доказів цифрової інформації, отриманої внаслідок проведення слідчих дій чи НСРД, потрібне виконання щонайменше трьох умов. По-перше, необхідно здійснити оформлення всіх необхідних документів, що підтверджують правові підстави, окреслюють коло суб'єктів й умови фіксації даних відповідно до чинного законодавства України. По-друге, під час фіксації необхідно уникнути можливих фізичних дефектів відповідного носія та забезпечити максимально високу якість фіксації з метою можливості подальшого експертного дослідження такої інформації. По-третє, у разі відсутності в слідчого необхідних спеціальних технічних знань і навичок роботи з апаратними засобами та програмним забезпеченням, слід залучати спеціалістів, здатних кваліфіковано поводитися з ними, а згодом підтвердити технічну можливість і факт отримання таких відомостей у судовому засіданні [188].

Необхідно зауважити, що чинне кримінальне процесуальне законодавство не містить специфічних засобів у формі СРД, які за своєю функціональною спрямованістю повинні забезпечувати вилучення цифрових слідів і подальше формування цифрових доказів. Саме тому, залежно від типової слідчої ситуації початкового етапу розслідування, ця тактична операція може об'єднувати широкий спектр традиційних слідчих дій і тактичних прийомів, алгоритм реалізації яких зумовлений стратегією, визначеною слідчим, для виконання завдань конкретної слідчої ситуації. Водночас аналіз практики роботи слідчих підрозділів, наукових джерел, а також проведене нами дослідження дає змогу виокремити організаційно-тактичні особливості проведення слідчих дій у межах реалізації такого криміналістичного комплексу, зокрема:

– обов’язкове залучення до проведення будь-якої слідчої дії експерта, спеціаліста у сфері інформаційних технологій;

– вибір і підготовка оптимальних апаратних засобів та програмного забезпечення, яке може бути використано для коректної фіксації відповідної доказової інформації;

– підготовка належних носіїв для копіювання та фіксації цифрової інформації у випадках, якщо апаратні засоби та програмне забезпечення не можуть бути вилучені для подальшого дослідження і долучені до матеріалів кримінального провадження;

– планування заходів технічного характеру, спрямованих на нейтралізацію можливості знищення суб’єктом цифрової інформації під час безпосереднього проведення слідчої дії;

– у випадку, коли слідча дія передбачає обов’язкове залучення понятих, ужиття заходів щодо залучення понятих, які мають достатній рівень знань у сфері інформаційних технологій, розуміють сутність дій працівників правоохоронних органів під час її проведення, а також, за необхідності, зможуть дати показання щодо особливостей процесу вилучення слідчим цифрових слідів і коректності останнього.

Продовжуючи аналіз, необхідно спрямувати увагу на тактичну операцію, яку реалізують у межах початкового етапу розслідування кримінально протиправної діяльності економічної спрямованості, вчинювану з використанням кіберпростору, – «*Виявлення та вилучення речових доказів»*. Для злочинів цієї категорії характерним є доволі специфічний механізм слідоутворення, зокрема формування цифрових слідів, як наслідок – постає необхідність формування цифрових доказів. Водночас практика роботи підрозділів кіберполіції засвідчує, що під час розслідування злочинів цієї категорії слідчі виявляють значну кількість речових доказів, які використовують під час доказування окремих елементів кримінально релевантної події.

Узагальнення матеріалів практики дає змогу виокремити типові групи речових доказів, які можуть бути виявлені та вилучені під час розслідування цієї категорії кримінальних проваджень:

– апаратні засоби, які використовували в злочинній діяльності. Зауважимо, що в цьому контексті апаратними засобами слід вважати будь-який тип ЕОМ, що використовують у злочинній діяльності;

– інструктивні матеріали та література щодо роботи з відповідними апаратними засобами та програмним забезпеченням. Необхідно зауважити, що такі матеріали додатково можуть бути класифіковані на дві підгрупи: а) матеріали, які описують загальні алгоритми та процедури використання апаратних засобів і програмного забезпечення; б) матеріали, які описують алгоритми та процедури використання конкретних апаратних засобів і програмного забезпечення для здійснення кримінально протиправної діяльності;

– платіжні картки й інші платіжні інструменти, які мають відповідну фізичну сутність і можуть бути використані під час здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору;

– документи, зокрема чорнові записи щодо економічних операцій та руху активів під час кримінально протиправної діяльності;

– готівкові кошти в національній та іноземній валюті, отримані за результатами кримінально протиправної діяльності;

– «традиційні речові докази», які: а) підтверджують перебування особи в конкретному місці та роботу за відповідними апаратними засобами; б) забезпечують встановлення часового періоду перебування особи в конкретному місці; в) деталізують роль особи в механізмі кримінально протиправної діяльності.

Додатково необхідно зауважити, що в окремих випадках відокремлену групу речових доказів у провадженнях цієї категорії становить вогнепальна зброя та інші спеціальні засоби, що властиво діяльності організованих

злочинних угруповань, які забезпечують фізичну охорону об’єктів, на яких розміщується основна частина апаратних засобів, які використовують для кримінально протиправної діяльності.

Структурно в межах цього комплексу проводять дві тактичні операції: *«Пошук речових доказів»* і *«Вилучення речових доказів»*. Практика роботи підрозділів кіберполіції засвідчує, що за структурною побудовою тактична операція «Пошук речових доказів» охоплює:

а) агентурно-оперативні заходи, спрямовані на орієнтування негласного апарату, який перебуває на зв’язку у відповідного оперативного працівника щодо встановлення можливих місць знаходження речових доказів, зокрема місць, які використовують злочинці для розміщення стаціонарних апаратних засобів для здійснення кримінально протиправної діяльності;

б) СРД і НСРД пошукового характеру.

Тактична операція *«Вилучення речових доказів»* структурно охоплює:

а) систему тактичних прийомів, які обирають відповідно до тактичної ситуації, що склалася на відповідному етапі розслідування та є основою для планування і проведення подальших СРД;

б) систему СРД і НСРД фіксуючого спрямування (наприклад, тимчасовий доступ до речей і документів, обшук);

в) тактичні заходи забезпечення оптимального проведення СРД. Аналіз методичних рекомендацій та наукових робіт щодо виявлення і розслідування кіберзлочинів засвідчує, що вчені зосереджують чимало уваги на особливостях формування оптимальних алгоритмів вилучення цифрових слідів і формування цифрових доказів, натомість особливості вилучення апаратного забезпечення як речових доказів майже не досліджують, що призводить до тактичних помилок з боку слідчих і порушення процесуального порядку поводження з речовими доказами. З огляду на викладене, у подальших підрозділах дослідження ми будемо акцентувати увагу на проблемних питаннях вилучення речових доказів у провадженнях цієї категорії.

Логіка розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, у разі успішної реалізації описаних нами вище криміналістичних комплексів передбачає застосування тактичної операції *«Встановлення всіх учасників кримінально протиправної діяльності»*. Опрацювання матеріалів практики засвідчує, що реалізація та структурні елементи такої тактичної операції безпосередньо залежать від низки чинників, які сформовані за результатами документування кримінально протиправної діяльності та проведення першочергових СРД, зокрема:

а) чітке розуміння слідчим сутності кримінально релевантної події та механізму кримінально протиправної діяльності;

б) кількості встановлених і задокументованих епізодів кримінально протиправної діяльності;

в) встановлення місця знаходження та вилучення апаратних засобів і програмного забезпечення, яке використовували для здійснення кримінально протиправної діяльності;

г) встановлення та затримання окремих співучасників кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору.

Безумовно, найсприятливішою є ситуація, коли встановлено та затримано одного чи декількох учасників кримінально протиправної діяльності, оскільки проведення ефективних допитів таких осіб з використанням обґрунтованих тактичних прийомів дає змогу встановити інших учасників кримінально протиправної діяльності. Водночас, з огляду на високий інтелектуальний рівень таких осіб й активну протидію розслідуванню, традиційні засоби не завжди дають очікувані результати. Зважаючи на викладене, можна запропонувати дві моделі роботи, які спрямовані на реалізацію цього завдання:

по-перше, використання можливостей негласних працівників, які перебувають на зв’язку з працівником оперативного підрозділу, орієнтування

їх на виконання таких завдань: а) негласне відпрацювання зв’язків затриманих осіб; б) виявлення в середовищі кіберзлочинців та осіб, які вчиняють шахрайські дії в кіберпросторі, осіб, модель поведінки яких зазнала суттєвих змін після затримання конкретної особи чи групи осіб, наприклад, термінова зміна місця проживання та спроби виїхати поза межі України, раптове звільнення з роботи тощо; в) виявлення осіб, які намагаються терміново реалізувати апаратні засоби та програмне забезпечення, яке могло бути використане чи є аналогічним тому, яке використано для здійснення кримінально протиправної діяльності. Крім того, наявні на зв’язку негласні працівники можуть бути залучені для проведення візуального спостереження за встановленими злочинцями, щодо яких обрано запобіжний захід, не пов'язаний з ізоляцією від суспільства;

по-друге, використання методик кримінального аналізу, з огляду на обґрунтовані логічні припущення на основі наявної інформації. У такому випадку для здійснення кримінального аналізу використовують відповідну систему методів, спрямовану на реалізацію окремих тактичних завдань, зокрема:

метод аналогії та порівняння, на підставі використання якого аналізують наявні поточні кримінальні провадження, архівні кримінальні провадження та оперативні матеріали з метою встановлення осіб зі схожою моделлю злочинної поведінки, їх місцеперебування та можливості причетності до вчинення кримінального правопорушення. Необхідно зауважити, що об’єктами такого аналізу, за можливості, мають бути всі матеріали, незалежно від адміністративно-територіальної одиниці їх формування;

метод виключень – спрямований на виключення з наявних оперативних та інших даних осіб, які могли бути учасниками відповідної кримінально протиправної діяльності шляхом їх відпрацювання та перевірки за допомогою засобів і методів ОРД та проведення окремих СРД. Застосування цього методу шляхом аналізу наявної інформації щодо конкретних категорій осіб дає змогу

на початковому етапі виключити з переліку осіб, які підлягають обов'язковому відпрацюванню тих, що в силу встановлених об'єктивних причин не могли брати участі в конкретній злочинній діяльності;

метод побудови мережі зв'язків – передбачає розроблення графічних зображень і матриць асоціацій між людьми з метою встановлення можливості зв'язків між ними та рівня інтенсивності таких зв'язків. Необхідно зауважити, що в практичній площині побудова такої матриці асоціативних зв'язків є доволі складним завданням, оскільки потребує встановлення та перевірки соціальних контактів особи за тривалий проміжок часу, зокрема відпрацювання з цією метою закладів освіти, де навчалася особа, попередніх місць роботи тощо.

Водночас під час розслідування складних кримінальних проваджень побудова таких матриць у межах кримінального аналізу забезпечує виявлення неочевидних зв'язків між особами.

3.2. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) дій

Розслідування кримінально релевантних подій як процес пізнання має власний, напрацьований тривалою практикою та законодавчо закріплений інструментарій, який забезпечує виконання завдань у межах конкретного кримінального провадження, а також загальних завдань, визначених у ст. 2 КПК України. Безумовно, такий інструментарій ґрунтується на відповідній системі СРД і НСРД.

Відповідно до ст. 223 КПК України, слідчі (розшукові) дії є діями, спрямованими на отримання (збирання) доказів або перевірку вже отриманих доказів у конкретному кримінальному провадженні.

У контексті цього ми поділяємо позицію дослідників, які стверджують, що проведення слідчих дій є обов'язковою складовою процесуальної

діяльності слідчого та безпосереднім способом виконання завдань доказування. Ці дії є важливою частиною діяльності слідчого з розслідування кримінальних правопорушень, але це не вичерпує їх у процесі розслідування, оскільки процесуальні, організаційні та слідчі (розшукові) дії, що проводить слідчий, знаходяться у взаємозв'язку, взаємозалежності, доповнюючи одна одну, зрештою всі вони спрямовані на досягнення завдань кримінального судочинства. Доходимо висновку, що не кожна процесуальна діяльність слідчого спрямована на збирання доказів. Процесуальну діяльність, спрямовану на збирання доказів, здійснюють у двох формах: проведення СРД і проведення інших процесуальних дій [174]. Не заперечуючи таку позицію, вважаємо, що в контексті досліджуваної категорії злочинів СРД є основою діяльності з розслідування, тому саме вони привертають пріоритетну увагу. Видається слушним підхід Ю. Чорноус, яка вважає, що сутність слідчої (розшукової) дії як складного й багатоаспектного правового явища може бути висвітлена через її кримінальну процесуальну, морально-етичну, психологічну й організаційно-тактичну характеристики:

– кримінальна процесуальна характеристика СРД визначає процесуальну форму, дотримання якої є обов'язковим;

– морально-етична характеристика СРД полягає в неухильному дотриманні суспільної моралі, норм законодавства, професійної етики всіма учасниками слідчої (розшукової) дії. Під час проведення СРД мають бути дотримані: загальні морально-етичні норми суспільства; норми кримінального процесуального законодавства, міжнародних договорів України, що регламентують права та свободи людини, порядок кримінального провадження і проведення СРД; криміналістичні рекомендації; вимоги професійної етики уповноважених суб'єктів;

– психологічна характеристика СРД обумовлена психологічною характеристикою слідчої роботи, пізнавальним, конструктивним, комунікативним, організаційним, засвідчувальним характером діяльності.

Проведення СРД є складним процесом, зміст якого в психологічному аспекті формують пізнавальні, пошукові, конструктивні операції;

– організаційно-тактичну характеристику СРД слід висвітлювати крізь призму тактики їх проведення [193, с. 186–211].

Зважаючи на те, що визначення сутності СРД та інших криміналістичних і кримінально-процесуальних аспектів цієї проблематики ґрунтовно проаналізовано в криміналістичній літературі, ми не акцентуватимемо уваги на узагальненні теоретичних напрацювань учених.

Здійснене нами узагальнення матеріалів кримінальних проваджень дає підстави запропонувати умовну класифікацію СРД, які проводять під час розслідування злочинів цієї категорії. Зокрема, на нашу думку, такі дії можуть бути класифіковані за критерієм мети проведення на:

а) пошукові слідчі (розшукові) дії, спрямовані на отримання нових фактичних даних щодо вчиненого кримінального правопорушення, які раніше не були відомі слідству;

б) перевірочні слідчі (розшукові) дії, спрямовані на перевірку та підтвердження інформації, отриманої під час проведення інших СРД та інших процесуальних й оперативно-розшукових заходів.

З огляду на запропоновану класифікацію, на нашу думку, до першої групи можуть бути віднесені такі СРД, як допит та огляд, а до другої групи – пред’явлення особи для впізнання, пред’явлення речей для впізнання, обшук, слідчий експеримент. Водночас одразу слід зауважити, що такий розподіл слідчих дій є доволі умовним, оскільки деякі з них можуть бути віднесені до обох класифікаційних груп, зокрема обшук, який, з одного боку, спрямовується на перевірку інформації, наявної в слідчого, а з другого – забезпечує виявлення раніше не відомих слідчому фактичних даних.

Розпочинаючи аналіз особливостей проведення СРД під час розслідування злочинів цієї категорії, насамперед слід проаналізувати організаційно-тактичні особливості проведення огляду.

У ст. 237 КПК України законодавець визначає, що з метою виявлення та фіксації відомостей щодо обставин вчинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей, документів і комп'ютерних даних.

Аналіз матеріалів кримінальних проваджень щодо розслідування злочинів економічної спрямованості, які вчиняють з використанням кіберпростору, дає змогу виокремити типові об'єкти огляду, зокрема: а) приміщення, де концентрується основна система засобів кримінально протиправної діяльності (61 %, п. 16 додатка Б); б) апаратні засоби (66 %, п. 16 додатка Б); в) вебсайти (92 %, п. 16 додатка Б); г) програмні засоби в реальному часі їх функціонування (63 %, п. 16 додатка Б); д) документи (59 %, п. 16 додатка Б); е) інші речові докази, які мають значення для встановлення обставин, які підлягають доказуванню під час розслідування цієї категорії кримінальних проваджень (23 %, п. 16 додатка Б).

Насамперед слід зосередити увагу на особливостях огляду приміщень, де знаходиться основна частина засобів кримінально протиправної діяльності. Вище зазначено, що більша частина кримінальних проваджень цієї категорії розпочинається за результатами реалізації підрозділами кіберполіції оперативної інформації, саме тому проведення такої СРД не є спонтанним, як під час розслідування злочинів загальнокримінальної спрямованості, коли слідчий фактично реагує на вчинення завершеної кримінально релевантної події. В аналізованій ситуації слідчий має достатньо часу для підготовки до проведення такого огляду. Досліджуючи проблему розслідування комп'ютерних злочинів, науковці переважно оминають увагою зазначене питання. Це передусім зумовлено тим, що з організаційно-тактичного боку проведення такого огляду є аналогічним проведенню огляду місця події під час розслідування інших категорій кримінальних проваджень. Водночас, на нашу думку, огляд приміщення під час розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору, має певні особливості: *по-перше,* формує в слідчого уявлення не лише про сутність

кримінально релевантної події, а й щодо рівня організованості та системності кримінально протиправної діяльності, що дає змогу конкретизувати подальшу стратегію розслідування (92 %, п. 17 додатка Б); *по-друге,* під час огляду приміщень, виявляють інфраструктурні елементи, які забезпечують кримінально протиправну діяльність підозрюваних (76 %, п. 17 додатка Б).

У межах *першого блоку* під час огляду слідчому необхідно відобразити в протоколі огляду такі елементи: а) просторово-технічні характеристики приміщення, зокрема його доступність для випадкового огляду іншими особами; б) віддаленість від публічних місць і місць масового скупчення людей; в) конструктивні особливості окремих частин будівлі, зокрема вікон – обладнання їх засобами маскування; г) планування приміщення, що дає змогу зробити припущення щодо його спеціального пристосування до здійснення кримінально протиправної діяльності, що свідчить про високий рівень її організації.

У межах *другого блоку* увагу слідчий має фокусувати на окремих елементах інфраструктурного забезпечення приміщення, зокрема: встановлення додаткових систем безперебійного електропостачання; наявність у приміщенні генераторів автономного енергопостачання; камер спостереження в межах периметра приміщення та ззовні; систем охорони та сигналізації, а також відокремленого місця для дислокації фізичної охорони. Виявлення під час огляду приміщень зазначених елементів дає змогу слідчому дійти попередніх висновків щодо особливостей виявленої кримінально протиправної діяльності злочинців, а саме:

а) організаційної форми співпраці учасників кримінально протиправної діяльності. У контексті цього необхідно пояснити, що йдеться не лише про модель організації конкретного злочинного угруповання, а й про обізнаність інших осіб із сутністю подій, які там відбувалися, оскільки останні могли не брати безпосередньої участі в злочинній діяльності економічної спрямованості, яку здійснювали з використанням кіберпростору, проте володіти інформації щодо суб’єктів такої діяльності, особливостей

взаємовідносин між цими особами, зокрема наявності внутрішніх конфліктів усередині угруповання тощо;

б) тривалості кримінально протиправної діяльності та професійного рівня організаторів останньої, про що може свідчити обсяг капітальних вкладень у приміщення з метою забезпечення кримінально протиправної діяльності;

в) імовірна наявність в організаторів кримінально протиправної діяльності інших приміщень, де здійснюють аналогічну протиправну діяльність.

Наступним традиційним об'єктом огляду під час розслідування злочинів економічної спрямованості, які вчиняють з використанням кіберпростору, є апаратні засоби. З огляду на різноманітність апаратних засобів, які використовують у злочинній діяльності, сформувати тактичні рекомендації для огляду кожного з них неможливо й недоцільно через їх швидку адаптивність і постійну трансформацію. На нашу думку, можна виокремити дві тактичні ситуації огляду апаратних засобів, які потребують детальнішого аналізу.

Першою тактичною ситуацією є попередній огляд апаратних засобів на місці події або під час їх вилучення в особи. Вище ми зазначали, що огляд місця події в провадженнях цієї категорії не проводять спонтанно, слідчий має можливість забезпечити його підготовку. З організаційно-тактичного боку така підготовка охоплює відповідну систему дій, зокрема:

– потенційну оцінку виду та класу апаратних засобів, які будуть оглядати на місці події, що ґрунтується на наявній у слідчого інформації щодо сутності кримінально релевантної події;

– визначення кількості та фахової спрямованості спеціалістів, яких необхідно залучити до проведення огляду. У контексті цього слід зауважити, що фах спеціаліста зумовлений тим, чи розглядає слідчий тактичну можливість огляду апаратних засобів у процесі їх безпосередньої роботи з використанням засобів фіксації роботи програмного забезпечення певного

виду. Наприклад, огляд з використанням відеозйомки моніторів відповідних пристроїв, на яких відображається робота окремих програмних продуктів у реальному режимі часу. На нашу думку, за наявності організаційно-тактичної можливості такої фіксації її здійснення є обов'язковим, оскільки згодом забезпечує доказування використання алгоритмів і програмних продуктів для вчинення економічних злочинів, а спеціаліст, який бере участь у такому огляді, може бути допитаний під час досудового розслідування та судового розгляду щодо особливостей та функціональної спрямованості роботи конкретного типу програмного забезпечення, роботу якого задокументовано в реальному режимі часу. Водночас необхідно зауважити, що огляд робочих апаратних засобів з метою відеофіксації роботи програмного забезпечення передбачає значні тактичні ризики, оскільки за наявності віддаленого доступу й можливості контролю за роботою таких апаратних засобів є реальна загроза миттєвого знищення даних, які зберігаються на відповідних носіях інформації;

– визначення переліку засобів для вилучення виявлених на місці події апаратних засобів;

– формування групи забезпечення, що спрямована на недопущення умисного припинення електропостачання в приміщення та вимкнення апаратних засобів;

– добір понятих, які обізнані щодо особливостей роботи апаратних засобів і програмного забезпечення та можуть надалі бути допитані щодо сутності проведеної СРД.

Розглянемо тактичні особливості початкових дій після прибуття на місце, де будуть проводити огляд і подальше вилучення апаратних засобів. Слушною видається позиція О. Тарасенка, який зазначає, що початковим завданням є вжиття заходів, що спрямовані на забезпечення збереження відповідної інформації:

– не дозволяти нікому з осіб, що працюють у цей час або які перебувають у приміщенні з інших причин, торкатися до комп'ютерної техніки (серверів),

а також користуватися телефоном (у разі екстреної ситуації такий дозвіл може бути надано виключно під контролем працівника поліції);

– не дозволяти будь-кому вимикати електропостачання об’єкта та комп’ютерної техніки;

– не дозволяти здійснення жодних маніпуляцій з комп’ютерною технікою, якщо їх результат не є прогнозованим;

– визначити, чи знаходяться комп’ютери в приміщенні, яке оглядають, у локальній мережі. Водночас потрібно зважати, що сервером може бути не один, а декілька комп’ютерів, які розташовані в різних приміщеннях;

– встановити, чи є з’єднання комп’ютерної техніки з іншими апаратними засобами, зокрема поза межами приміщення;

– з’ясувати, яка система завантажена та які програми запущені [171].

Не заперечуючи такий підхід щодо початкових тактичних дій під час огляду загалом, необхідно зосередити увагу на окремі позиції, які, на нашу думку та з огляду на практику роботи підрозділів кіберполіції, видаються дискусійними. Під час візуального огляду апаратних засобів навіть за участю спеціаліста неможливо без втручання в роботу програмного забезпечення, встановленого на відповідному апаратному засобі, визначити об’єднаність декількох апаратних засобів у локальну мережу та керованість такими апаратними засобами ззовні. У контексті цього слідчому необхідно на початковому етапі огляду враховувати ситуацію тактичного ризику та можливого управління апаратними засобами дистанційно, що може призвести до втрати інформації. Практика роботи правоохоронних органів засвідчує, що на місці події здебільшого перебувають виконавці програмно-технічного аспекту кримінально протиправної діяльності, а апаратні засоби контролюють ззовні, як і безпосередньо приміщення за допомогою камер відеоспостереження.

За результатами реалізації початкового етапу огляду слідчий може обрати дві типові моделі його продовження: 1) фіксація роботи апаратних засобів і програмного забезпечення в режимі реального часу (97 %, п. 18

додатка Б), наприклад, до завершення виконання програмними продуктами певних алгоритмів, і лише після цього відключення апаратних засобів від мережі енергопостачання та їх вилучення; 2) негайне відключення апаратних засобів від мережі енергопостачання та їх вилучення (98 %, п. 18 додатка Б). Вибір другої моделі здійснюють за наявності достатніх підстав вважати, що апаратні засоби знаходяться під зовнішнім управлінням та інформація на них може бути знищена дистанційно.

Повертаючись до безпосереднього огляду апаратних засобів на місці події, необхідно зауважити, що в переважній більшості випадків слідчі обирають модель попереднього огляду таких апаратних засобів, метою якого є: а) фіксація локації їх розташування в приміщенні (98 %, п. 19 додатка Б); б) встановлення інструментів фізичного з'єднання апаратних засобів між собою, а також із периферійним обладнанням (63 %, п. 19 додатка Б); в) виявлення та фіксація в протоколі ідентифікаційних ознак кожного апаратного засобу, який оглядають і згодом буде вилучений працівниками правоохоронних органів (100 %, п. 19 додатка Б). Такий підхід видається логічним, оскільки детальний огляд апаратних засобів потребує тривалого часу та спеціальних умов, тож його проведення навіть за участю спеціаліста на місці події є неможливим. Залучений спеціаліст до огляду апаратних засобів безпосередньо на місці події виконує допоміжні завдання в аспекті: а) конкретизації переліку апаратних засобів, які потребують огляду та вилучення, оскільки брак у слідчого спеціальних знань може призвести до того, що він не ідентифікує окреме обладнання як апаратний засіб, який має відношення до кримінально протиправної діяльності (86 %, п. 20 додатка Б); б) надання слідчому допомоги в здійсненні коректного відключення апаратних засобів від мережі енергопостачання (69 %, п. 20 додатка Б); в) надання слідчому допомоги щодо коректного роз'єднання та локалізації апаратних засобів, які фізично пов'язані між собою (76 %, п. 20 додатка Б); г) консультування та надання безпосередньої допомоги щодо коректного упакування та опечатування

вилучених апаратних засобів і рекомендацій щодо їх безпечного транспортування (92 %, п. 20 додатка Б).

Загалом ми поділяємо позицію дослідників, які розподіляють такий огляд на статичний і динамічний. Статична фіксація технічних (комп'ютерних) пристроїв та інших матеріальних об'єктів, наявних мережевих підключень (спосіб підключення: за допомогою технологій Wi-Fi чи кабелю), кількість роз'ємів підключення в кожного пристрою, їх види, схема взаємного розташування пристроїв, порядок з'єднань у мережі, вид використовуваних кабелів, їх кількість, зовнішній вигляд пристроїв (номер, модель, форма, колір), стан (увімкнений/ вимкнений) на момент проведення огляду. Усі ці дії супроводжують криміналістичною фото- та відеозйомкою, складають план приміщення та схему розміщення комп'ютерного обладнання, локальних мереж, інших точок підключення до системи, локальної мережі чи мережі Інтернет. Також важливо унеможливити фізичний доступ до комп'ютерної техніки осіб, які з нею працюють, ужити спеціальних заходів для блокування спроб здійснення віддаленого доступу до такої техніки. Зазначені дії рекомендовано попередньо узгодити зі спеціалістом до початку проведення огляду для оперативної координації дій учасників слідчої групи. Далі слідчий переходить до динамічної стадії – детального огляду. Динаміка зумовлена тим, що предмети, визначені як окремі об'єкти огляду, можуть зрушуватися з місця. Об'єкти огляду за вказівкою слідчого детально опрацьовує спеціаліст-криміналіст на предмет слідів пальців рук, нігтів, слідів фізичного контакту з іншими твердими поверхнями, зокрема тими, що спричинили механічні пошкодження, для їх фіксації та вилучення. Цей підхід є типовим для фіксації слідів злочину (відомий для слідчих), однак слід ураховувати можливість відшарування чи нашарування речовин, порошків, фарби, інших мікроелементів на поверхнях комп'ютерного устаткування, зокрема біологічних слідів ДНК-профілю чи виявлення одорологічних слідів [191].

Продовжуючи аналіз, необхідно також акцентувати на тактичні особливості проведення допиту в кримінальних провадженнях цієї категорії, оскільки допит є найпоширенішою слідчою дією, за його допомогою здобувають найбільшу кількість доказів, які дають змогу встановити обставини кримінального правопорушення.

У юридичній літературі сталою практикою є розподіл слідчих дій на вербальні й невербальні, з огляду на це, насамперед необхідно розглянути особливості проведення допиту осіб, безпосередньо причетних до вчинення таких злочинів. На думку В. Безлєпкіна, допит передбачає регламентований законодавством усний діалог між посадовою особою, у провадженні якої знаходиться кримінальна справа, і свідком, підозрюваним й обвинуваченим, що проводиться з метою отримання фактичних даних (усних відомостей), які мають доказове значення [179, с. 75].

Зважаючи на достатньо високий рівень розроблення тактики проведення допиту особи, яку підозрюють у вчиненні кримінального правопорушення, вважаємо за необхідне зосередити свою увагу саме на особливостях проведення окресленої слідчої дії під час допиту кіберзлочинців.

Особа, причетна до вчинення злочинів економічної спрямованості з використанням кіберпростору, володіє відповідною системою спеціальних знань у сфері функціонування інформаційних технологій та за своєю інтелектуально-психологічною організацією суттєво відрізняється від осіб, які вчиняють злочини загальнокримінальної спрямованості. У контексті цього слідчий зосереджує увагу на підготовці до проведення допиту конкретної особи, крім того, на нашу думку, під час підготовки до проведення такого допиту слідчому доцільно залучати спеціаліста з метою: а) конкретизації предмета допиту відповідної особи; б) надання слідчому допомоги у формулюванні конкретних запитань, які стосуються технічної сторони роботи відповідних апаратних засобів і програмного забезпечення, а також алгоритмів та моделей кримінально протиправної діяльності. Слушно зазначають науковці, що під час розслідування кіберзлочинів необхідними є

знання в галузі телекомунікаційних систем, комп'ютерних технологій і комп'ютерної техніки. Водночас не кожен слідчий володіє такими знаннями або володіє ними в недостатньому обсязі, у зв'язку із чим під час підготовки до допиту слід вирішити питання про необхідність залучення спеціаліста, допомога якого уможливить точне формулювання питань, а також повне й усебічне розуміння слідчим відповідей на них та їх правильну фіксацію. Пов'язана із цим і проблема можливої інтелектуальної протидії з боку злочинця, для чого можуть використовувати спеціальні знання та навички, на що також має спрямувати увагу спеціаліст [49].

На стадії підготовки до допиту у справах про кіберзлочини необхідно провести інформаційне забезпечення допиту, дослідження особистості допитуваного та планування допиту. Інформаційне забезпечення є важливою складовою на стадії підготовки до допиту особи, яка вчиняє злочини із використанням кіберпростору, адже високий рівень знань слідчого та володіння ним усіма зібраними у справі матеріалами й допоміжною інформацією технічного характеру гарантує контрольованість ситуації на допиті. Ще однією умовою інформаційного забезпечення допиту під час розслідування кіберзлочинів є наявність знань комп'ютерних технологій, а також нормативно-правової бази, що регулює галузь порушених прав й інтересів.

Підготовка до допиту конкретної особи в цій категорії кримінальних проваджень потребує від слідчого значної аналітичної роботи з метою встановлення окремих даних, які визначають предмет і тактику проведення допиту. На підготовчому етапі з метою конкретизації предмета допиту слідчому необхідно системно проаналізувати: а) роль конкретної особи в злочинній діяльності (71 %, п. 21 додатка Б); б) на підставі раніше побудованої працівниками оперативного підрозділу чи безпосередньо слідчим матриці зв'язків визначити ступінь інтенсивності зв'язків цієї особи з іншими учасниками кримінально протиправної діяльності (69 %, п. 21 додатка Б); в) тривалість участі особи в злочинній діяльності (92 %, п. 21 додатка Б).

Водночас з метою конкретизації тактичних прийомів допиту слідчому необхідно акцентувати увагу на таких аспектах: а) вік допитуваної особи, оскільки практика роботи підрозділів кіберполіції засвідчує, що до вчинення шахрайств із використанням інформаційних технологій часто залучають неповнолітніх, які самостійно здобули достатні компетентності щодо роботи кіберпростору та використання відповідних апаратних засобів і програмного забезпечення; б) сімейний стан особи й наявність у неї відповідної системи корисних соціальних зв'язків; в) чи притягували особу раніше до будь-яких форм кримінальної відповідальності, чи обізнана вона з методами та прийомами роботи слідчих підрозділів; в) ступінь задокументованості кримінально протиправної діяльності конкретної особи, наявність у кримінальному провадженні зібраних доказів, які в необхідних випадках за тактичної необхідності можуть бути продемонстровані особі, яку допитують; г) час встановлення причетності особи до кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору. Безумовно, ці блоки аналітичної оцінки слідчим під час підготовки до проведення допиту не є вичерпними і варіюються залежно від слідчої ситуації, яка склалася в розслідуванні на момент проведення цієї слідчої дії.

Аналіз тактичних складових допиту в кримінальному провадженні потребує акцентування уваги на формах і методиках встановлення психологічного контакту з допитуваним. Водночас у межах нашого дослідження залишаємо цю проблему поза увагою, оскільки це питання ґрунтовно проаналізовано в криміналістичній літературі, а напрацьовані методики щодо встановлення психологічного контакту можуть бути використані для допиту осіб, які вчиняють злочини економічної спрямованості з використанням кіберпростору без особливих модифікацій.

Вважаємо необхідним акцентувати увагу на проведенні допиту осіб, які причетні до кримінально протиправної діяльності економічної спрямованості, вчиненої з використанням кіберпростору. Закономірно, що предмет допиту

таких осіб залежить від їх ролі в структурі досліджуваної нами кримінально протиправної діяльності.

Особливим є предмет допиту особи – виконавця злочинних дій, пов'язаних із використанням кіберпростору. Водночас акцентуємо увагу на тому, що предмет такого допиту різнитиметься залежно від того, чи здійснює особа кримінально протиправну діяльність у складі угруповання, чи є автономним злочинцем, що займається злочинною діяльністю економічної спрямованості з використанням кіберпростору.

У межах допиту особи виконавця, що входить до складу злочинного угруповання, можна виокремити такі структурні блоки предмета допиту:

по-перше, дані, які характеризують механізм залучення особи до кримінально протиправної діяльності (66 %, п. 22 додатка Б). У межах цього блоку з'ясовують питання щодо:

– способу встановлення особою контакту з представниками угруповання чи іншими злочинцями: а) ініціативна діяльність особи щодо пошуку інших осіб для подальшого здійснення кримінально протиправної діяльності; б) реакція особи на відповідні повідомлення в соціальних мережах і подальший контакт зі злочинцями з використанням різного типу месенджерів;

– система кваліфікаційних вимог до особи, яка вирішила здійснювати кримінально протиправну діяльність економічної спрямованості з використанням кіберпростору;

– особливості попередньої співбесіди з такою особою, зокрема, хто її проводив, її зміст;

– чи надавали особі перевірочні завдання з метою перевірки її кваліфікації щодо використання апаратних засобів і програмного забезпечення для здійснення кримінально протиправної діяльності економічної спрямованості;

– чи проводили навчання особи щодо психологічних методик входження у довіру та використання засобів психологічного маніпулювання під час особистих розмов з потерпілими, зокрема у випадках вчинення шахрайств із

використанням засобів стільникового зв'язку, механізм яких передбачає особистий вербальний контакт злочинця і потерпілого за допомогою засобів стільникового зв'язку;

– чи було обумовлено «випробувальний термін» перед постійним входженням до складу злочинного угруповання;

– чи вимагали від особи рекомендації інших злочинців або спеціалістів у сфері інформаційних технологій з метою підтвердження її кваліфікації та готовності здійснювати злочинну діяльність;

по-друге, дані, які характеризують безпосередню кримінально протиправну діяльність виконавця (97 %, п. 22 додатка Б). У межах цього блоку з'ясовують питання щодо:

– безпосереднього алгоритму кримінально протиправної діяльності виконавця, зокрема, які конкретно дії вчиняв він з використанням апаратних засобів і програмного забезпечення, що мають протиправний характер;

– спосіб забезпечення виконавця конкретними апаратними засобами та програмним забезпеченням;

– часові проміжки здійснення кримінально протиправної діяльності;

– основне місце базування комплексу апаратних засобів, які використовували для здійснення кримінально протиправної діяльності;

– використання спеціалізованого програмного забезпечення для маскування власної протиправної діяльності. У контексті з'ясування питань цього блоку предмета допиту, на нашу думку, слідчому доцільно залучати спеціаліста, що не суперечить вимогам КПК України. Науковці слушно зауважують, що під час здійснення допиту кіберзлочинців у програмному забезпечені комп'ютерної техніки, комп'ютерних технологіях, телекомунікаційних мережах тощо, такими знаннями володіє спеціаліст, який може надати консультативну допомогу в роз'ясненні термінів, побудові питань, встановлювати зв'язок між здійснюваними особою операціями та вчиненим злочином. Однак слід ураховувати, що присутність спеціаліста на допиті, з одного боку, не впливає на особу кіберзлочинця і допит проводять у

звичайному режимі, з другого – може негативно позначитися на допитуваному, оскільки викликає недовіру щодо професіоналізму слідчого [93].

Вважаємо, що функціональною спрямованістю спеціаліста у сфері інформаційних технологій під час допиту є: а) уточнення запитань слідчого щодо апаратних засобів і програмного забезпечення, яке використовували під час здійснення кримінально протиправної діяльності; б) конкретизація питань щодо безпосередньої технологічної складової кримінально протиправної діяльності; в) надання консультативної допомоги слідчому щодо оцінки повноти та правдивості показань, наданих особою;

по-третє, дані, що характеризують структуру й чисельність злочинного угруповання, яке вчиняє злочини економічної спрямованості з використанням кіберпростору (62 %, п. 22 додатка Б). У межах цього блоку питань з'ясовують дані щодо:

– чисельності злочинного угруповання, якщо вона відома конкретному виконавцю;

– інтенсивності зв'язків між виконавцями кримінально протиправної діяльності;

– організаторів злочинного угруповання та інших осіб, які входять до його керівної ланки;

– моделі побудови злочинного угруповання;

по-четверте, дані щодо розподілу доходів, отриманих за результатами кримінально протиправної діяльності (99 %, п. 22 додатка Б). У межах цього блоку предмета допиту встановлюють:

– модель розподілу доходів між виконавцями кримінально протиправної діяльності: а) отримання відсотків від протиправних транзакцій; б) фіксована оплата за здійснення кримінально протиправної діяльності; в) спосіб і частота виплат; г) суб'єкт, який проводить виплати;

– банківські рахунки та будь-які фінансові інструменти, які використовували для отримання винагороди за здійснення кримінально протиправної діяльності.

Розглянемо предмет допиту організатора такого угруповання та осіб, які входять до його керівної ланки. Вважаємо, що його можна структурувати за такими блоками:

по-перше, мотиви та передумови створення злочинного угруповання для здійснення такої кримінально протиправної діяльності (87 %, п. 23 додатка Б);

по-друге, модель структурної побудови угруповання (розподіл ролей) і модель безпосереднього здійснення кримінально протиправної діяльності (66 %, п. 23 додатка Б);

по-третє, біографічні дані організатора й активних учасників, зокрема щодо їхньої попередньої трудової діяльності, з метою виявлення інших осіб, які можуть бути причетними до вчинення злочинів і не відомі працівникам правоохоронних органів (90 %, п. 23 додатка Б);

по-четверте, особливості забезпечення злочинного угруповання загалом й окремих виконавців необхідними апаратними засобами та програмним забезпеченням для вчинення злочинів (99 %, п. 23 додатка Б);

по-п'яте, дані щодо інфраструктурних елементів такої кримінально протиправної діяльності, зокрема системи зв'язків, які використовують для її забезпечення (60 %, п. 23 додатка Б);

по-шосте, форми та фінансові інструменти, які використовували для легалізації доходів, отриманих злочинним шляхом (86 %, п. 23 додатка Б);

по-сьоме, модель підбору нових учасників угруповання (71 %, п. 23 додатка Б).

Безумовно, запропонована нами структура предмета допиту не є вичерпною, а лише типовою і повинна коригуватися залежно від слідчої ситуації, яка склалася на відповідному етапі розслідування, особливостей технології кримінально протиправної діяльності, кількості встановлених і затриманих учасників кримінально протиправної діяльності тощо.

Продовжуючи, слід спрямувати увагу на аналіз окремих організаційно-тактичних особливостей проведення обшуку під час розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору. З огляду на предмет і межі нашого дослідження, ми залишаємо поза увагою кримінальні процесуальні питання, які стосуються порядку санкціонування проведення обшуку, а також загальні організаційно-тактичні аспекти його проведення, оскільки їх уже ґрунтовно досліджено в науці [13; 35; 40; 73; 94; 107; 178; 182; 183; 197].

На переконання О. Тарасенка, особливості проведення обшуку під час розслідування кримінальних правопорушень, пов'язаних із поширенням протиправного контенту в мережі Інтернет, залежать від таких ознак: 1) протиправну діяльність здійснює одна, декілька чи значна кількість осіб (понад п'ять); 2) таку діяльність здійснюють приховано чи законспіровано (з використанням знарядь і засобів, які ускладнюють пошук злочинців, наприклад, на закинутих промислових чи охоронюваних об'єктах, бункерах); 3) таку діяльність здійснюють з метою отримання коштів, здобутих злочинним шляхом, або ж вона має ідейний характер; 4) розповсюдження протиправного контенту здійснюють в Україні чи на зарубіжних інтернет-сайтах [171, с. 348].

У межах розслідування аналізованої кримінально протиправної діяльності здійснений аналіз кримінальних проваджень засвідчує, що можна виокремити дві тактичні ситуації проведення обшуку, які визначають його особливості: по-перше, проведення обшуку на початковому етапі розслідування одразу після початку кримінального провадження; по-друге, проведення обшуку на подальшому етапі розслідування, коли підставами для його проведення є фактичні дані, отримані за результатами проведення першочергових СРД.

У *першій ситуації*, на нашу думку, організаційно-тактичні особливості обшуку полягають у тому, що: а) інформаційною основою для проведення обшуку є матеріали оперативного підрозділу, які стали підставою для початку кримінального провадження; б) проведення такої СРД є наслідком

необхідності реагування на отриману інформацію з метою недопущення втрати фактичних даних, які можуть бути доказами в кримінальному провадженні, а також речових доказів і документів; в) проведення одночасних обшуків у різних місцях, що передбачає необхідність залучення значної кількості ресурсів і виокремлення пріоритетного місця обшуку, який організовуватиме безпосередньо слідчий, що здійснює досудове розслідування; г) поєднання таких обшуків з іншими процесуальними діями, наприклад, затриманням осіб за підозрою в причетності до кримінально протиправної діяльності. На нашу думку, у класифікаційній системі СРД такий обшук можна віднести до пошукових слідчих дій, а безпосередні тактичні особливості його проведення істотно збігаються з особливостями проведення огляду, окресленими вище.

Водночас *друга тактична ситуація* проведення обшуку має певні відмінності, які пов'язані насамперед з поінформованістю злочинців щодо початку кримінального провадження та проведення слідчим відповідної системи СРД і НСРД. Зважаючи на це, видається, що тактичні завдання такого обшуку матимуть певну специфіку, зокрема до них слушно віднести:

– виявлення апаратних засобів і програмного забезпечення, яке використовували для здійснення кримінально протиправної діяльності та переховують злочинці з метою протидії розслідуванню. Необхідно зауважити, що, на відміну від переважної більшості злочинів загальнокримінальної спрямованості, засоби такої кримінально протиправної діяльності є коштовними, з огляду на їх адаптацію до реалізації конкретної технології вчинення злочинів економічної спрямованості, тому їх не знищують злочинці, а переміщають з метою приховання та подальшого використання в злочинній діяльності чи реалізації іншим особам;

– виявлення матеріальних цінностей, які отримано за результатами кримінально протиправної діяльності;

– виявлення та вилучення інших речових доказів і документів, які можуть бути долучені до матеріалів кримінального провадження;

– виявлення та копіювання цифрових слідів кримінально протиправної діяльності.

У цьому випадку необхідно зосередити увагу на безпосередній залежності мети слідчої дії, тактики її підготовки та проведення, оскільки останню спрямовують на виявлення та вилучення речових доказів і документів, а не на документування роботи апаратних засобів та програмного забезпечення в реальному режимі часу. Водночас, на нашу думку, планування проведення обшуку в такій тактичній ситуації потребує використання методології тактичного кримінального аналізу з метою прийняття слідчим правильних управлінських та організаційно-тактичних рішень. Зокрема, першочергової оцінки потребує аналіз джерела інформації, яка є підставою для проведення обшуку, оскільки в окремих випадках в умовах здійснення активної протидії розслідуванню можливою є дезінформація слідчого з метою створення сприятливих умов для приховування засобів кримінально протиправної діяльності злочинцями, які не відомі правоохоронним органам. У зв’язку із цим, вважаємо, що підготовчий етап обшуку в такій слідчій ситуації охоплює такі дії:

– оцінка джерела отримання інформації, яка є підставою для проведення обшуку;

– оцінка відношення джерела до інформації, яку воно повідомляє. Наприклад, у разі повідомлення даних щодо місця знаходження апаратних засобів та інших доказів, які підтверджують факти кримінально протиправної діяльності, яку здійснювали з використанням кіберпростору, слідчому слушно з’ясувати й оцінити мотиви надання підозрюваним такої інформації, оскільки в окремих випадках це може бути використано як тактичний прийом протидії розслідуванню та створення умов для не встановлених слідством осіб щодо переміщення знарядь вчинення злочину та їх реалізації;

– визначення залежностей між отриманою інформацією та іншими фактичними даними, які містяться в матеріалах кримінального провадження;

– підготовка засобів для коректного вилучення, упаковки і транспортування вилучених апаратних засобів, інших речових доказів та документів;

– залучення спеціаліста з метою забезпечення коректності вилучення апаратних засобів і копіювання цифрових доказів. Під час обшуку, огляду чи тимчасового доступу до засобів комп'ютерної техніки, зазначає О. Самойленко, створюють абсолютно ідентичний оригіналу екземпляр інформації у формі документа як процесуального джерела доказів. Ступінь зберігання інформації на «копії» становить 100 %, копіювання жодного традиційного в криміналістиці сліду не має такого показника. Слід акцентувати, що власник, володілець або утримувач комп'ютерної системи, яку досліджують, може застосувати різні способи захисту від копіювання. За такої умови ідентичне копіювання буде неможливе, що обґрунтовує фізичне вилучення носія інформації під час обшуку для його вивчення та подолання систем захисту в процесі проведення відповідної судової експертизи [158].

Підсумовуючи викладене, слід зауважити, що під час досудового розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють з використанням кіберпростору, основним інструментом збирання доказів залишаються СРД, організація і тактика проведення яких адаптується до особливостей механізму такої кримінально протиправної діяльності. Тож можна виокремити такі особливості їх проведення: необхідність підготовки та використання спеціальних засобів для фіксації цифрової інформації, яка функціонує у цифровій формі; обов'язкове залучення спеціаліста у сфері інформаційних технологій для надання консультативної та іншої допомоги слідчому; необхідність ужиття нетрадиційної системи заходів, що спрямована на забезпечення ефективності СРД, зокрема недопущення знищення цифрових доказів під час її безпосереднього проведення.

3.3. Особливості проведення окремих негласних слідчих (розшукових) дій

Прийняття нового кримінального процесуального законодавства розв'язало важливу прикладну проблему в частині зближення кримінальної процесуальної та оперативно-розшукової діяльності шляхом запровадження інституту НСРД, що своєю чергою оптимізувало розслідування різних форм кримінально протиправної діяльності. Не є винятком і розслідування різних форм кримінально протиправної діяльності, яку здійснюють з використанням кіберпростору, оскільки значну частину фактичних даних під час розслідування останньої отримують шляхом проведення дій, які передбачають обов'язкове використання технічних засобів і програмного забезпечення різного функціонального призначення.

Безумовно, система та функціональна спрямованість НСРД є важливою науковою проблемою, яка потребує перманентного й системного аналізу. Водночас необхідно зазначити, що систему, процесуальні й організаційно-тактичні особливості проведення НСРД ґрунтовно досліджували вчені [19; 23; 68; 101; 128; 162; 163; 164; 185; 189], тому ми не акцентуємо на аналізі цих положень. Водночас зосередимо увагу на наявності нормативно визначеної залежності між можливістю проведення НСРД під час розслідування та тяжкістю кримінального правопорушення, відповідно до ст. 12 КК України. З огляду на це, а також те, що досліджувані нами злочини, згідно з кримінально-правовою класифікацією, належать до злочинів середньої тяжкості, використання окремих НСРД під час розслідування є неможливим. Водночас практика роботи підрозділів кіберполіції дає підстави стверджувати, що можливості окремих НСРД активно використовують під час розслідування злочинів цієї категорії.

Опрацювання практичних матеріалів підрозділів кіберполіції дає змогу запропонувати умовну класифікацію НСРД, які проводять під час

розслідування злочинів цієї категорії, на дві групи, залежно від їх пріоритетної функціональної спрямованості:

– негласні слідчі (розшукові) дії, які за функціональним призначенням у більшості випадків спрямовані на забезпечення підготовки та проведення інших слідчих дій;

– негласні слідчі (розшукові) дії, які за функціональним призначенням спрямовані на формування фактичних даних, які можуть бути доказами під час розслідування.

Безумовно, така класифікація не є безапеляційною, адже функціональним призначенням будь-якої слідчої дії є формування фактичних даних, які можуть бути використані як докази під час розслідування певного кримінального провадження. Водночас практика роботи підрозділів кіберполіції засвідчує, що на початковому етапі розслідування деякі НСРД проводять з метою: а) перевірки й уточнення інформації, яка міститься в початкових матеріалах, зокрема матеріалах оперативного підрозділу, за якими розпочато кримінальне провадження; б) отримання інформації, яка необхідна для якісного подальшого планування досудового розслідування; в) отримання інформації, необхідної для організаційно-тактичного забезпечення проведення СРД на подальшому етапі розслідування тощо.

Крім того, у контексті розслідування кримінальних проваджень щодо кримінально протиправної діяльності економічної спрямованості, здійснюваної з використанням кіберпростору, на нашу думку, негласні слідчі (розшукові) дії залежно від об’єкта спрямування можна додатково поділити на такі підгрупи: а) НСРД, які спрямовані на отримання інформації у фізичному середовищі; б) НСРД, які спрямовані на отримання інформації в кіберпросторі чи з транспортних телекомунікаційних систем.

Аналізуючи особливості розслідування високотехнологічних злочинів різних типів, учені залишають поза увагою окремі НСРД, які не пов’язані з виявленням інформації у фізичному середовищі щодо кримінально протиправної діяльності особи чи групи осіб, а також інших фактичних даних,

які мають значення для прийняття організаційно-тактичних рішень у межах розслідування кримінального провадження. На нашу думку, системно підходячи до аналізу цієї проблематики, необхідно зауважити, що суб'єкт кримінально протиправної діяльності функціонує не лише в кіберпросторі, а й у фізичному (традиційному) середовищі, де вчиняє дії, виявлення та фіксація яких може мати вагоме значення і для досліджуваних нами кримінальних проваджень. Зважаючи на викладене, необхідно акцентувати на спостереженні за особою, місцем або річчю як на самостійній НСРД. Проведене дослідження засвідчує, що, з організаційно-тактичних позицій, ця НСРД не має суттєвих особливостей щодо організації і тактики її проведення під час розслідування таких кримінальних проваджень, тому ми спрямовуємо увагу на її функціональній спрямованості під час розслідування. Для її проведення необхідним є існування певних передумов, зокрема наявності в слідчого фактичних даних, які свідчать про можливість причетності конкретної особи до вчинення такого кримінального правопорушення, оскільки, з огляду на анонімність користувачів мережі, встановлення особи злочинця є одним із найскладніших завдань під час розслідування такого виду кримінальних проваджень. Функціонально така НСРД може бути спрямована на:

– отримання системи установчих даних щодо особи з метою аналітичного опрацювання даних щодо її особистості, складання різного типу профілів і планування досудового розслідування. Опрацювання результатів такої НСРД у контексті порівняння з даними щодо активності користувача в мережі дає змогу: а) встановити взаємозв'язки між конкретною особою та відомим слідству користувачем мережі, тобто частково виконати завдання щодо ідентифікації користувача мережі; б) визначити локалізацію апаратних засобів і програмного забезпечення, з якого здійснюють підключення до мережі з метою здійснення протиправної діяльності, у випадках неможливості чи технічної складності виконати таке завдання за допомогою технічних засобів; в) вирішити організаційно-тактичні завдання щодо структурування

СРД і формування можливої алгоритмізованої моделі їх проведення в межах кримінального провадження;

– встановлення системи зв’язків особи, що дає змогу: а) ідентифікувати осіб, які причетні до безпосередньої реалізації кримінально протиправної діяльності, адже опрацювання матеріалів практики засвідчує, що злочинні угруповання під час вчинення таких злочинів доволі часто створюють з осіб, які знайомі між собою, зокрема й шляхом втягнення злочинцем свого оточення в кримінально протиправну діяльність економічної спрямованості, які вчиняють з використанням кіберпростору; б) ідентифікувати осіб, які забезпечують здійснення такої кримінально протиправної діяльності, зокрема:

а) осіб, які здійснюють індивідуальну модернізацію апаратних засобів під конкретний запит клієнта, а також можуть забезпечити особу периферійними засобами, що необхідні для забезпечення відповідної потужності ЕОМ і безперебійної роботи для реалізації злочинного задуму;

б) осіб, які за рівнем знань і кваліфікації можуть надавати відповідне програмне забезпечення чи застосунки, які необхідні для здійснення кримінально протиправної діяльності;

– встановлення місця розташування основної маси апаратних засобів і програмного забезпечення, що використовують у злочинній діяльності;

– вивчення приміщень, де сконцентровано основні апаратні засоби, які використовують у злочинній діяльності, зокрема: а) оцінка можливості доступу до такого приміщення; б) план-модель такого приміщення для встановлення наявності інших виходів тощо; в) наявність постійної охорони приміщення та її озброєність тощо.

Ще однією НСРД, яка має значення та дає результат, є установлення місцезнаходження радіоелектронного засобу. Суть цієї НСРД полягає в застосуванні технічних засобів для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного терміналу системи зв’язку й інших радіовипромінювальних пристроїв, активованих у межах операторів рухомого (мобільного) зв’язку, без висвітлення змісту повідомлень, які

передають, якщо в результаті його проведення можна встановити обставини, які мають значення для кримінального провадження. Унаслідок її проведення можна встановити низку обставин, які мають значення в кримінальному провадженні. Серед них: 1) місцезнаходження в певний час або проміжок часу (до моменту вчинення, під час або після вчинення кримінального правопорушення пристроїв, активованих у мережі операторів мобільного зв'язку, що належать або були на той час у користуванні осіб, які можуть бути причетними до вчинення кримінального правопорушення, свідків, потерпілого); 2) місце розташування в реальному часі таких пристроїв. Крім того, виявивши всі активні мобільні телефони, що знаходилися в певній місцевості в певний час, можливо встановити: номер абонента користувача інтернету за допомогою мобільного терміналу за протоколом «gprs/edge/ cdma», у разі якщо відомі його IP адреса і час виходу в інтернет за цією адресою; адреси розташування та номери базових станцій, які забезпечували зв'язок кінцевого обладнання з визначеними абонентськими номерами; види послуги, обсягу наданої послуги, суми коштів до сплати за кожен сеанс зв'язку; типи з'єднання визначеного абонента; вхідні й вихідні дзвінки, повідомлення; дату і тривалість з'єднання (час початку та закінчення кожного сеансу зв'язку) визначеного абонента, зокрема з'єднання нульової тривалості (неприйняті виклики); адресу місцеперебування споживача зазначеного абонентського номера в момент кожного з'єднання тощо.

Фактично слідчий ініціює її проведення в кримінальних провадженнях різного ступеня тяжкості задля визначення параметрів базових станцій операторів телекомунікацій, що забезпечують роботу в певному місці кінцевого обладнання систем зв'язку, і місцезнаходження інших радіовипромінювальних пристроїв, активованих у мережі операторів рухомого (мобільного) зв'язку. Це місце може бути об'єктом огляду як місце події. Отримана інформація також дає змогу конкретизувати операторів і провайдерів телекомунікаційних послуг, зв'язку, абонента. Стосовно обставин надання телекомунікаційних послуг оформлюють запити чи здійснюють

заходи забезпечення кримінального провадження. Аналогічну інформацію може бути отримано в межах оперативно-розшукової справи або під час перевірки первинної інформації. Зазначене положення є важливим для слідчого з позицій оптимізації процесу розслідування, адже його локальним завданням стосовно цієї НСРД є своєчасність ініціативи щодо проведення необхідної дії або заходу, тим самим недопущення дублювання останніх [158, с. 255].

Загалом поділяючи запропоновані підходи, необхідно визначити основні блоки завдань, які виконують за допомогою цієї НСРД під час розслідування досліджуваних форм кримінально протиправної діяльності, а саме:

– встановлення всіх учасників кримінально протиправної діяльності. Безумовно, таке комплексне завдання розслідування виконують за допомогою системи слідчих дій та інших процесуальних заходів, але проведення цієї НСРД на початковому етапі оптимізує розслідування в частині: а) звуження кола осіб, які потребують встановлення та відпрацювання в межах кримінального провадження; б) формування в слідчого організаційно-тактичної пріоритетності щодо необхідності проведення першочергових слідчих дій з конкретними учасниками кримінального провадження; в) алгоритмізує процес розслідування, зокрема забезпечує можливість стратегічного планування послідовності проведення інших СРД, зокрема допитів. Надзвичайно корисною за результатами проведення цієї НСРД є інформація, яку надалі опрацьовують спеціалісти з кримінального аналізу, що дедалі частіше використовують в оперативно-розшуковій та слідчій діяльності, та формування для слідчого зручних у використанні аналітичних продуктів (схем, матриць тощо). У цьому контексті необхідно зауважити, що, аналізуючи результати такої НСРД під час розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору, необхідно охоплювати хронологічно тривалий проміжок часу та за можливості (наявність достатніх вихідних даних на початку розслідування)

здійснювати умовний поділ на періоди: а) підготовка до здійснення кримінально протиправної діяльності; б) безпосередня кримінально протиправна діяльність.

Зазначений підхід зумовлений тим, що структурно-функціональне забезпечення цих стадій кримінально протиправної діяльності різниться. Зокрема, акцент слідчого лише на періоді безпосередньої реалізації злочинного задуму призводить до залишення поза увагою осіб, які брали участь у розробленні та підготовці до реалізації відповідної технології кримінально протиправної діяльності, але не брали участі на інших стадіях вчинення злочину. Встановлення таких осіб є необхідним для забезпечення повноти розслідування, а в разі наявності в їхніх діях складу кримінального правопорушення – притягнення їх до кримінальної відповідальності.

Необхідно також зауважити, що в цьому випадку досліджувана НСРД не виконує завдання щодо встановлення ролі кожного учасника в злочинній діяльності, тому є передумовою для проведення інших СРД і тактичних операцій на відповідній інформаційній основі;

– встановлення місця реалізації відповідної злочинної технології. Вище зазначено, що цю кримінально протиправну діяльність здійснюють у специфічному середовищі – кіберпросторі. Водночас під час її розслідування значну частину фактичних даних можна отримувати й у звичному середовищі, оскільки для реалізації таких технологій необхідним є використання складних апаратних засобів, а також їх значної кількості, що вимагає специфічних умов електропостачання, охолодження та розміщення для використання в злочинній діяльності. Фактично можна стверджувати, що, попри те, що безпосередню кримінально протиправну діяльність здійснюють у кіберпросторі, засоби для її забезпечення мають фізичний вимір у конкретному місці. Отже, аналітичне опрацювання місця розташування термінала мобільного зв’язку та зіставлення таких даних із відповідними часовими показниками, а також даними щодо пріоритетного знаходження інших терміналів, з якими контактує абонент, дають змогу виявити

місцезнаходження основної частини апаратних засобів і програмного забезпечення, яке використовують у такій злочинній діяльності, що дає змогу провести обшуки й інші слідчі (розшукові) дії фіксуючого характеру, а також вилучити предмети та документи, які можуть бути доказами в кримінальному провадженні;

– забезпечення реалізації окремих тактичних прийомів під час проведення інших слідчих дій, зокрема демонстрації допитуваному аналітичних продуктів, сформованих за результатами аналізу даних, для спростування його показань, виявлення фактів неправдивої дачі показань тощо.

Проаналізуємо також зняття інформації з електронної інформаційної системи. Ми поділяємо позицію О. Тарасенка, який вважає, що ця НСРД передбачає ретельну підготовку під час її проведення, використання спеціальних знань, навичок і програмних засобів з метою проникнення до інформаційної системи, пошуку й відбирання інформації. Можливість використання програмних засобів під час проведення зняття інформації з електронної інформаційної системи потребує нормативного врегулювання з метою ефективного та повноцінного використання інформаційних технологій з пошуку, встановлення та вилучення необхідної інформації. Інші вчені слушно зауважують, що зняття інформації з електронних інформаційних систем може мати характер розвідувальної чи контррозвідувальної інформаційно-пошукової діяльності або ж пізнавально-фіксувальної, засвідчувальної, доказової діяльності, яку найчастіше застосовують у сфері кримінального процесуального судочинства [118].

Увагу зосередимо на знятті інформації з електронних інформаційних систем без відома її власника, володільця чи утримувача (ст. 264 КПК України). Згідно з твердженням О. Самойленко, цю НСРД слідчий ініціює виключно в кримінальному провадженні щодо тяжких чи особливо тяжких злочинів, її проводять на підставі дозволу слідчого судді на втручання в приватне спілкування. Проведення такої НСРД потребує спеціальних знань у

галузі інформаційних технологій. Нині таким спеціалістом є інспектор кіберполіції, який за допомогою програмних і технічних засобів, призначених для подолання обмежень доступу до електронної інформації, встановлених власником певної інформаційної системи, отримує доступ до інформації в конкретній системі, розшифровує, обробляє, систематизує цю інформацію та копіює її. Увесь документальний обіг щодо її проведення здійснюють з дотриманням режиму секретності, а в більшості випадків протокол за результатами проведення такої НСРД складає безпосередньо слідчий [158].

У контексті безпосереднього проведення такої НСРД ми поділяємо позицію В. Луцика, який зазначає, що всі способи зняття інформації з електронних інформаційних систем можна об'єднати в дві основні групи.

Перша група – це способи безпосереднього доступу. Під час їх реалізації інформацію отримують шляхом видачі відповідних команд з комп'ютера, на якому ця інформація знаходиться.

Друга група охоплює способи опосередкованого (віддаленого) доступу до комп'ютерної інформації. До них можна віднести:

підключення до лінії зв'язку користувача (наприклад, до телефонної лінії або оптоволоконної лінії) та отримання цим шляхом доступу до електронної інформаційної системи;

проникнення в комп'ютерну систему за допомогою підбору паролів тощо.

До способів опосередкованого (віддаленого) доступу до комп'ютерної інформації належать безпосереднє та електромагнітне перехоплення.

Безпосереднє перехоплення – найпростіший спосіб доступу до електронної інформаційної системи. Перехоплення здійснюють або безпосередньо через зовнішні комунікаційні канали системи, або шляхом підключення до ліній периферійних пристроїв. Об'єктами безпосереднього перехоплення є кабельні та дротові системи, наземні мікрохвильові системи, системи урядового зв'язку.

Електромагнітне перехоплення. Сучасні технічні засоби дають змогу отримати інформацію без безпосереднього підключення до електронної інформаційної системи за рахунок перехоплення випромінювань центрального процесора, дисплея, комунікаційних каналів, принтера тощо. Усі ці дії можна вчинити, перебуваючи на значній відстані від об'єкта перехоплення (наприклад, використовуючи спеціальну апаратуру, можна «знімати» інформацію з електронної інформаційної системи, розташованої в сусідньому приміщенні, будівлі. Сучасні технічні засоби дають змогу знімати й розшифрувати випромінювання принтера, який працює, на відстані до 150 м, а випромінювання моніторів і з'єднувальних кабелів – до 500 м.

У протоколі негласної слідчої дії підлягають відображенню такі відомості: у пам'яті якого пристрою виявлено віртуальні сліди; кому належить пристрій; чи має пристрій вихід у мережу Інтернет, інші телекомунікаційні або локальні мережі; яка оперативна система функціонує на пристрої (Windows, Linux – на комп'ютері, Windows mobile, Android, Symbian – на мобільному телефоні, комунікаторі, планшеті тощо); у яких файлах виявлено сліди втручання, які саме; коли файл було створено, змінено, відкривали востаннє. Щоб уникнути вивчення кожного файлу комп'ютера (кількість файлів може сягати сотень тисяч), до проведення негласної слідчої дії необхідно залучати спеціаліста (програміста, системного адміністратора та ін.) [102]. Також слушною видається позиція вчених, які зазначають, що в слідчій практиці трапляються ситуації, коли необхідно вилучити (зняти) інформацію, яка знаходиться на електронному носії (смартфоні, планшеті, ноутбуці тощо), вилученому під час проведення процесуальних дій (обшук, огляд місця події тощо). Так виникає «помилка» практики огляду такого носія або ж його направлення експерту (проведення експертного дослідження) з метою вилучення та дослідження змісту відповідної інформації. Правильним є прийняття рішення про проведення НСРД, що передбачена ч. 1. ст. 264 КПК України, і залучення відповідної особи до зняття інформації [171].

У контексті досліджуваних нами форм кримінально протиправної діяльності слід зазначити, що інформація, яку отримують унаслідок такої НСРД, може бути класифіковано на такі види:

– фактичні дані щодо організаційно-структурної побудови злочинного угруповання, яке здійснює таку злочинну діяльність, оскільки аналітичне опрацювання даних дає змогу: а) виокремити осіб, які систематично вчиняють однотипні дії, що відображають елементи конкретної технології кримінально протиправної діяльності; б) визначити осіб, які забезпечують етапи посткримінальної діяльності конкретних суб'єктів, наприклад, легалізацію (відмивання) доходів, отриманих за результатами кримінально протиправної діяльності, та/або зміну форми таких активів, зокрема їх переведення в інноваційні платіжні засоби, які недостатньо контрольовані державними фінансовими інституціями; в) виокремлення осіб, які виконують координаційні й управлінські функції в структурі конкретної кримінально протиправної діяльності;

– інформація щодо осіб, які ситуативно причетні до вчинення таких злочинів, а також потенційних жертв кримінально протиправної діяльності. Необхідно акцентувати на особливій важливості такого напряму роботи під час розслідування, оскільки практика роботи підрозділів кіберполіції свідчить про високу латентність злочинів економічної спрямованості, які вчиняють з використанням кіберпростору, що зумовлено такими чинниками: а) заволодіння злочинцями сумою коштів, яка не є критично важливою для особи, як наслідок – жертва злочинного посягання не звертається до правоохоронних органів; б) заволодіння такими коштами шляхом зловживання довірою, що створює в жертви злочину певні психологічні перешкоди для звернення до правоохоронних органів через небажання розголошення; в) приховування окремими суб'єктами господарської діяльності та фінансовими інституціями фактів вчинення щодо них протиправних дій з метою уникнення дискредитації та формування в клієнтів недовіри щодо надійності систем захисту та зберігання активів;

– дані щодо технології кримінально протиправної діяльності, зокрема системи способів і засобів, які використовують для вчинення таких кримінальних правопорушень. У контексті цього увагу необхідно зосередити на тому, що на початковому етапі розслідування слідчий обізнаний щодо типу апаратних засобів і програмного забезпечення, яке використовують для вчинення злочинів, а проведення такої НСРД дає змогу конкретизувати дані, що оптимізує проведення окремих СРД у частині вибору оптимальної методики фіксації цифрових доказів і подолання логічних систем захисту в разі необхідності, зокрема під час проведення обшуків;

– дані щодо фінансових інструментів, які використовують злочинці, зокрема в частині визначення платіжних засобів і засобів, які забезпечують зберігання коштів, отриманих за результатами кримінально протиправної діяльності;

– інша інформація, яка може бути використана як доказ у кримінальному провадженні.

Необхідно також зауважити, що для розслідування злочинів цієї категорії характерною є відповідна структурно-логічна схема проведення СРД, тому аналізовану нами вище НСРД проводять здебільшого на початковому етапі розслідування, оскільки вона забезпечує формування інформаційної основи для проведення перевірочних СРД. Логіка організаційно-тактичних рішень під час розслідування цієї форми кримінально протиправної діяльності засвідчує, що оптимальним є проведення такої НСРД до повідомлення особі про підозру чи проведення інших СРД за її участю. Зазначене насамперед зумовлено тим, що в разі усвідомлення особою факту потрапляння у поле контролю правоохоронних органів, з огляду на високий рівень технічної підготовки таких осіб, вони негайно вживають заходів щодо захисту своїх комп’ютерних систем від негласного проникнення та витоку інформації. З тактичного погляду, досліджувана НСРД під час розслідування виконує функцію негласного документування окремих складових технології такої кримінально

протиправної діяльності. Додатково необхідно зауважити, що такий комплекс дій можуть також проводити в межах оперативно-розшукової справи до початку кримінального провадження. У цьому випадку в разі належної фіксації всіх обставин, що підлягають документуванню, проведення аналогічної за змістом НСРД є недоцільним на початковому етапі розслідування.

Також у контексті організаційно-тактичних особливостей проведення такої НСРД необхідно зауважити, що її здійснюють через реалізацію віддаленого доступу, зважаючи на можливості підрозділів кіберполіції, а безпосередній доступ у разі необхідності здійснюють під час проведення інших СРД, зокрема обшуку з урахуванням змін, внесених до КПК України.

Сукупність таких технічних і програмних засобів для проведення зазначеної НСРД становить окремий вид спеціальних технічних засобів для зняття інформації з каналів зв'язку й інших технічних засобів негласного отримання інформації. Автори визначають їх як створені або модернізовані та пристосовані з наданням нової якості й властивості технічні засоби, обладнання, інструменти, програмне забезпечення, препарати та інші вироби, які за своєю технічною забезпеченістю або безпосередньою обумовленістю їх застосування придатні для негласного отримання інформації або доступу до неї в прихований спосіб під час виконання завдань оперативно-розшукової, контррозвідувальної, розвідувальної діяльності або проведення НСРД [36].

Водночас слід зауважити, що однією з важливих організаційно-тактичних проблем залишається відсутність переліку програмних засобів, які можуть бути використані для проникнення у відповідну систему та зняття інформації. З одного боку, відсутність такого переліку видається цілком обґрунтованою, оскільки динаміка розвитку інформаційних технологій вимагає постійної адаптації таких засобів, у практичній діяльності відбувається конкуренція засобів доступу до системи й відповідно її захисту, а з другого – така ситуація створює певні загрози щодо можливості використання отриманих даних у доказуванні, оскільки доцільним є

використання сертифікованих продуктів для уникнення помилок під час отримання таких даних. Досліджуючи питання використання цифрової інформації, Д. Цехан зазначає, що ключовим фактором її використання в кримінальному судочинстві є коректна фіксація та подальша незмінність. У кожній ситуації необхідним є дотримання вимог щодо коректності фіксації інформації. Будь-яке програмне забезпечення може містити помилки, які можна класифікувати на систематичні та спорадичні (епізодичні). Виявлена помилка повинна відповідати трьом умовам: бути підтвердженою службою технічної підтримки виробника програмного забезпечення, його уповноваженим представником або компетентною організацією, яка вивчає та узагальнює помилки програмного забезпечення; помилка повинна безпосередньо стосуватися фіксації інформації, саме тому могла призвести до її модифікації, що підтверджено висновком експерта; модифікувала під час фіксації саме ту інформацію, яка має значення для доказування, що підтверджують висновком експерта [186]. У нормативних документах немає визначення програмних засобів як засобів негласного отримання інформації. На думку дослідників, під час визначення поняття програмних засобів негласного зняття інформації передусім слід зауважити, що програмним засобом негласного зняття інформації є не технічний пристрій, а виключно комп'ютерна програма, яка діє на основі технічного пристрою, що може бути в загальному вжитку. Комп'ютерна програма – це набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування (комп'ютером), які приводять його в дію для досягнення певної мети або результату [168]. Ми поділяємо думку С. Шитого й І. Огороднікової стосовно визначення програмних засобів негласного зняття інформації як: набору інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для зчитування ЕОМ або комп'ютером, які приводять його в дію для негласного отримання інформації з каналів зв'язку, інших ЕОМ, комп'ютерів, пристроїв із функцією комп'ютера, технічних, електронних або цифрових

пристроїв і відповідають критеріям належності до засобів негласного отримання інформації, призначені для використання в прихований спосіб, характерний для оперативно-розшукової, контррозвідувальної або розвідувальної діяльності [200].

Виконання завдань цією НСРД можливо за допомогою програмно-апаратного комплексу «Cellebrite UFED». За допомогою цього технічного засобу можливо отримати інформацію з таких месенджерів, як: Viber, WhatsApp, Telegram тощо. Крім цього, шляхом застосування цього технічного засобу можна отримати доступу до хмарних сховищ інформації. Відбувається це за рахунок:

– вилучення з мобільного пристрою тимчасових ключів авторизації;

– відновлення видаленої інформації, зокрема фотографій;

– побудови маршрутів пересування шляхом аналізу історії використання точок доступу до «Wi-Fi» тощо.

Проаналізуємо особливості зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи не пов’язаний з подоланням системи логічного захисту, як одного з двох видів такої НСРД, як зняття інформації з електронних інформаційних систем [134]. Згідно з результатами аналізу практики опрацювання матеріалів підрозділів кіберполіції, основним функціональним призначенням такої НСРД під час розслідування досліджуваних нами форм кримінально протиправної діяльності є встановлення додаткових даних щодо особи злочинця, які необхідні слідчому для прийняття відповідних організаційно-тактичних рішень. Таку НСРД реалізують через пошук слідчим або інспектором кіберполіції (за дорученням слідчого) в різноманітних інтернет-спільнотах відкритої інформації про особу злочинця.

Виконавець за результатами дії складає протокол, у якому фіксує такі відомості:

– персоналізовані відомості про особу злочинця;

– ознаку, за якою об’єднують коло осіб, що потрапляють під підозру;

– зв’язки особи, що потрапила під підозру;

– відомості, що можуть сприяти виконанню інших тактичних завдань (пошук свідків, потерпілих, забезпечення встановлення мотивів злочину тощо).

До протоколу зняття інформації з електронних інформаційних систем або її частини додають відповідні носії електронної інформації, що містять файли з відеограмою та зображенням екрана монітора (або знімками екрана), створеними під час дослідження системи, також їх роздруківки як додатків до протоколу.

Проведення цієї дії не потребує дозволу слідчого судді, не обмежує приватності спілкування осіб і не залежить від тяжкості злочину, який розслідують. Єдине, у чому може виникнути потреба під час її провадження, – це застосування технічного та програмного обладнання (через значний обсяг опрацьовуваної інформації або використання злочинцем під час вчинення злочину закордонного сегмента мережі Інтернет). На відповідному фаховому рівні застосовувати таке обладнання (програмні засоби) може спеціаліст, тому в абсолютній більшості випадків доручають проведення цієї НСРД інспектору кіберполіції. Якщо персоналізацію особи здійснено під час ОРД, то сенсу в цій дії на початковому етапі розслідування не буде. Водночас на практиці її проводять з метою отримання формальних підстав для обґрунтування подальших СРД, що вимагають погодження з прокурором або звернення до слідчого судді (обшуку за певною адресою, тимчасового доступу до документів конкретного постачальника інтернет-послуг тощо) [158, с. 254].

Аналіз функціональної спрямованості та сутності такої НСРД дає підстави стверджувати про її спрямованість на встановлення осіб, які вчинили кримінальні правопорушення (їх персоналізацію) та інших осіб, причетних до здійснення відповідної кримінально протиправної діяльності. Водночас зауважимо, що під час досудового розслідування доцільним є проведення такої НСРД, коли слідчому необхідні фактичні дані в порядку, визначеному

КПК України, для використання їх у процесуальній комунікації з прокурором чи судом, зокрема отримання ухвали щодо проведення СРД, які потребують санкціонування.

В інших випадках, зокрема за потреби отримати інформацію, яка необхідна для прийняття організаційно-тактичних рішень під час розслідування, можуть використовувати інші інструменти, що не потребують надмірного документального забезпечення на етапі підготовки до їх застосування.

Аналізуючи практику розслідування злочинів економічної спрямованості, які вчиняють з використанням кіберпростору, можна зазначити, що досліджувана НСРД має такі особливості:

а) її проводять на початковому етапі розслідування за браку детальної інформації про учасників кримінально протиправної діяльності;

б) проводять у разі початку кримінального провадження не за матеріалами оперативних підрозділів, що закономірно супроводжується високим рівнем інформаційної невизначеності;

в) її проведення може бути доручене інспектору кіберполіції або проводити буде безпосередньо слідчий за наявності в нього достатньої кваліфікації щодо використання апаратних засобів і програмного забезпечення;

г) результати, отримані внаслідок проведення такої НСРД, використовують: по-перше, для формування фактичних підстав з метою отримання дозволів на проведення НСРД, які пов’язані з втручанням у приватне спілкування; по-друге, прийняття організаційно-тактичних рішень у кримінальному провадженні; по-третє, для формування психологічного профілю особи з метою підготовки до проведення вербальних СРД.

Частково підсумовуючи, доходимо таких висновків: 1) порівняно з традиційними СРД, під час розслідування кримінально протиправної діяльності цієї категорії динаміка застосування НСРД є нижчою, що зумовлено, зокрема, і ступенем тяжкості таких злочинів; 2) додаткового

регулювання потребує використання програмних продуктів як різновиду спеціальних засобів для забезпечення проведення окремих НСРД, пов'язаних із втручанням у приватне спілкування.

Висновки до розділу 3

1. Зміст, початок реалізації, суб'єкти проведення тактичних операцій безпосередньо залежать від: підстав для початку кримінального провадження; типової слідчої ситуації, яка склалася на відповідному етапі розслідування кримінально протиправної діяльності економічної спрямованості, вчиненої з використанням кіберпростору.

2. Слідчі (розшукові) дії, які проводять під час розслідування злочинів цієї категорії, класифіковано за критерієм мети проведення на: а) пошукові СРД, спрямовані на отримання нових фактичних даних щодо вчиненого кримінального правопорушення, які раніше не були відомі слідству; б) перевірочні СРД, спрямовані на перевірку й підтвердження інформації, отриманої під час проведення інших СРД та інших процесуальних й оперативно-розшукових заходів.

До першої групи може бути віднесено такі СРД, як допит та огляд, а до другої групи – пред'явлення особи для впізнання, пред'явлення речей для впізнання, обшук, слідчий експеримент. Водночас такий розподіл слідчих дій є доволі умовним, оскільки окремі з них можуть бути віднесені до обох класифікаційних груп, зокрема обшук, який, з одного боку, спрямований на перевірку інформації, яка наявна в розпорядженні слідчого, а з другого – забезпечує виявлення раніше не відомих слідчому фактичних даних.

З метою конкретизації тактичних прийомів допиту слідчому необхідно акцентувати увагу на таких аспектах: а) вік допитуваної особи, оскільки до вчинення шахрайств із використанням інформаційних технологій доволі часто залучають неповнолітніх, які самостійно здобули достатні

компетентності для роботи в кіберпросторі та використання відповідних апаратних засобів і програмного забезпечення; б) сімейний стан особи, наявність у неї відповідної системи корисних соціальних зв'язків; в) чи притягували особу раніше до будь-яких форм кримінальної відповідальності, чи обізнана вона з методами та прийомами роботи слідчих підрозділів; в) ступінь задокументованості кримінально протиправної діяльності конкретної особи й наявність у кримінальному провадженні зібраних доказів, які за тактичної необхідності можуть бути продемонстровані особі, яку допитують; г) час встановлення причетності особи до кримінально протиправної діяльності економічної спрямованості, яку здійснюють з використанням кіберпростору. Такі блоки аналітичної оцінки слідчим під час підготовки до проведення допиту не є вичерпними й варіюються залежно від слідчої ситуації, яка склалася в розслідуванні на момент проведення цієї слідчої дії.

Негласні слідчі (розшукові) дії, що проводять під час розслідування злочинів цієї категорії, умовно розподілено на два види залежно від їх пріоритетної функціональної спрямованості: 1) НСРД, які за функціональним призначенням у більшості випадків спрямовані на забезпечення підготовки та проведення інших слідчих дій; 2) НСРД, які за функціональним призначенням спрямовані на формування фактичних даних, які можуть бути доказами під час розслідування.

Негласні слідчі (розшукові) дії залежно від об'єкта спрямування можна додатково поділити на такі підгрупи: а) НСРД, спрямовані на отримання інформації у фізичному середовищі; б) НСРД, спрямовані на отримання інформації в кіберпросторі чи з транспортних телекомунікаційних систем.

ВИСНОВКИ

У дисертації на підставі дослідження комплексу питань сформовано наукові положення методики виявлення та розслідування злочинів економічної спрямованості, вчинених з використанням кіберпростору, одержано результати, що в сукупності спрямовані на виконання наукового завдання в галузі криміналістичної методики й містять практичні рекомендації щодо розслідування кримінальних проваджень зазначеної категорії, зокрема:

1. Формами реакції держави на трансформацію соціально-економічного життя у зв'язку з розвитком кіберпростору є: криміналізація окремих форм людської діяльності, невід'ємною частиною якої є використання ЕОМ; встановлення як кваліфікуючої ознаки використання ЕОМ під час вчинення окремих видів традиційних злочинів, зокрема шахрайства; створення спеціалізованих суб'єктів, діяльність яких спрямована на виявлення та документування кримінально протиправної діяльності у сфері інформаційних технологій.

Специфіка наукових досліджень кіберпростору та пов'язаних із ним явищ зумовлена такими чинниками: 1) постійне розширення переліку кримінальних правопорушень, які можуть бути вчинені за допомогою різних складових інформаційних технологій; 2) безперервна модифікація способів вчинення таких злочинів, що прямо корелює з механізмом слідоутворення, як наслідок – організаційно-тактичними моделями проведення СРД і НСРД; 3) формування нових типів доказів – цифрових доказів, які постійно видозмінюються та потребують систематичного вивчення.

Науковий пошук у сфері протидії злочинам, які вчиняють з використанням кіберпростору, здійснюють за такими основними напрямами: а) форми й алгоритми використання інформаційних технологій у протидії злочинності; б) ознаки та сутність кіберпростору як середовища функціонування соціально-економічних процесів; в) особливості розслідування кіберзлочинів; г) особливості аналізу комп'ютерних об'єктів;

д) використання спеціальних знань під час розслідування комп'ютерних злочинів.

2. Взаємозв'язки між розвитком кіберпростору й окремими формами кримінально протиправної діяльності у сфері економіки виявляються в таких формах: *по-перше,* криміналізація окремих діянь, зумовлена широкомасштабним упровадженням інформаційних технологій та їх структурної складової – кіберпростору у всі форми суспільного життя; *по-друге,* якісна трансформація інфраструктури економічної злочинності, що зумовлена перетворенням кіберпростору на невід'ємну складову економічних відносин; *по-третє,* трансформація окремих способів вчинення економічних злочинів у складні технології кримінально протиправної діяльності; *по-четверте,* якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій; *по-п'яте,* формування цифрових кримінальних ринків.

Кіберпростір як складова інфраструктури економічної злочинності може виконувати такі функції: а) інтелектуальне й інформаційне забезпечення кримінально протиправної діяльності; б) створення умов для формування стійких безконтактних зв'язків між особами, які надалі можуть здійснювати спільну кримінально протиправну діяльність; в) забезпечення ринку збуту відповідних кримінальних послуг і кримінальних компетенцій.

Ознаками цифрових кримінальних ринків є: *по-перше*, транснаціональний характер і можливість функціонування на таких ринках агентів з будь-якої юрисдикції; *по-друге*, високий рівень анонімності агентів таких ринків і підвищення рівня активності за рахунок створення відповідної репутації на ринку; *по-третє*, можливість безконтактної передачі окремих видів товарів і послуг із використанням кіберпростору, окремих типів програмного забезпечення чи інших протиправних даних та/або контенту; *по-четверте*, використання специфічних інструментів оплати, зокрема криптовалютних та інших нетрадиційних засобів платежів.

3. *Кримінально протиправна діяльність економічної спрямованості, яку вчиняють із використанням кіберпростору*, – це систематична, багатоетапна протиправна діяльність особи (групи осіб), яку здійснюють за допомогою використання інформаційних технологій, забезпечують створенням необхідної інфраструктури та яка спрямована проти функціонування фінансово-економічної системи держави, фінансової діяльності юридичних і фізичних осіб.

Формування в особи задуму й умислу на здійснення кримінально протиправної діяльності з використанням кіберпростору безпосередньо залежить від таких чинників: *по-перше*, рівень професійних знань і навичок особи щодо організації фінансово-економічних процесів у кіберпросторі та можливостей використання кіберпростору як інфраструктурної складової для здійснення кримінально протиправної діяльності; *по-друге*, можливість застосування особою наявних знань і навичок у легальній сфері; *по-третє*, становище особи в професійній спільноті та приналежність до груп, які керуються відповідною субкультурою.

Типовими способами залучення спеціаліста на стадії підготовки кримінально протиправної діяльності економічної спрямованості, яку вчиняють із використанням кіберпростору, є: а) спеціаліст у сфері інформаційних технологій, який, надаючи консультативні послуги, не знає, що бере участь у підготовці вчинення злочинів; б) спеціаліст у сфері інформаційних технологій, який, надаючи консультаційні послуги, знає, що бере участь у підготовці злочину.

Типовими способами сприяння персоналу установи (організації) злочинцям є: а) умисне невжиття заходів щодо збереження паролів, іншої конфіденційної інформації та розголошення відомостей щодо конфіденційної інформації, яка знаходиться в мережі; б) невиконання належних заходів захисту, зокрема допуск до роботи в локальних мережах сторонніх осіб; в) неповідомлення керівництву чи правоохоронним органам про виявлені ознаки злочинної активності в мережі.

4. Інформація, необхідна для аналізу оперативної обстановки в кіберпросторі, упорядкована в такі групи: 1) детермінанти злочинів у кіберпросторі; 2) відомості про власників (або розпорядників) систем; 3) відомості про володільців інформації в системі; 4) наявні оперативні позиції на об'єкті оперативного обслуговування.

Пріоритетними об'єктами для формування та розстановки оперативних позицій є: Державна служба спеціального зв'язку та захисту інформації України та підпорядковані їй регіональні органи (управління в областях); Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації (НКРЗІ); національні оператори зв'язку; національні оператори та провайдери телекомунікацій; регіональні оператори та провайдери телекомунікацій; локальні оператори та провайдери телекомунікацій; «точки обміну трафіком» (організацій, що надають послуги обміну трафіком); представництва, українські офіси глобальних інтернет-сервісів; власники й розпорядники національних інтернет-сервісів; банки (державні та комерційні; центральні, регіональні відділення та їх філії); платіжні організації, які не є банківськими установами; оператори послуг платіжної інфраструктури; об'єкти критичної інфраструктури (включені до переліку підприємств, що мають стратегічне значення для економіки й безпеки держави, та об'єкти потенційно небезпечних технологій і виробництв); інтернет-ресурси (електронні дошки оголошень, вебсайти, соціальні мережі, форуми тощо).

Оперативна робота в організаційних структурах власників (або розпорядників) системи, володільців інформації дає змогу завчасно отримати інформацію: 1) про користувачів системи, місце та обладнання для здійснення доступу до інформації; 2) про злочини, які готують або вчинені; 3) про злочинні зв'язки особи-користувача; 4) про латентні злочини й осіб, що їх вчинили; 5) про створення та діяльність злочинних груп.

Технічний персонал власників електронно-інформаційних систем володіє такою інформацією, що становить оперативний інтерес: *по-перше*, про

розподілення меж і функцій між структурними підрозділами (відділами, дільницями, службами) з обслуговування обладнання, точок доступу, окремих будівель, споруд і комунікацій; *по-друге*, про конкретних суб'єктів, які здійснювали загальне оперативно-технологічне керування об'єктом, штатне й нештатне обслуговування певного об'єкта; *по-третє*, про осіб, що зайняті на конкретному об'єкті, їх характеристики, поєднання не сумісних, з позицій забезпечення інформаційної безпеки, посад, причини звільнення окремих осіб; *по-четверте*, про кіберінциденти.

5. Виокремлено дві моделі реалізації оперативної інформації про злочини економічної спрямованості, які вчиняють з використанням кіберпростору: 1) виявлення та документування такої кримінально протиправної діяльності працівником оперативного підрозділу з подальшим поданням рапорту з відповідними матеріалами керівнику слідчого підрозділу; 2) документування такої кримінально протиправної діяльності в межах оперативної розробки із залученням слідчого для надання методичної допомоги.

Чинниками, які ускладнюють оперативний пошук ознак злочинів економічної спрямованості, вчинених із використанням кіберпростору, є: 1) упровадження в суспільне життя комп'ютерних технологій, унаслідок чого до сфери кримінально протиправної діяльності залучаються об'єкти нетрадиційної природи; 2) кримінально протиправна діяльність у сфері комп'ютерних технологій виявляється в нових, не звичних для правоохоронної практики формах, способах тощо (вчинення кримінальних правопорушень з використанням інформаційних ресурсів, які територіально розміщені в різних країнах, що ускладнює проведення оперативно-розшукових заходів); 3) неможливе виявлення та фіксування слідів кримінально протиправної діяльності без використання спеціальних знань і відповідних програмно-технічних засобів; 4) працівник оперативного підрозділу не завжди володіє спеціальними знаннями щодо того, як ознаки шахрайських дій у сфері комп'ютерних технологій можуть відображатися в

електронному середовищі; 5) у частині випадків оперативний пошук здійснюють за принципом «від факту злочину до особи», а в інших випадках – за схемою, яка притаманна виявленню економічних злочинів «від конкретної особи до вчиненого злочину».

Аналіз інформації під час виявлення та документування кримінально протиправної діяльності інтернет-магазинів здійснюють за такими напрямами: аналіз суб'єкта господарської діяльності (інтернет-магазину); аналіз контрагентів (ключових партнерів у бізнесі); аналіз особливостей руху товарно-матеріальних цінностей.

Типовими схемами використання електронних грошей з протиправною метою є: а) незаконний обмін, конвертація валюти та виведення валюти за кордон; б) використання електронних грошей для розрахунку з інтернет-магазинами та компаніями, які надають послуги за допомогою мережі Інтернет.

6. За результатами дослідження сформовано тактичні операції на початковому етапі розслідування злочинів економічної спрямованості, вчинених з використанням кіберпростору. Основними завданнями, які виконують під час реалізації тактичної операції *«Аналітичне опрацювання та оцінка матеріалів»,* є: *по-перше,* визначення сутності кримінально релевантної події, яку схарактеризовано в матеріалах оперативного підрозділу; *по-друге,* встановлення якості попереднього документування кримінально протиправної діяльності; *по-третє,* виокремлення обставин кримінально протиправної діяльності, які потребують першочергової фіксації за допомогою проведення СРД і НСРД.

Аналітична робота слідчого під час реалізації тактичної операції *«Встановлення особи злочинця»* виконує такі завдання: *по-перше,* формування типового портрета (моделі) особи (групи осіб), які могли вчинити таке кримінальне правопорушення; *по-друге,* звуження кола осіб, серед яких необхідно здійснювати пошукові заходи та СРД; *по-третє,* прогнозування можливих моделей протидії досудовому розслідуванню, зокрема: а)

приховування невстановлених епізодів кримінально протиправної діяльності; б) знищення елементів слідової картини встановлених фактів кримінально протиправної діяльності.

Особливості СРД у межах проведення тактичної операції *«Фіксація цифрових слідів та формування цифрових доказів»* полягають у: 1) обов'язковому залученні до проведення будь-якої слідчої дії експерта, спеціаліста у сфері інформаційних технологій; 2) виборі й підготовці оптимальних апаратних засобів і програмного забезпечення, яке може бути використано для коректної фіксації відповідної доказової інформації; 3) підготовці належних носіїв для копіювання та фіксації цифрової інформації у випадках, якщо апаратні засоби та програмне забезпечення не можуть бути вилучені для подальшого дослідження та приєднані до матеріалів кримінального провадження; 4) плануванні заходів технічного характеру, спрямованих на нейтралізацію можливості знищення суб'єктом цифрової інформації під час безпосереднього проведення слідчої дії; 5) у випадку, коли слідча дія передбачає обов'язкове залучення понятих, – вжитті заходів щодо залучення понятих, які володіють достатнім рівнем знань у сфері інформаційних технологій, розуміють сутність дій працівників правоохоронних органів під час її проведення, а також, за необхідності, зможуть дати показання щодо особливостей процесу вилучення слідчим цифрових слідів і коректності останнього.

Тактична операція *«Виявлення та вилучення речових доказів»* спрямована на вилучення: *по-перше*, апаратних засобів, які використовували в злочинній діяльності; *по-друге*, інструктивних матеріалів і літератури щодо роботи з відповідними апаратними засобами та програмним забезпеченням; *по-третє*, платіжних карток й інших платіжних інструментів, які мають відповідну фізичну сутність і можуть бути використані під час здійснення кримінально протиправної діяльності економічної спрямованості з використанням кіберпростору; *по-четверте*, документів, зокрема чорнових записів щодо економічних операцій та руху активів під час кримінально

протиправної діяльності; *по-п'яте*, готівкових коштів у національній та іноземній валюті, які отримані за результатами кримінально протиправної діяльності; *по-шосте*, «традиційних речових доказів», які: а) підтверджують перебування особи в конкретному місці та роботу за відповідними апаратними засобами; б) забезпечують встановлення періодизації перебування особи в конкретному місці; в) деталізують роль особи в механізмі кримінально протиправної діяльності.

7. Типовими об'єктами огляду під час розслідування злочинів цієї категорії є: а) приміщення, де сконцентровано основну систему засобів кримінально протиправної діяльності; б) апаратні засоби; в) вебсайти; г) програмні засоби в реальному часі їх функціонування; д) документи; е) інші речові докази, які мають значення для встановлення обставин, що підлягають доказуванню під час розслідування цієї категорії кримінальних проваджень.

Підготовка до проведення огляду в провадженнях цієї категорії передбачає: а) потенційну оцінку виду та класу апаратних засобів, які буде оглянуто на місці події, що ґрунтується на наявній у слідчого інформації щодо сутності кримінально релевантної події; б) визначення кількості та фахової спрямованості спеціалістів, яких необхідно залучити до проведення огляду; в) визначення переліку засобів для вилучення виявлених на місці події апаратних засобів; г) формування групи забезпечення, яку спрямовують на недопущення умисного припинення електропостачання в приміщення та вимкнення апаратних засобів; д) добір понятих, які обізнані щодо особливостей роботи апаратних засобів і програмного забезпечення та можуть бути допитані щодо сутності проведеної СРД.

Типовими тактичними моделями продовження огляду є: фіксація роботи апаратних засобів і програмного забезпечення в режимі реального часу; негайне відключення апаратних засобів від мережі енергопостачання та їх вилучення.

Залучений спеціаліст до огляду апаратних засобів безпосередньо на місці події виконує допоміжні завдання в частині: а) конкретизації переліку

апаратних засобів, які потребують огляду та вилучення, оскільки відсутність у слідчого спеціальних знань може призвести до того, що він не ідентифікує окреме обладнання як апаратний засіб, який має відношення до кримінально протиправної діяльності; б) надання слідчому допомоги в здійсненні коректного відключення апаратних засобів від мережі енергопостачання; в) надання слідчому допомоги щодо коректного роз'єднання та локалізації апаратних засобів, які фізично пов'язані між собою; г) консультування та надання безпосередньої допомоги щодо коректного упакування та опечатування вилучених апаратних засобів і рекомендацій щодо їх безпечного транспортування.

На підготовчому етапі з метою конкретизації предмета допиту аналізують: а) роль конкретної особи в злочинній діяльності; б) на підставі раніше побудованої працівниками оперативного підрозділу чи безпосередньо слідчим матриці зв'язків визначити ступінь інтенсивності зв'язків цієї особи з іншими учасниками кримінально протиправної діяльності; в) тривалість участі особи в злочинній діяльності.

Предмет допиту виконавця злочину, який входить до складу злочинного угруповання, охоплює такі блоки: *по-перше,* дані, які характеризують механізм залучення особи до кримінально протиправної діяльності; *по-друге,* дані, які характеризують безпосередню кримінально протиправну діяльність виконавця; *по-третє,* дані, які характеризують структуру й чисельність злочинного угруповання, що вчиняє злочини економічної спрямованості з використанням кіберпростору; *по-четверте,* дані щодо розподілу доходів, отриманих за результатами кримінально протиправної діяльності.

Обов'язковими елементами предмета допиту організатора кримінально протиправної діяльності є: 1) мотиви та передумови створення злочинного угруповання для здійснення такої кримінально протиправної діяльності; 2) модель структурної побудови угруповання (розподіл ролей) і модель безпосереднього здійснення кримінально протиправної діяльності; 3) біографічні дані організатора й активних учасників, зокрема щодо їх

попередньої трудової діяльності з метою виявлення інших осіб, які можуть бути причетними до вчинення злочинів і не відомі працівникам правоохоронних органів; 4) особливості забезпечення злочинного угруповання загалом й окремих виконавців необхідними апаратними засобами та програмним забезпеченням для вчинення злочинів; 5) дані щодо інфраструктурних елементів такої кримінально протиправної діяльності, зокрема й системи зв'язків, які використовують для її забезпечення; 6) форми та фінансові інструменти, які використовували для легалізації доходів, отриманих злочинним шляхом; 7) модель добору нових учасників угруповання.

Типовими ситуаціями, які зумовлюють організаційно-тактичні особливості проведення обшуку, є: проведення обшуку на початковому етапі розслідування одразу після початку кримінального провадження; проведення обшуку на подальшому етапі розслідування, коли підставами для його проведення є фактичні дані, отримані за результатами проведення першочергових СРД.

У *першій ситуації*, на нашу думку, організаційно-тактичні особливості обшуку полягають у тому, що: а) інформаційною основою для проведення обшуку є матеріали оперативного підрозділу, які стали підставою для початку кримінального провадження; б) проведення такої СРД є наслідком необхідності реагування на отриману інформацію з метою недопущення втрати фактичних даних, які можуть бути доказами в кримінальному провадженні, а також речових доказів і документів; в) проведення одночасних обшуків у різних місцях, що передбачає необхідність залучення значної кількості ресурсів і виокремлення пріоритетного місця обшуку, що організовуватиме безпосередньо слідчий, який здійснює досудове розслідування; г) поєднання таких обшуків з іншими процесуальними діями, наприклад, затриманням осіб за підозрою в причетності до кримінально протиправної діяльності.

8. Визначено організаційно-тактичні особливості проведення НСРД. Функціональною спрямованістю спостереження за особою, місцем або річчю під час розслідування кримінально протиправної діяльності економічної спрямованості, яку вчиняють із використанням кіберпростору, є: *по-перше*, отримання системи установчих даних щодо особи з метою аналітичного опрацювання даних щодо її особистості, складання різного типу профілів і планування досудового розслідування; *по-друге*, встановлення системи зв'язків особи; *по-третє*, встановлення місця розташування основної маси апаратних засобів і програмного забезпечення, використовуваного в злочинній діяльності; *по-четверте*, вивчення приміщень, де концентруються основні апаратні засоби, які використовують у злочинній діяльності.

Встановлення місця знаходження радіоелектронного засобу під час розслідування такої кримінально протиправної діяльності виконує такі завдання: встановлення всіх учасників кримінально протиправної діяльності; визначення місця реалізації відповідної злочинної технології; забезпечення реалізації окремих тактичних прийомів під час проведення інших слідчих дій, зокрема демонстрації допитуваному аналітичних продуктів, сформованих за результатами аналізу даних для спростування його показань, виявлення фактів неправдивої дачі показань тощо.

Дані, що отримано за результатами зняття інформації з електронних інформаційних систем без відома її власника, володільця чи утримувача, класифіковано на такі види: 1) фактичні дані щодо організаційно-структурної побудови злочинного угруповання, яке здійснює таку злочинну діяльність, оскільки аналітичне опрацювання даних дає змогу: а) виокремити осіб, які систематично вчиняють однотипні дії, що відображають елементи конкретної технології кримінально протиправної діяльності; б) визначити осіб, які забезпечують етапи посткримінальної діяльності конкретних суб'єктів, наприклад, легалізацію (відмивання) доходів, отриманих за результатами кримінально протиправної діяльності та/або зміну форми таких активів, зокрема їх переведення в інноваційні платіжні засоби, які недостатньо

контролюють державні фінансові інституції; в) виокремлення осіб, які виконують координаційні й управлінські функції в структурі конкретної кримінально протиправної діяльності; 2) інформація щодо осіб, які ситуативно причетні до вчинення таких злочинів, а також потенційних жертв кримінально протиправної діяльності; 3) дані щодо технології кримінально протиправної діяльності, зокрема системи способів і засобів, які використовують для вчинення таких кримінальних правопорушень; 4) дані щодо фінансових інструментів, які використовують злочинці, зокрема в частині визначення платіжних засобів і засобів, які забезпечують зберігання коштів, отриманих за результатами кримінально протиправної діяльності; 5) інша інформація, яку може бути використано як доказ у кримінальному провадженні.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Авдєєва Г. К., Стороженко С. В. Електронні сліди: поняття та види. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. №1. С.168-175.

2. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження) : монографія. К.: Атіка, 2007. 304 с.

3. Албул С. В. Щодо поняття та складових оперативного пошуку. *Організаційно-правові засади боротьби з правопорушеннями на транспорті* : матеріали Міжнар. наук.-практ. конф., м. Одеса, 15 грудня 2010 р. Одеса, 2010. С. 4-5.

4. Анапольська А. І. Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : автореф. дис… канд. юрид. наук : 12.00.09. Луганськ, 2010. 20 с.

5. Антонов К. В. Державно-правове забезпечення економічної безпеки України від злочинних посягань (за матеріалами ДСБЕЗ ОВС) : монографія. Луганськ : РВВ ЛАВС, 2004. 407 с.

6. Арешонков В. В. Теоретичні, правові та праксеологічні засади техніко-криміналістичних досліджень у розслідуванні злочинів : автореф. дис. … докт. юрид. наук : 12.00.09. Київ, 2021. 40 с. http://elar.naiau.kiev.ua/bitstream/123456789/18534/1/avtoref_areshonkov.pdf

7. Арешонков В. В. Теоретичні, правові та праксеологічні засади техніко-криміналістичних досліджень у розслідуванні злочинів : дис. … докт. юрид. наук : 12.00.09. Київ, 2021. 559 с. http://elar.naiau.kiev.ua/jspui/bitstream/123456789/18807/4/dysertatsia_areshonkov_compressed.pdf

8. Аркуша Л. І. Легалізація (відмивання) доходів, одержаних у результаті організованої кримінально протиправної діяльності: характеристика, виявлення, розслідування. Одеса : Юридична література. 2010. 376 с.

9. Ахтирська Н. М. Актуальні проблеми розслідування кіберзлочинів : навчальний посібник. Київ, 2018. 229 с.

10. Ахтирська Н. М. До питання доказової сили кіберінформації в аспекті міжнародного співробітництва під час кримінального провадження. *Науковий вісник Ужгородського національного університету.* 2016. Вип. 36. С.123-125.

11. Балобанова Д. О. Теорія криміналізації : дис. … канд. юрид. наук : 12.00.08. Одеса, 2007. 200 с.

12. Бандурка О. М., Перепелиця М. М., Манджай О. В. Оперативно-розшукова компаративістика : монографія. Харків : ХНУВС, 2013. 352 с.

13. Басиста І. В. Щодо правомірності проведення обшуку та/або огляду житла чи іншого володіння особи за дорученням слідчого, дізнавача, прокурора. *Соціально-правові студії*. 2021. Випуск 3. С. 115-122.

14. Бахін В. П., Гора І. В., Цимбал П. В. Криміналістика : курс лекцій (ч. 1). Ірпінь : Академія ДПС України, 2002. 356 с.

15. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2008. 20 с.

16. Біляєв В. О. Організаційно-тактичні основи оперативного пошуку у місцях із складною оперативною обстановкою : автореф. дис. … канд. юрид. наук : 12.00.09. Х., 2005. 236 с.

17. Біляєв В. О. Організаційно-тактичні форми оперативно-розшукової протидії злочинності. *Південноукраїнський правничий часопис*. 2012. №3. С.184-186.

18. Бірюков В. В. Використання компютерних технологій для фіксації криміналістично значимої інформації у процесі розслідування : автореф. дис. … канд. юрид. наук : 12.00.09. К. 2001. 20 с.

19. Благута Р. І. Негласні слідчі (розшукові) дії: проблеми підготовки та проведення. *Юридичний часопис Національної академії внутрішніх справ*. 2013. №1. С. 147-152.

20. Богінський О. В. Кримінальна розвідка у кіберсфері : автореф. дис. … канд. юрид. наук : 12.00.09. Харьков, 2018. 20 с.

21. Бойко А. Організована економічна злочинність у період переходу України до ринкової економіки. *Вісник Львівського університету. Серія юридична*. 2008. Вип.46. С.169-177.

22. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : автореф. дис. … канд. юрид. наук : 12.00.09. К., 2007. 20 с.

23. Бортун М. І. Повноваження прокурора під час проведення негласних слідчих (розшукових) дій. *Юридична наука*. 2019. № 9. С.36-41.

24. Бугера О.І. Кримінологічні засади використання мережі інтернет для запобігання злочинності : дис. … докт. юрид. наук : 12.00.09. Київ, 2020. 474 с.

25. Бутузов В. М., Гавловський В. Д., Тітуніна К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посіб. Київ, 2009.182 с.

26. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк, В. Г. Хахановський та ін.; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

27. Вирок Луцького міськрайонного суду Волинської області від 21 березня 2018 р. по справі № 161/1345/18. *Єдиний державний реєстр судових рішень*. URL: http://www.reyestr.court.gov.ua/Review/72886703.

28. Вирок Луцького міськрайонного суду Волинської області від 21 жовтня 2013 р. Справа № 161/10410/13-к. *Єдиний державний реєстр судових рішень*. URL: http://www.reyestr.court.gov.ua/ Review/34405754.

29. Виявлення та розслідування злочинів, пов'язаних з використанням засобів доступу до банківських рахунків : метод. рек. Київ : Нац. акад. внутр. справ, 2013. 79 с.

30. Вознюк А. А., Дуда А. В., Арешонков В. В. Затримання уповноваженою службовою особою в житлі чи іншому володінні особи: актуальні проблеми теорії та практики. *Науковий вісник Національної академії внутрішніх справ.* 2021. № 4 (121). С. 7-16. http://elar.naiau.kiev.ua/bitstream/123456789/21619/1/Науковий%20вісник%20№4%202021_p07-16.pdf

31. Волошина М. О. Науковий генезис проблематики оперативного пошуку первинної оперативно-розшукової інформації підрозділами кримінальної поліції. *Юридичний бюлетень*. Випуск 11. Ч.2 2019. С. 241-247.

32. Волошина М. О. Оперативний пошук первинної оперативно-розшукової інформації підрозділами кримінальної поліції: зміст поняття. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2019. Вип.1. С.235-243.

33. Гахов С. О. Кіберпростір як основна категорія кібернетики. *Сучасний захист інформації.* 2017. №1. С.53-57.

34. Гладій А. Л. Філософія впливу кіберпростору на психологічні властивості сучасних суспільств. *Філософія і політологія у контексті сучасної культури.* 2014. Випуск 7. С.49-54.

35. Главюк І. В. Проблемні питання забезпечення належної правової процедури обшуку (у розрізі новел КПК України). *Вісник Південного регіонального центру Національної академії правових наук України.* 2018. №14. С.141-149.

36. Говоруха В. І., Степанов В. А. Зняття інформації з електронних інформаційних систем як різновид негласної слідчої (розшукової) дії. *Інформація і право.* 2020. №3. С.69-74.

37. Голубєв В. О. Інформаційна безпека : проблеми боротьби з кіберзлочинами : монографія. Запоріжжя : ГУ “ЗІДМУ”, 2003. 237 с.

38. Гонгало С. Й. Судова техніко-криміналістична експертиза документів: сучасні можливості дослідження та перспективи розвитку : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2013. 20 с.

39. Горбаньов І. М. Особливості методики розслідування порушень авторського права щодо незаконного відтворення та розповсюдження комп'ютерних програм : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ. 2007. 20 с.

40. Грига М. А. Деякі процедурні та тактичні недоліки під час проведення обшуку. *Порівняльно-аналітичне право*. 2020. №2. С.195-197.

41. Гриненко І., Прокофьєв М. Структура кримінальних відносин у кіберпросторі. *Правове, нормативне та методологічне забезпечення системи захисту інформації в Україні*. 2013. Вип. №1. С.27-33.

42. Грібов М. Л. Розвідувальні заходи органів внутрішніх справ : сутність та питання застосування у боротьбі з організованою злочинністю. *Боротьба з організованою злочинністю та корупцією: теорія і практика.* 2009. № 20. С. 26-33.

43. Гуцалюк М. Протидія злочинам у сфері обігу пластикових карток. URL: http://www.crime-research.ru/library/.1.

44. Гуцалюк М. В. Сучасні тенденції організованої кіберзлочинності. *Інформація і право*. 2019. №1. С.118-128.

45. Давидюк В. М., Некрасов В.А., Горбач Ю.В. Оперативно-розшукова діагностика злочинів у сфері зовнішньоекономічної діяльності : монографія. К. : ДП «Розвиток», 2014. 198 с.

46. Даніл'ян В. О. Інформаційне суспільство та перспективи його розвитку в Україні (соціально-філософський аналіз) : автореф. дис. ... канд. філософ. наук : 09.00.03. Х., 2006. 19 с.

47. Денисюк С. Ф. Злочинна діяльність: поняття, структура та характеристика її елементів. *Право і безпека*. 2011. №1. С.135-140.

48. Димчиков М., Бондаренко О. Кримінологічні аспекти протидії легалізації корупційних доходів у кіберпросторі. *Легальні горизонти*. №14. 2021. С.105-110.

49. Довженко О. Ю. До питання про тактику допитів у справах про кіберзлочини. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2019. №37. С.143-145.

50. Документування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-практ. посіб. Київ, 2010. 245 с.

51. Дрьомін В. М. Злочинність як соціальна практика: інституціональна теорія криміналізації суспільства : монографія. Одеса : Юридична література, 2009. 616 с.

52. Дудніков А. Л. Правове та криміналістичне поняття способу вчинення злочину. *Теорія та практика судової експертизи та криміналістики*. 2010. Випуск 10. С.55-61.

53. Жаровська Г. П. Основні моделі транснаціональних злочинних організацій. *Юридичний часопис Національної академії внутрішніх справ*. 2018. №1. С.49-60.

54. Жерж Н. А. Пошуковий портрет злочинця: зарубіжний та вітчизняний досвід. *Науковий вісник Національного університету ДПС України.* 2014. №2. С.172-179.

55. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис… канд. юрид. наук : 12.00.09. Харків, 2008. 191 с.

56. Захаров В. П. Особливості оперативного документування злочинів у сфері економіки: навчально-методичний посібник. Львів : Львівський державний університет внутрішніх справ, 2008. 200 с.

57. Іванків І. І. Соціально-психологічні особливості кіберпростору. *Молодий вчений*. 2015. №6. (21) Ч.3. С. 96-104.

58. Інформаційно-телекомунікаційна інфраструктура забезпечення надання електронних послуг в Україні. *Електронне врядування*. URL: http://egov.at.ua/index/pro_sajt/0-2

59. Іщенко В. В. Адміністративне розслідування у справах про адміністративні правопорушення фізичних осіб у сфері оподаткування. Матеріали VIII-их наук. читань, присвяч. пам'яті акад. В.В. Копєйчикова (м. Київ, 22 лист. 2018 р.). Київ, 2018. С. 79-81. http://elar.naiau.kiev.ua/jspui/bitstream/123456789/13548/1/Матеріали%20VIII-их%20наук.%20читань%2c%20присвяч.%20пам'яті%20акад.%20В.В.%20Копєйчикова%20%28м.%20Київ%2c%2022%20лист.%202018%20р.%29_p079-081.pdf

60. Капітанський А. І. Сутність і поняття оперативного обслуговування. *Науковий вісник НАВСУ*. 2002. №3. ч.2. С.93-105.

61. Капустін О. Умисел у складі злочину. *Підприємництво, господарство і право.* 2019. №12. С.294-299.

62. Карпенко Д. О. Техніко-криміналістичне забезпечення розслідування злочинів, пов'язаних із порушенням правил безпеки дорожнього руху або експлуатації транспорту : автореф. дис. … канд. юрид. наук : 12.00.09. Х., 2017. 23 с.

63. Карпов Н. С. Злочинна діяльність. К. 2004. 11 с.

64. Карпов Н. С., Євдокименко С.В. Злочинна діяльність; під ред. В.П. Бахіна. К. : Нац. акад. внутрішн. справ України, 2001. 60 с.

65. Карпов Н. С. Криміналістичні засади вивчення злочинної діяльності : монографія. К. : Київ. Нац. ун-т внутр. справ, 2007. 522 с.

66. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія. Луганськ : МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка, 2012. 528 с.

67. Кваліфікація та розслідування порушення законів і звичаїв війни : наук.- К32 практ. посіб. / А. А. Вознюк, І. В. Жук, О. В. Таран, С. С. Чернявський та ін.; за заг. ред. М. С. Цуцкірідзе, В. В. Чернєя, А. А. Вознюка. К. : Норма права, 2023. 322 с. http://elar.naiau.kiev.ua/bitstream/123456789/24144/1/КВАЛІФІКАЦІЯ_ТА_РОЗСЛІДУВ_ПОРУШЕННЯ_ПОСІБНИК_28_06_2023_ТИП_скороч.pdf

68. Коваль А. А. Забезпечення прав людини при проведенні НС(Р)Д : монографія. Миколаїв : Видавництво ЧНУ, 2019. 265 с.

69. Козак Н. С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2011. 19 с.

70. Козаченко І. П., Регульський В. Л. Правові, морально-етичні та організаційні основи оперативно-розшукової діяльності. Львів : ЛІВС, 1999. 219 с.

71. Колодіна А. С. Принципи криміналістичної методики у діяльності з розслідування злочинів : монографія. Одеса : Юридична література, 2022. 176 с.

72. Комар О. М. Протидія оперативними підрозділами МВС України шахрайствам, вчинюваним шляхом незаконних операцій з використанням електронно-обчислювальної техніки : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2013. 20 с.

73. Комарова М. В. Обшук особи у кримінальному провадженні: сучасні реалії, європейський досвід. *Юридичний науковий електронний журнал*. 2017. № 4. С.158-159.

74. Конкурс на посаду Інспектор кіберполіції (з функціями спецагента) у ДКП НП України: система відбору кандидатів. *НП України* : вебсайт. URL: https://nabir.np.gov.ua/index.php?r=recruitment/process_recruitment&id=91

75. Конституція України : Закон України від 28.06.1996 р. № 254к/96-ВР. URL: https://zakon.rada.gov.ua/laws/show/254к/96-вр#Text

76. Коршикова Т. В. Розслідування шахрайств, учинених із використанням електронно-обчислювальної техніки : дис. … докт. філософ. : 081. Київ, 2021. 255 с. URL: http://elar.naiau.kiev.ua/bitstream/123456789/18989/2/Дисертація_Романенко%20%28Коршикова%29.pdf

77. Кофанов А. В., Арешонков В. В. Генезис застосування ІТ-технологій у профілактиці та розслідуванні злочинів із використанням вогнепальної зброї. http://elar.naiau.kiev.ua/jspui/bitstream/123456789/18936/1/ГЕНЕЗИС%20ЗАСТОСУВАННЯ%20ІТ-ТЕХНОЛОГІЙ%20У%20ПРОФІЛАКТИЦІ%20ТА%20РОЗСЛІДУВАННІ%20ЗЛОЧИНІВ%20ІЗ%20ВИКОРИСТАННЯМ%20ВОГНЕПАЛЬНОЇ%20ЗБРОЇ.pdf

78. Кравчук О. В. Криміналістична характеристика злочинів, пов'язаних із порушенням авторських і суміжних прав : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2012. 23 с.

79. Криміналістика : підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко, О. О. Алєксєєв та ін. К. : Центр учбової літератури, 2015. 544 с. http://elar.naiau.kiev.ua/bitstream/123456789/1700/1/Підручник%20Криміналістика.pdf

80. Криміналістика : підручник / В. В. Пясковський, Ю. М. Чорноус, А. В. Самодін та ін.; за заг. ред. В. В. Пясковського. 2-ге вид., перероб. і допов. Харків : Право, 2020. 752 с.

81. Кримінальне провадження № 0005349731/294990/14. Архів Дніпровського районного суду м. Києва

82. Кримінальний кодекс України : Закон України від 05.04.2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14#Text

83. Кримінальний процесуальний кодекс України : Закон України від 13.04.2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17#Text

84. Кримський Т. С. Способи вчинення злочинів, пов'язаних із несанкціонованим доступом до комп'ютерних мереж та мереж електрозв'язку. *Юридична наука*. 2020. № 7. С.331-338.

85. Крицька І. О. Речові докази та цифрова інформація: поняття та співвідношення. *Часопис Київського університету права*. 2016. №1. С.301-304.

86. Куліуш В. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) дій під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Правові новели*. 2021. №15. С. 217-224. URL: http://legalnovels.in.ua/journal/15_2021/29.pdf

87. Куліуш В. М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178-183. URL: http://www.sulj.oduvs.od.ua/archive/2022/3/29.pdf

88. Куліуш В. М. Обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали Міжнародної науково-практичної конференції. м. Дніпро, 14-15 січня 2022 р. Дніпро : 2022. С. 92-94.

89. Куліуш В. М. Окремі аспекти оперативного (ініціативного) пошуку ознак злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Актуальні питання кримінального провадження у сучасних умовах* : матеріали міжнародної науково-практичної конференції, (м. Одеса, 31 травня 2023 р.) Одеса : ОДУВС, 2023. С. 137-139. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/391cb1b2-076a-4807-8a7f-e1475032c703/content

90. Куліуш В. М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнародної науково-практичної конференції, (м. Львів, 18-19 лютого 2022 р.) Львів, 2022. С. 14-17.

91. Куліуш В. М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. №2. С. 190-193. URL: http://www.lsej.org.ua/2_2022/42.pdf

92. Куліуш В. М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. №1. С. 80-84. URL: http://www.sulj.oduvs.od.ua/archive/2023/1/14.pdf

93. Курилін І. В. Тактика допиту при розслідуванні кіберзлочинів. *Міжнародний науковий журнал «Інтернаука». Серія: «Юридичні науки»*. 2020. №9. С.49-54.

94. Левін В. І. Онтологічна характеристика обшуку як слідчої (розшукової) дії. *Вісник ЛДУВС ім. Е.О. Дідоренка*. 2017. № 4. С.88-96.

95. Літвінов М. Ю. Розкриття оперативними підрозділами ДСБЕЗ МВС України злочинів у сфері використання комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2010. 305 с.

96. Лобойко Л. М. Підстави і момент початку досудового розслідування. *Питання боротьби зі злочинністю*. 2014. Випуск 27. С.132-141.

97. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : монографія. К. : Нац. акад. внутр. справ України, 2005. 360 с.

98. Лук'янчиков Є. Д. Деякі проблеми досудового провадження. *Правничий часопис Донецького університету.* 2000. № 1 (4). С. 68-70.

99. Лук'янчиков Є. Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти) : дис. … докт. юрид. наук : 12.00.09. Київ, 2005. http://www.disslib.org/informatsiyne-zabezpechennja-rozsliduvannja-zlochyniv-pravovi-i-taktyko.html

100. Лук’янчиков Є. Д. Удосконалення засобів інформаційного забезпечення розслідування. *Науковий вісник НАВС України*. 1998. № 3. С. 114-119.

101. Лук’янчиков Є. Д., Лук’янчиков Б. Є. Формування інституту негласних слідчих (розшукових) дій. *Вісник Луганського державного університету внутрішніх справ ім. Е. О. Дідоренка.* 2019. Вип. 1. С.147-155.

102. Луцик В. В. Зняття інформації з електронних інформаційних систем. *Правовые реформы в постсоветских странах: достижения и проблемы* : международная научно-практическая конференция, г. Кишинев, 28-29 марта 2014 г. Кишинев, 2014. С. 316-318. URL: https://dspace.univd.edu.ua/server/api/core/bitstreams/2f45c4a8-67a5-4b87-b904-b6d65e746000/content#page=316

103. Манжай О. В., Богінський О. В. Особливості здійснення кримінальної розвідки у кіберсфері щодо злочинів, пов’язаних з розповсюдженням дитячої порнографії. *Вісник ХНУВС*. 2017. Спец випуск №1(76). С.248-253.

104. Манжай О., Жицький Є. Кримінальна розвідка та її співідношенння з оперативним обслуговуванням. *National law journal : theory and practice*. 2015. №3(30). С.100-105.

105. Марков В. В. Про механізми скоєння злочинів у кіберпросторі та особливості їх кваліфікації. *Південноукраїнський правничий часопис*. 2013. №1. С.112-115.

106. Метелев О. П. Гносеологічна і правова природа цифрових доказів у кримінальному процесі. *Правова позиція.* 2018. №1. С.75-86.

107. Михайлова А. Відеозапис як спосіб фіксації під час обшуку. *Молодий вчений*. 2021. № 4. С.265-268.

108. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 222 с.

109. Мовчан А. В. Інформаційно-аналітична робота в оперативно-розшуковій діяльності міліції : монографія. К. : ДНДІ МВС України; Дніпропетровськ : Дніпроп. держ. Ун-т внутр. справ, 2013. 352 с.

110. Мотлях О. І. Питання методики розслідування злочинів у сфері комп'ютерних технологій : автореф. дис… канд. юрид. наук : 12.00.09. К., 2005. 21 с.

111. Нейдьон Я. Поняття та класифікація віртуальних слідів кіберзлочинів. *Підприємництво, господарство і право*. 2019. №5. С.304-307.

112. Некрасов В. А., Баб'як А. В. Оперативне обслуговування об'єктів бюджетної сфери : проблеми та шляхи їх вирішення. *Радник: український юридичний портал* : вебсайт. URL: http://radnuk.info/statti/229-kruminal-pravo/15031-2011-01-21-04-44-33.html.

113. Некрасов В. А., Мацюк В. Я., Філіпенко Н. Є., Родинюк Л. В. Оперативне розпізнання : монографія. К. : КНТ, 2007. 216 с.

114. Нізовцев Ю. Ю. Судово-експертне дослідження ознак несанкціонованого втручання в роботу інформаційно-телекомунікаційних систем: теоретико-прикладні аспекти : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2018. 20 с.

115. Ніколаюк С. І. Алгоритмізація дій оперативних працівників в процесі оперативного пошуку ознак господарських злочинів шляхом використання можливостей нечіткої логіки. *Південноукраїнський правничий часопис*. 2009. № 1. С. 45-52.

116. Німчик В. П. Розпізнання як елемент оперативного пошуку. URL: http://www.naiau.kiev.ua/tslc/pages/biblio/visnik/2003_1/_zmist01/nimc hik.htm

117. Новікова Л. В. Глобалізація та транснаціональна економічна злочинність: питання сьогодення. *Право і Безпека*. 2010. № 3. С. 26-30.

118. Олашин М. М., Гапяк С. С. Кримінальні процесуальні аспекти зняття інформації з електронних інформаційний систем. *Вісник Львівського торговельно-економічного університету. Юридичні науки.* 2018. Вип. 7. С. 233-242.

119. Оперативно-розшукова діяльність (особлива частина): протидія злочинам загальнокримінального спрямування : навчальний посібник / В. П. Захаров, А. В. Баб'як, Л. Ф. Гула. Львів : ЛьвДУВС, 2013. 476 с.

120. Організаційно-правові та тактичні основи протидії злочинності у сфері інформаційних технологій: навч. посіб. Київ, 2011. 404 с.

121. Ортинський В. Л., Клюс В. В. Особливості оперативного обслуговування підприємницьких структур. *Вісник ЛІВС*. 2003. № 3. С. 3-17.

122. Особливості виявлення та розслідування злочинів у сфері використання комп'ютерних технологій : наук.-практ. посібник. Київ, 2001. 90 с.

123. Пазиніч В.І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : дис. … канд. юрид. наук : 12.00.09. Київ, 209. 217 с.

124. Паламарчук Л. П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж : автореф. дис. … канд. юрид. наук : 12.00.09. К., 2008. 20 с.

125. Панченко О. А., Гнатенко В. С. Економічна кібербезпека в державній системі національної безпеки. С. 22-31. URL: http://journals.maup.com.ua/index.php/public-management/article/view/1085/1596

126. Пашнев Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09. К., 2008. 20 с.

127. Піддубна Л. В. Кіберпростір як соціокультурний фактор мережевого суспільства. *Гілея*. Випуск. 105. С.204-207.

128. Погорецький М., Старенький О. Негласні слідчі (розшукові) дії як засоби отримання доказів: окремі проблемні питання. *Право України*. 2018. №8. С.85-106.

129. Поливода В. В. Оперативне обслуговування за зональним принципом об’єктів та територій підрозділами карного розшуку : дис. … канд. юрид. наук : 21.07.04. Київ, 2007. 205 с.

130. Попко В. В., Попко Є. В. Міжнародно-правова регламентація транснаціональної кіберзлочинності у кіберпросторі. *Науковий вісник Ужгородського національного унверситету. Серія Право.* 2021. Випуск. 66. С. 276-283.

131. Правові й організаційно-процедурні основи здійснення оперативно-пошукової діяльності органів внутрішніх справ в Україні. Загальна частина: навчальний посібник / Б. І. Борисенко, Д. О. Бабічев, О. В. Бочковий та ін.; за ред. А. В. Іщенка, Б. І. Бараненка. Луганськ: РВВ ЛДУВС ім. Е.О. Дідоренка, 2011. 360 с.

132. Приходько Ю. П. Техніко-криміналістичне забезпечення розслідування злочинів, повязаних із кримінальними вибухами : автореф. дис. … канд. юрид. наук : 12.00.09. К., 2016. 19 с.

133. Про Державну службу спеціального зв’язку та захисту інформації України : Закон України від 23 лютого 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15.

134. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБУ, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листопада 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

135. Про затвердження переліку об’єктів державної власності, що мають стратегічне значення для економіки і безпеки держави : постанова Кабінету Міністрів України від 4 березня 2015 р. № 83. URL: https://zakon.rada.gov.ua/laws/show/83-2015-%D0%BF

136. Про затвердження Положення про Департамент захисту економіки НП України : наказ НП України від 7 листопада 2015 р. № 81. *Офіційний матеріал Департаменту Документального забезпечення НП України*. Відомчий документ.

137. Про затвердження Положення про Департамент карного розшуку НП України : Наказ НП України від 14 лист. 2015 р. № 90. *Офіційний матеріал Департаменту Документального забезпечення НП України*. Відомчий документ;

138. Про затвердження Положення про Департамент кіберполіції НП України : Наказ НП України від 10 листопада 2015 р. № 85. *Офіційний матеріал Департаменту Документального забезпечення НП України.* Відомчий документ. 9 с.

139. Про затвердження Положення про Департамент протидії наркозлочинності НП України : Наказ НП України від 17 листодада 2015 р. №95. *Офіційний матеріал Департаменту Документального забезпечення НП України.* Відомчий документ.

140. Про затвердження Штату Департаменту кіберполіції Національної поліції України : Наказ України від 7 листопада 2015 р. № 10. *Офіційний матеріал Департаменту Документального забезпечення НП України.* Відомчий документ. 12 с.

141. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 липня 1994 р. № 80/94-В. URL: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80?find=1&text=%EA%EE%F0%E8%F1%F2%F3#w11;

142. Про інформацію : Закон України від 2 жовтня 1992 р. № 2657-XII. URL: https://zakon.rada.gov.ua/laws/show/2657-12#Text

143. Про національну безпеку України : Закон України від 21 червня 2018 р. № 2469-VIII. URL: https://zakon.rada.gov.ua/laws/show/2469-19#n355

144. Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації : Указ Президента України від 23 листопада 2011 р. № 1067/2011. URL: https://zakon.rada.gov.ua/laws/show/1067/2011

145. Про Національну поліцію України : Закон України від 2 липня 2015 р. №580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

146. Про організацію діяльності слідчих підрозділів Національної поліції України : наказ МВС України від 06.07.2017 р. № 570 URL: https://zakon.rada.gov.ua/laws/show/z0918-17/paran9#Text

147. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовтня 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text

148. Про платіжні системи та переказ коштів в Україні : Закон України 5 квітня 2001 р. №2346-III. URL: https://zakon.rada.gov.ua/laws/show/2346-14

149. Про розвідувальні органи України : Закон України 22 березня 2001 р. № 2331-14. URL: https://zakon.rada.gov.ua/laws/show/2331-14.

150. Про Службу безпеки України : Закон України від 25 березня 1992 р. №2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

151. Про телекомунікації : Закон України від 18 листопада 2003 р. № 1280-IV. URL: https://zakon.rada.gov.ua/laws/show/1280-15

152. Пушина Н. Л. Способи вчинення незаконних операцій із використанням платіжних карток та інших засобів доступу до банківських ресурсів, електронних грошей, обладнання для їх виготовлення. *Науковий вісник Ужгородського національного університету. Серія. Право.* 2020. Випуск. 61. Том. 2. С.112-115.

153. Реєстр щодо платіжних організацій, систем та операторів послуг платіжної інфраструктури. URL: https://bank.gov.ua/control/uk/publish/article?art_id=8436153

154. Розслідування злочинів, вчинених із використанням шкідливих програмних чи технічних засобів : метод. реком. Київ, 2016. 56 с.

155. Розслідування злочинів, пов’язаних з незаконним розповсюдженням у мережі Інтернет недійсного контенту провайдерами програмних послуг та Інтернет провайдерами : метод. реком. Київ, 2017. 44 с.

156. Розслідування окремих видів злочинів : навч. посіб. для студ. вищ. навч. закл. / О. О.Алєксєєв, В. К. Весельський, В. В. Пясковський. 2-е вид., перероб. і доповн. Київ : Центр навч. літ., 2014. 277 с. https://lawbook.online/metodika-kriminalisticheskaya/rozsliduvannya-okremih-vidiv-zlochiniv-tekst.html

157. Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського. Серія: Юридичні науки».* 2018. Том 29 (68) № 4. С. 165-169.

158. Самойленко О. А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія. Одеса : ТЕС, 2020. 372 с.

159. Самойленко О. А. Особливості розслідувань викрадень майна, вчинених із використанням комп’ютерних технологій : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2011. 19 с.

160. Самойленко О. А. Природа кіберпростору як об’єкта криміналістичного дослідження. *Криміналістика і судова експертиза*. Випуск 63. С.174-184.

161. Самойлов С. В. Розслідування шахрайств із використанням мережі Інтернет : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. 226 с.

162. Сергєєва Д. Б. Проблемні аспекти законодавчого визначення відомостей щодо НС(Р)Д, що не підлягають розголошенню. *Вісник кримінального судочинства*. 2015. №1. С.104-110.

163. Сергєєва Д. Б. Щодо класифікації негласних слідчих (розшукових) дій. *Вісник кримінального судочинства*. 2015. №2. С.69-76.

164. Скрябін О. М. Слідчі дії як основний спосіб збирання доказів у кримінальному провадженні. *Правова позиція*. 2020. №4. С.90-93.

165. Соколов К. О., Гудима О. П. Підхід до розробки елементів структури системи виявлення деструктивного впливу у кіберпросторі. *Наукоємні технології*. 2019. №4 (44). С.426-432.

166. Стащак М. В. Складові елементи оперативного пошуку злочинів. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка.* 2015. № 3. С.307-314.

167. Стащак М. В. Форми оперативно-розшукової діяльності підрозділів кримінальної поліції у протидії злочинності: концептуальні засади : автореф. дис. … докт. юрид. наук : 12.00.09. Х., 2017. 40 с.

168. Стрельцов Л. Є. Поняття та ознаки компютерної програми у міжнародному праві. *Науковий вісник Міжнародного гуманітарного університету*. 2014. Вип. 11. С.168-171.

169. Таран О. В. Криміналістичне забезпечення розслідування кримінально протиправної діяльності у сфері порушення авторських прав : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.

170. Тарасенко О. С. Виявлення інформації в мережі Інтернет : погляд на положеня проєкту закону «Про оперативно-розшукову діяльність». *Наукове забезпечення досудового розслідування: проблеми теорії та практики* : зб. тез доповідей V Всеукр. наук.-практ. конф. м. Київ, 8 липня 2016 р. Київ : Нац. акад. внутр. справ, 2016. С. 162-164.

171. Тарасенко О. С. Теорія та практика протидії кримінальним правопорушенням, пов’язаним з обігом протиправного контенту у мережі Інтернет : монографія. Одеса : Видавничий дім «Гельветика», 2021. 426 с.

172. Телійчук В. Т. Способи вчинення злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку і засади протидії. *Держава та регіони*. *Сер. Право*. 2014. № 2. С.31-37.

173. 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 : автореф. дис. … канд. юрид. наук : 12.00.09. К., 2021. 268 с.

174. Терещенко Ю. В. Слідчі (розшукові) дії як різновид процесуальних дій. *Митна справа*. 2014. № 1(2.1). С. 112-117.

175. Тіщенко В. В. Структура окремих криміналістичних методик. Криміналістика : підручник. Одеса : Видавничий дім «Гельветика», 2017. С.352-361.

176. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

177. Ткач Ю. Концептуальна модель безпеки кіберпростору. *Технічні науки та технології*. 2020. №4 (22). С.96-108.

178. Торбас О. О. Кримінальна процесуальна характеристика майна, яке було вилучено під час обшуку. *Вісник Південного регіонального центру Національної академії правових наук України*. 2016. №7. С.195-200.

179. Удалова Л. Д. Вербальна інформація у кримінальному процесі України : монографія. Київ : Вид. Паливода А. В., 2006. 324 с.

180. Участь спеціаліста у проведенні слідчих (розшукових) дій під час розслідування корупційних злочинів : метод. рек. Б. Б. Теплицький, О. М. Шрамко, В. В. Юсупов. Київ, 2019. 68 с. https://www.naiau.kiev.ua/files/zakon_ukr/metod_rek/metod_04122019.pdf

181. Фінагеєв В. О. Способи вчинення злочинів, пов'язаних з використанням засобів доступу до банківських ресурсів. *Науковий вісник Національної академії внутрішніх справ.* 2016. №1. С.63-82.

182. Фролов О. П. Об'єктивні елементи обшуку у формі спеціальної операції. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія і практика)*. Вип. 3-4. 2018. С.257-263.

183. Фролов О. П. Поняті як суб'єкт обшуку у формі спеціальної операції. *Правова позиція*. 2019. №4. С. 112-115.

184. Фурашев В. М. Кіберпростір та інформаційний простір, кібербезпека та інформаційна безпека: сутність, визначення, відмінності.

Цифрова платформа: інформаційні технології у соціокультурній сфері. 2018. №1. С.75-86.

185. Хоменко І. В. Контроль та нагляд за проведенням негласних слідчих (розшукових) дій в умовах особливого режиму досудового розслідування. *Юридична наука*. 2020. №1. Т.2. С. 113-119.

186. Цехан Д. М. Використання інформаційних технологійв оперативно-розшуковій діяльності органів внутрішніх справ : монографія. Одеса : Юридична література. 2011. 216 с.

187. Цехан Д. М. Оперативно-розшукова протидія злочинності у місцях позбавлення волі : монографія. Одеса : Юридична література. 2021. 296 с.

188. Цехан Д. М. Цифрові докази : поняття, особливості та місце у системі доказування. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2013. №5. С.256-260.

189. Цилюрик І. І. Негласні слідчі (розшукові) дії в кримінальному провадженні. *Науковий вісник Міжнародного гуманітарного університету. Сер.: Юриспруденція.* 2014. №8. С.271-274.

190. Цифрова економіка: тренди, ризики та соціальні детермінанти. Київ : Вид-во «Заповіт», 2020. 274 с.

191. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 624 с.

192. Черняховський Б. В. Особливості процедури слідчого огляду під час розслідування несанкціонованого втручання в роботу комп’ютерів, автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. №2. С.58-68.

193. Чорноус Ю. М. Криміналістичне забезпечення розслідування злочинів : монографія. Вінниця, 2017. 492 с. http://elar.naiau.kiev.ua/handle/123456789/16029

194. Чорноус Ю. М. Слідчі дії: поняття, сутність, напрями розвитку та удосконалення : дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 245 с.

195. Чорноус Ю., Синоверська Т. Криміналістична методика розслідування жорстокого поводження з тваринами : монографія. Київ : «Право», 2022. 248 с. https://pravo-izdat.com.ua/index.php?route=product/product/download&product_id=4547&download_id=1509

196. Шаповалов О. О. Поняття та сутність оперативного пошуку. *Науковий вісник Національної академії внутрішніх справ.* 2017. №2. С.149-159.

197. Швидкова О. В. Обшук як спосіб збирання доказів. *Часопис Національного університету «Острозька академія». Серія «Право».* 2014. №2 (10). С.1-17.

198. Шеломенцев В. П. Кримінологічна безпека у кіберпросторі: система понять. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. №23. С.342-348.

199. Шепітько В. Ю. Проблеми типізації окремих криміналістичних методик. *Наукові праці Національного університету «Одеська юридична академія»* : збірник наукових праць. 2017. Т.19. С.445-451.

200. Шитий С. І., Огороднікова І. І. Особливості порушення прав людини шляхом незаконного використання програмних засобів негласного зняття інформації. *Наукові записки Інституту законодавства Верховної Ради України.* 2017. № 1. С. 82–92.

201. Юсупов В. Історія формування доктрини криміналістики в Україні. Право України. 2021. № 8. С. 44-64. https://pravoua.com.ua/ua/store/pravoukr/pravo_2021_8/pravo_2021_8_s3/

202. Яцишин М. Ю. Міжнародно-правове співробітництво у сфері боротьби з кіберзлочинністю : автореф. дис… канд. юрид. наук : 12.00.11. Київ, 2019. 20 с.

203. Bell D. The Coming of Post-Industrial Society. New York : Basic Books, 1973. 616 p.

204. Brzezinski Z. Between Two Ages : America’s Role in technetronic era. New York : Viking Press, 1970. 252 p.

205. Katz R. L. The Information Society : an International Perspective. N.Y. : Praeger 1988. 188 p.

206. Masuda Y. The Information Society as Post-Industrial Society. Washington, D.C. : World Future Society, 1981. 171 p.

207. Porat M, Rubin M. The Information Economy : development and Measurement. Wash. : DC. Prigogene, I., Stengers, I., 1978. 320 p.

208. Rostow W. The Stage of Economic Growth : non-Communist Manifesto Cambridge : Cambridge University Press, 1960. 198 p.

209. Stonier T. The wealth of Information : A Profile Of The Post-Industrial Economy. L. : Thames and Hudson, 1983. 224 p.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

в яких опубліковано основні наукові результати дисертації:

1. Куліуш В. М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. № 2. С. 190–193. URL: http://www.lsej.org.ua/2_2022/42.pdf.

2. Куліуш В. М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178–183. URL: http://www.sulj.oduvs.od.ua/archive/2022/3/29.pdf.

3. Куліуш В. М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. № 1. С. 80–84. URL: http://www.sulj.oduvs.od.ua/archive/2023/1/14.pdf.

4. Куліуш В. Організаційно-тактичні особливості проведення окремих слідчих (розшукових) дій під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Правові новели*. 2021. № 15. С. 217–224. URL: http://legalnovels.in.ua/journal/15_2021/29.pdf.

які засвідчують апробацію матеріалів дисертації:

5. Куліуш В. М. обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали

Міжнар. наук.-практ. конф. (Дніпро, 14–15 січ. 2022 р.). Дніпро, 2022. С. 92–94.

6. Куліуш В. М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнар. наук.-практ. конф. (Львів, 18–19 лют. 2022 р.). Львів, 2022. С. 14–17.

7. Куліуш В. М. Окремі аспекти оперативного (ініціативного) пошуку ознак злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Актуальні питання кримінального провадження у сучасних умовах* : матеріали Міжнар. наук.-практ. конф. (Одеса, 31 трав. 2023 р.). Одеса, 2023. С. 137–139. URL: https://dspace.oduvs.edu.ua/server/api/core/bitstreams/391cb1b2-076a-4807-8a7f-e1475032c703/content.

Додаток Б

Узагальнення результатів анкетування працівників Департаменту кіберполіції Національної поліції України щодо розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору

	Запитання	Кількість	%
	Працівники Департаменту кіберполіції Національної поліції України	143	100
1.	**Зважаючи на Ваш досвід, у яких формах існують зв'язки між розвитком кіберпростору та окремими формами кримінально протиправної діяльності у сфері економіки?**		
	а) криміналізація окремих діянь зумовлена широкомасштабним впровадженням інформаційних технологій та їх структурної складової – кіберпростору у всі форми суспільного життя	102	71
	б) якісна трансформація інфраструктури економічної злочинності, що зумовлено перетворенням кіберпростору у невід'ємну складову економічних відносин	98	69
	в) трансформація окремих способів вчинення економічних злочинів у складні технології кримінально протиправної діяльності	87	61
	г) якісна зміна особи злочинця та формування допоміжних технократичних сил, які виконують забезпечувальну функцію на окремих стадіях реалізації злочинних технологій	73	51
	д) формування цифрових кримінальних ринків	132	92
2.	**Які функції, на Вашу думку, може виконувати кіберпростір як складова інфраструктури економічної злочинності?**		
	а) інтелектуальне та інформаційне забезпечення кримінально протиправної діяльності	138	97
	б) створення умов для формування стійких безконтактних зв'язків між особами, які в подальшому можуть здійснювати спільну злочинну діяльність	140	98
	в) забезпечення ринку збуту відповідних кримінальних послуг та кримінальних компетенцій	128	90
3.	**На ваш погляд, фактичні дані, які вказують на наявність ознак вчинення або готування кримінального правопорушення з використанням обстановки кіберпростору, здобуті в результаті застосування технічних методів оперативного обслуговування**		

	кіберпростору, є достовірними лише з позицій носія спеціальних знань у сфері комп'ютерних технологій?		
	а) Так	129	90
	б) Ні	15	10
4.	**Які рівні обслуговування кіберпростору, на Ваш погляд, можна виокремити?**		
	а) центральний	132	92
	б) регіональний	111	78
	в) міжрегіональний	85	59
	г) територіальний	99	69
5.	**На які групи можна впорядкувати інформацію, необхідну для аналізу оперативної обстановки злочину, вчиненого в кіберпросторі?**		
	а) детермінанти злочинів у кіберпросторі	45	31
	б) відомості про власників (або розпорядників) систем	72	50
	в) відомості про володільців інформації в системі	139	97
	г) наявні оперативні позиції на об'єкті оперативного обслуговування	142	99
6.	**Які моделі реалізації оперативної інформації про кримінально протиправну діяльність економічної спрямованості, яку вчиняють з використанням кіберпростору, зважаючи на Ваш професійний досвід, можна виокремити?**		
	а) виявлення та документування такої кримінально протиправної діяльності працівником оперативного підрозділу з подальшим поданням рапорту з відповідними матеріалами керівнику слідчого підрозділу	143	100
	б) документування такої кримінально протиправної діяльності у межах оперативної розробки з залученням слідчого для надання методичної допомоги	141	99
7.	**Які, на Ваш погляд, можна виокремити основні ознаки оперативного (ініціативного) пошуку?**		
	а) оперативний пошук передує оперативній профілактиці та оперативній розробці	124	87
	б) об'єктами оперативного пошуку є особи, предмети та події (факти), які є джерелами оперативної інформації	101	71
	в) основним критерієм віднесення особи, події та предмета до об'єктів оперативного пошуку є те, що вони становлять оперативний інтерес для оперативних підрозділів правоохоронних органів, а первинна інформація про них є оперативно значущою для цих підрозділів	99	69

	г) оперативний пошук здійснюється поза зв’язком з конкретною особою або фактом, конкретною справою оперативного обліку, виконанням окремих завдань, виявленням та розслідуванням окремих злочинів вже відомими фактами та особами	142	99
	д) здійснення оперативного пошуку ґрунтується на потенційній можливості розпізнання об’єкта пошуку за попередньо відомими ознаками, що властиві саме цим, ще невідомим об’єктам пошуку, які підлягають встановленню в ході його здійснення	129	90
	е) основними завданнями оперативного пошуку є отримання первинної інформації про осіб, предмети, події (факти), які становлять оперативний інтерес, а також перевірка цієї інформації для встановлення ознак злочину чи спростування інформації про нього	140	98
	ж) зміст оперативного пошуку становить постійна, активна, цілеспрямована пошукова робота, яка є системою розвідувально-пошукових заходів, що здійснюються як особисто суб’єктами пошуку (особистий пошук), так і з залученням до нього відповідних сил і засобів, у тому числі інформаційних систем	94	66
	и) підставою для початку пошуку первинної оперативно значущої інформації слугує законодавчий припис	99	69
	к) для проведення розвідувально-пошукових заходів достатньо лише припущення щодо підготовки чи вчинення злочину за наявністю окремих ознак, що вказують на такі діяння або на осіб, які готують, вчиняють чи вчинили злочин, причому таке припущення може мати характер версії, що ґрунтується на певних фактах	123	86
	л) оперативний пошук здійснюється у місцях найбільш імовірного виявлення об’єктів пошуку	73	51
8.	**Які етапи оперативного пошуку можна, на Ваш погляд, виокремити?**		
	а) постановка завдання та формування (інформаційної) моделі об’єкта пошуку, що містить загальні відомості про риси та властивості об’єктів пошуку (ознаки розпізнання), їх прояви в зовнішньому середовищі (пошукові ознаки)	131	92
	б) здійснення конкретного комплексу пошуково-розвідувальних заходів з метою виявлення	85	59

	конкретного об’єкта, що становить оперативний інтерес		
	в) перевірка та оцінювання отриманої первинної інформації про об’єкт, що становить оперативний інтерес, а також прийняття відповідного рішення за результатами перевірки	143	100
9.	**Які первинні сигнали можуть свідчити про вчинення протиправної діяльності у кіберпросторі?**		
	а) скарги користувачів мережі Інтернет на протиправні дії інших	102	71
	б) стрімке збагачення програмістів-професіоналів, які знаходяться у полі оперативної уваги працівників оперативних підрозділів	55	38
	в) сигнали про пошуки в Інтернет-середовищі незаконних шляхів для розвитку торгової діяльності від е-комерції	59	41
	г) пропозиції щодо вчинення злочинних угод, фінансових афер	23	16
	д) замовлення на розробку спеціального програмного забезпечення, інформацію про реквізити (дані) банківських платіжних систем	103	72
10.	**Чи вдається отримувати необхідну інформацію для подальшого ефективного документування під час реалізації етапів виявлення ознак кримінально протиправної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору?**		
	а) Так	67	47
	б) Ні	76	53
11.	**З якою метою виникає необхідність практичного відпрацювання Інтернет-магазину для отримання додаткової інформації шляхом проведення перевірочної закупівлі?**		
	а) для ознайомлення з фактичним рухом товару від складу до покупця	120	84
	б) для встановлення порядку та форми розрахунку за товар	77	54
	в) для ознайомлення з документами, які надаються продавцем	92	64
	г) при застосуванні приватної кур’єрської служби, а не служби Інтернет-магазину, визначаються підприємці, які здійснюють дану діяльність	84	59
	д) отримання інформації про кур’єра (на яких умовах здійснюється працевлаштування, на яких складах здійснюється отримання товару)	109	76
	е) визначення умов, за яких здійснюється повернення товару, після чого встановлюється коло	102	71

	СГД, які задіяні при поверненні товару (який документ при цьому видається)		
	ж) визначення обігу готівкових коштів	132	92
12.	**Які класифікаційні критерії можна застосувати до системи електронних грошей?**		
	а) за типом носія	99	69
	б) за типом технології зберігання	134	94
	в) за ступенем анонімності	43	30
	г) за розміром платежу	59	41
13.	**Які основні блоки завдань, які вирішуються слідчим під час реалізації тактичної операції «Аналітичне опрацювання та оцінка отриманих матеріалів», на Вашу думку, варто виокремити?**		
	а) визначення сутності кримінально-релевантної події, яка охарактеризована у матеріалах оперативного підрозділу	124	87
	б) встановлення якості попереднього документування кримінально протиправної діяльності.	92	64
	в) виокремлення обставин кримінально протиправної діяльності, які потребують першочергової фіксації за допомогою проведення слідчих (розшукових) та негласних слідчих (розшукових) дій	106	74
14.	**До початку кримінального провадження чи реалізуються оперативними підрозділами оперативно-тактичні комплекси, які спрямовані на встановлення осіб, причетних до кримінально протиправної діяльності економічної спрямованості, яка здійснюється з використанням кіберпростору?**		
	а) Так	104	73
	б) Ні	39	27
15.	**Чи відомі на початковому етапі розслідування правоохоронним органам точні установчі дані осіб, які причетні до такої кримінально протиправної діяльності?**		
	а) Так	5	3
	б) Ні	138	97
16.	**Які типові об'єкти огляду можна, на Ваш погляд, виокремити у кримінальних провадженнях щодо розслідування злочинів економічної спрямованості, які вчиняються з використанням кіберпростору?**		
	а) приміщення, де концентрується основна система засобів кримінально протиправної діяльності	87	61
	б) апаратні засоби	94	66
	в) вебсайти	131	92

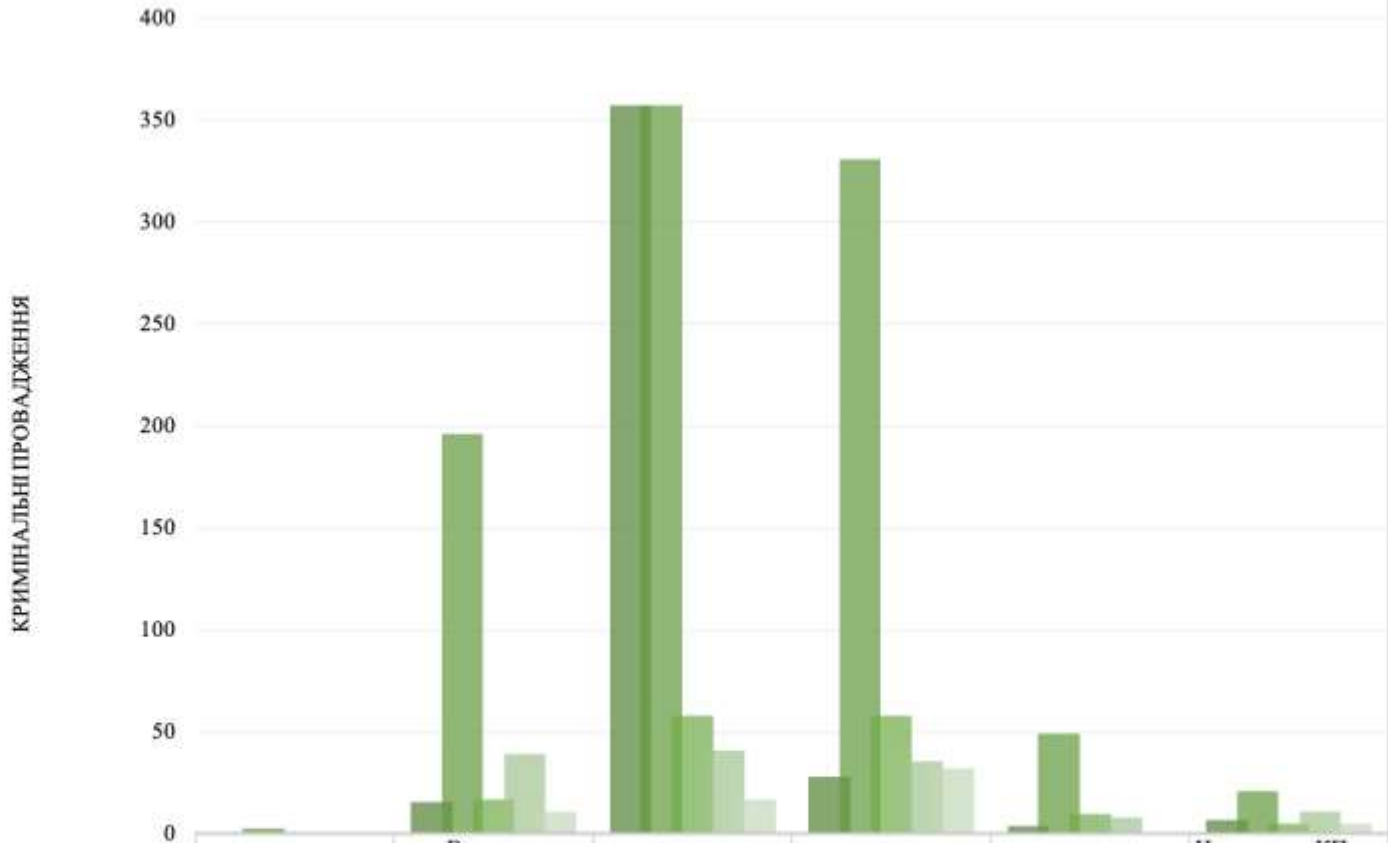
	г) програмні засоби у реальному часі їх функціонування	90	63
	д) документи	84	59
	е) інші речові докази, які мають значення для встановлення обставин, які підлягають доказуванню під час розслідування цієї категорії кримінальних проваджень	33	23
17.	**Які особливості має огляд приміщення під час розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору?**		
	а) формує у слідчого уявлення не лише щодо сутності кримінально-релевантної події, а й щодо рівня організованості та системності кримінально протиправної діяльності, що дозволяє конкретизувати подальшу стратегію розслідування	132	92
	б) під час огляду приміщень виявляються інфраструктурні елементи, які забезпечують злочинну діяльність	109	76
18.	**Які моделі продовження огляду можуть обратися слідчим за результатами реалізації початкового етапу огляду?**		
	а) фіксація роботи апаратних засобів та програмного забезпечення у режимі реального часу	139	97
	б) негайне відключення апаратних засобів від мережі енергопостачання та їх вилучення	140	98
19.	**Яка мета попереднього огляду апаратних засобів на місці події вчинення злочину економічної спрямованості з використанням кіберпростору?**		
	а) фіксація локації їх розташування у приміщенні	140	98
	б) встановлення інструментів фізичного з’єднання апаратних засобів між собою, а також із периферійним обладнанням	90	63
	в) виявлення та фіксація у протоколі ідентифікаційних ознак кожного апаратного засобу, який оглядається та у подальшому буде вилучений працівниками правоохоронних органів	143	100
20.	**Які задачі виконує залучений до огляду апаратних засобів безпосередньо на місці події вчинення злочину економічної спрямованості з використанням кіберпростору спеціаліст?**		
	а) конкретизація переліку апаратних засобів, які потребують огляду та вилучення, оскільки відсутність у слідчого спеціальних знань може призвести до того, що він не ідентифікує окреме обладнання як апаратний засіб, який має	123	86

	відношення до кримінально протиправної діяльності		
	б) надання слідчому допомоги у здійсненні коректного відключення апаратних засобів від мережі енергопостачання	99	69
	в) надання слідчому допомоги щодо коректного роз'єднання та локалізації апаратних засобів, які фізично пов'язані між собою	109	76
	г) консультування та надання безпосередньої допомоги щодо коректного упакування та опечатування вилучених апаратних засобів та рекомендацій щодо їх безпечного транспортування	132	92
21.	**Що необхідно проаналізувати слідчому підготовчому етапі з метою конкретизації предмета допиту у випадку вчинення злочину економічної спрямованості з використанням кіберпростору?**		
	а) роль конкретної особи у злочинній діяльності	101	71
	б) на підставі раніше побудованої працівниками оперативного підрозділу чи безпосередньо слідчим матриці зв'язків, визначити ступінь інтенсивності зв'язків цієї особи з іншими учасниками кримінально протиправної діяльності	98	69
	в) тривалість участі особи у злочинній діяльності	132	92
22.	**Які структурні блоки предмета допиту особи виконавця, що входить до складу злочинного угруповання, яке вчиняє злочини економічної спрямованості з використанням кіберпростору, зважаючи на Ваш досвід, можна виокремити?**		
	а) дані, які характеризують механізм залучення особи до кримінально протиправної діяльності	95	66
	б) дані, які характеризують безпосередню кримінально протиправну діяльність виконавця	138	97
	в) дані, які характеризують структуру та чисельність злочинного угруповання, яке вчиняє злочини економічної спрямованості з використанням кіберпростору	89	62
	г) дані щодо розподілу доходів, отриманих за результатами кримінально протиправної діяльності	141	99
23.	**На які блоки можна структурувати предмет допиту організатора та осіб, які входять до керівної ланки злочинного угруповання?**		
	а) мотиви та передумови створення злочинного угруповання для здійснення такої кримінально протиправної діяльності	124	87
	б) модель структурної побудови угруповання (розподіл ролей) та модель безпосереднього здійснення кримінально протиправної діяльності	94	66

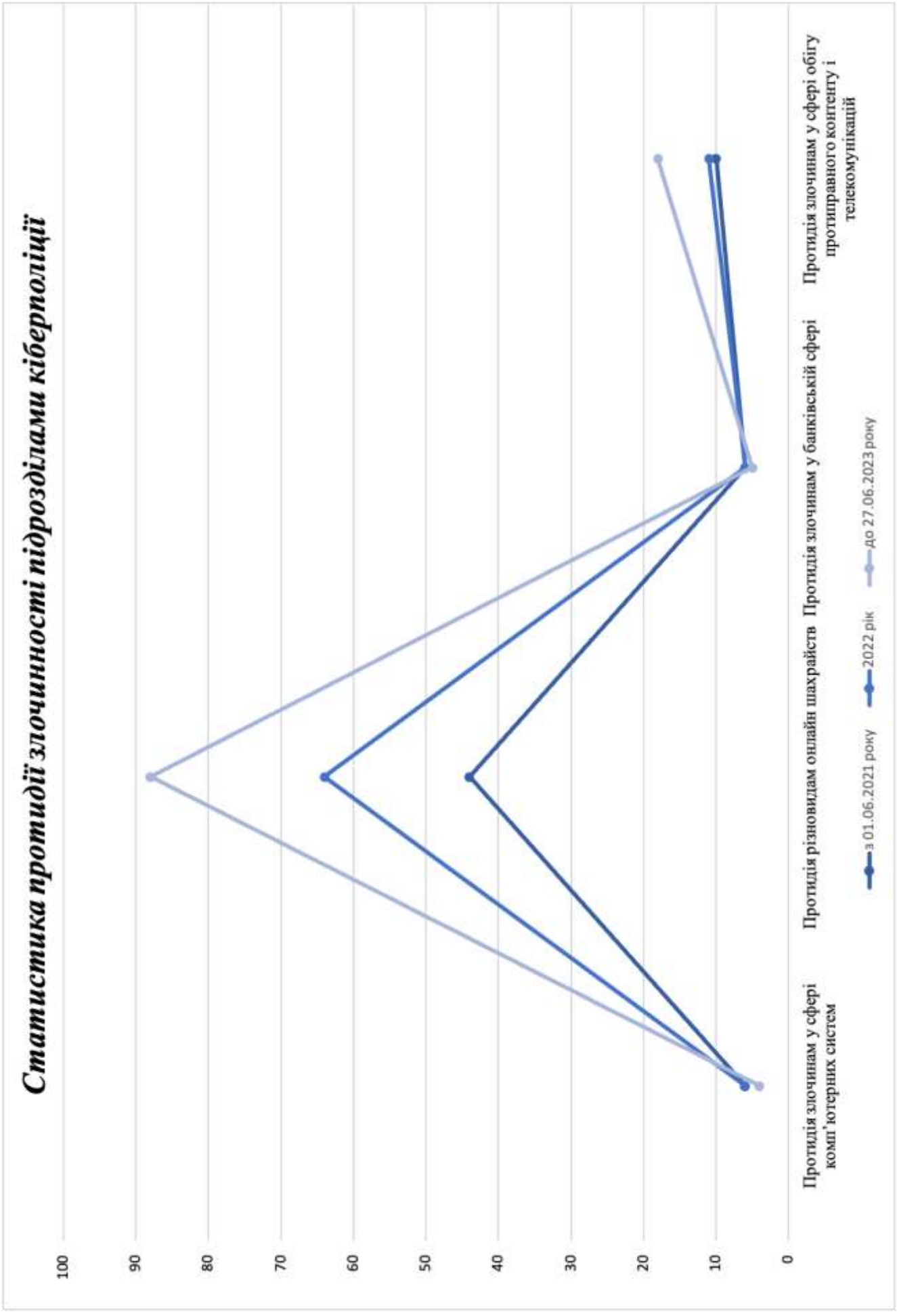
	в) біографічні дані організатора та активних учасників, зокрема щодо їх попередньої трудової діяльності з метою виявлення інших осіб, які можуть бути причетними до вчинення злочинів та невідомі працівникам правоохоронних органів	128	90
	г) особливості забезпечення злочинного угруповання загалом та окремих виконавців необхідними апаратними засобами та програмним забезпеченням для вчинення злочинів	141	99
	д) дані щодо інфраструктурних елементів такої кримінально протиправної діяльності, зокрема й системи зв’язків, які використовуються для її забезпечення тощо	86	60
	е) форми та фінансові інструменти, які використовувались для легалізації доходів, отриманих злочинним шляхом	123	86
	ж) модель підбору нових учасників угруповання	101	71

Додаток В

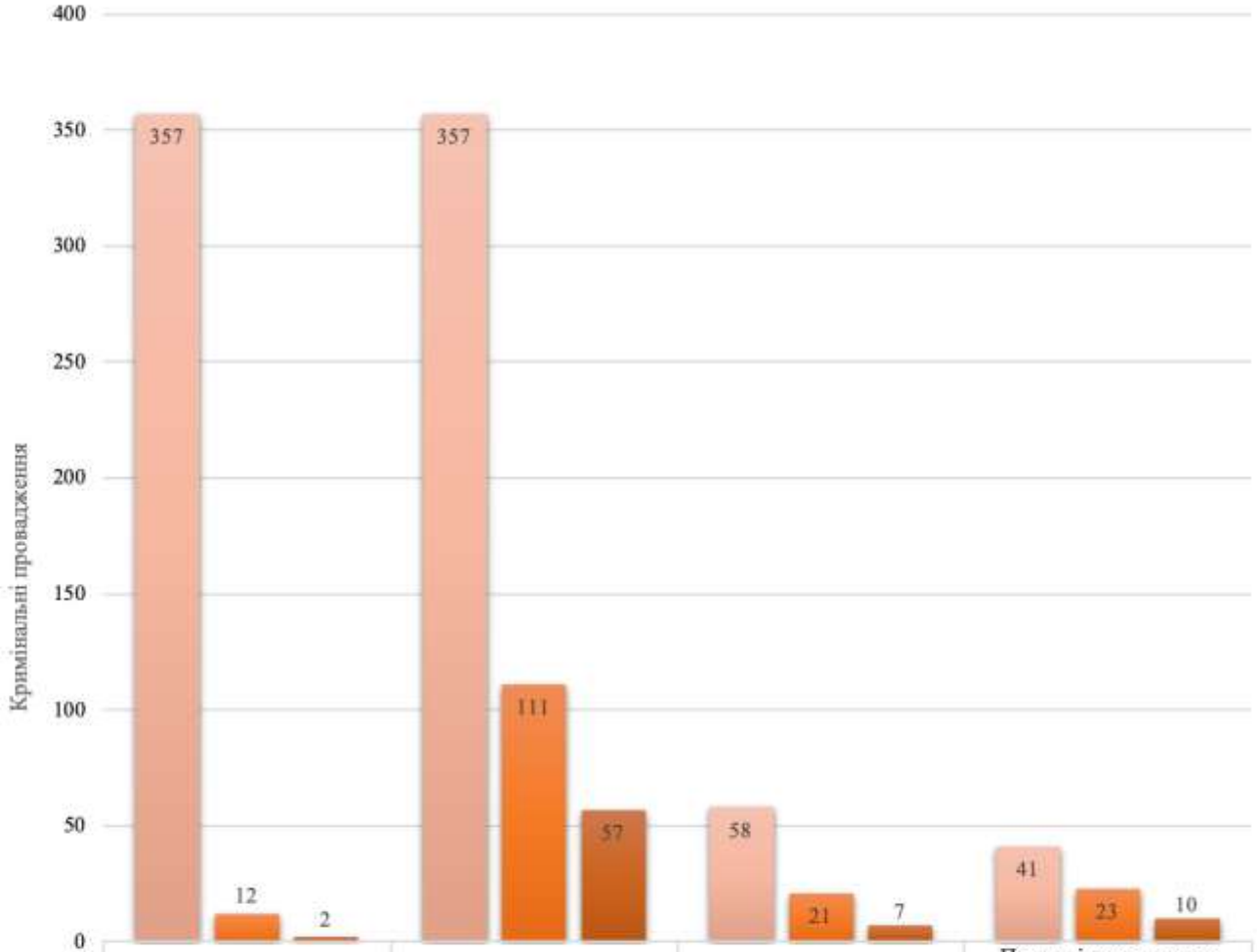
Довідка
про результати оперативно-службової діяльності підрозділів кіберполіції
(з 01.06.2021 до 27.06.2023)



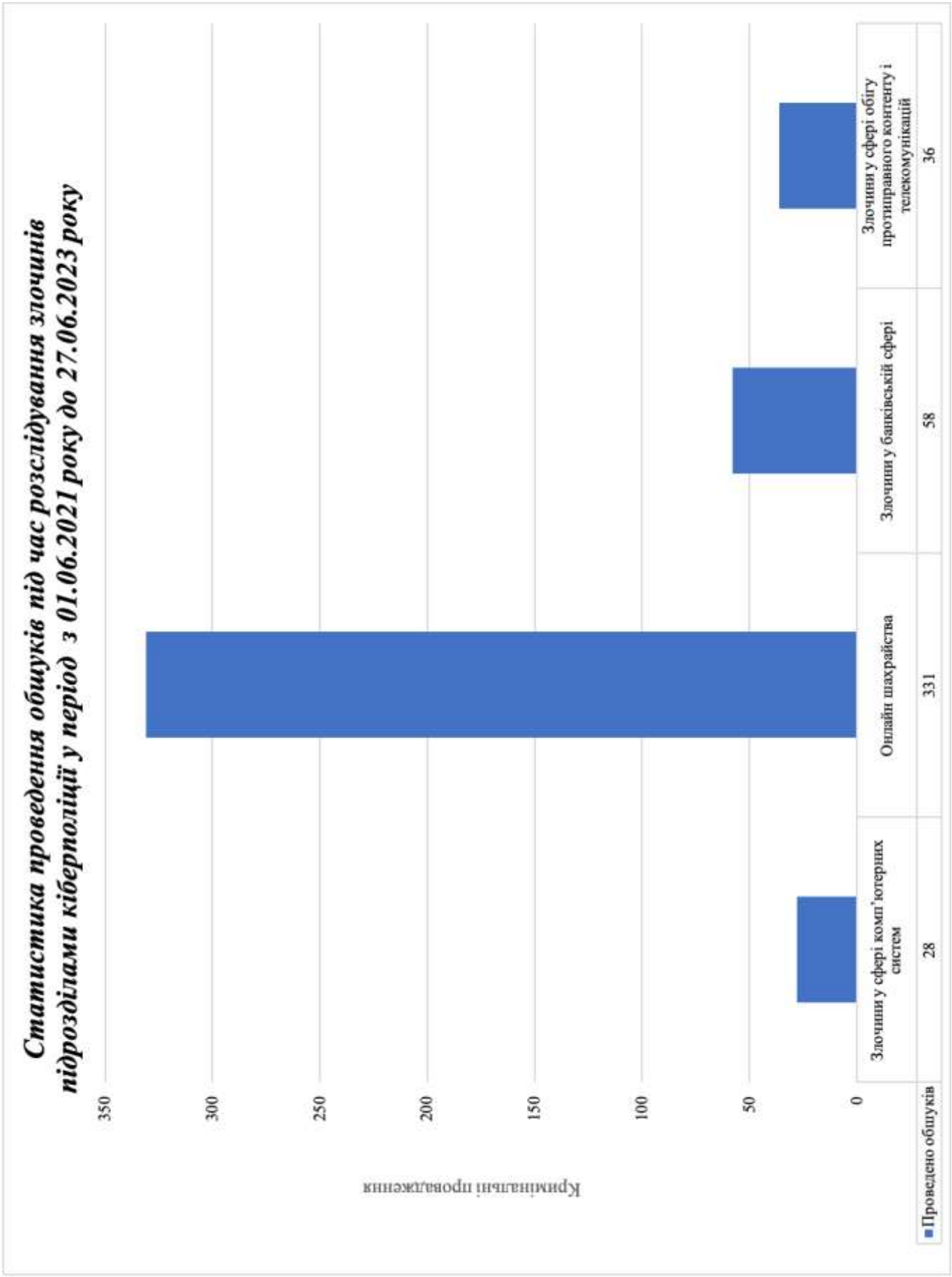
	Направлено до суду КП відносно учасників ОГ і ЗО	Внесення відомостей до ЄРДР (розпочато КП)	Реалізація матеріалів КП	Проведено обшуків	Обрання запобіжних заходів	Направлено КП до суду з обвинувальним актом
Протидія злочинам у сфері комп'ютерних систем	0	16	357	28	4	7
Протидія різновидам онлайн шахрайств	3	196	357	331	49	21
Протидія злочинам у банківській сфері	1	17	58	58	10	5
Протидія злочинам у сфері обігу протиправного контенту і телекомунікацій	0	39	41	36	8	11
Протидія злочинам у інших сферах	0	11	17	32	1	5


Статистика протидії злочинності підрозділами кіберполіції
100
90
80
70
60
50
40
30
20
10
0
Протидія злочинам у сфері комп'ютерних систем
Протидія різновидам онлайн шахрайств
Протидія злочинам у банківській сфері
Протидія злочинам у сфері обігу протиправного контенту і телекомунікацій
з 01.06.2021 року
2022 рік
до 27.06.2023 року

Статистика реалізації матеріалів кримінальних проваджень (з 01.06.2021 року до 27.06.2023 року)



	Протидія злочинам у сфері комп'ютерних систем	Протидія різновидам онлайн шахрайств	Протидія злочинам у банківській сфері	Протидія злочинам у сфері обігу протиправного контенту і телекомунікацій
Реалізація матеріалів КП (із повідомленнями про підозру та затриманням фігурантів)	357	357	58	41
Повідомлено про підозру (особам)	12	111	21	23
Затримано осіб	2	57	7	10


Статистика проведення обшуків під час розслідування злочинів підрозділами кіберполіції у період з 01.06.2021 року до 27.06.2023 року
Кримінальні провадження
350
300
250
200
150
100
50
0
Проведено обшуків
Злочини у сфері комп'ютерних систем
28
Онлайн шахрайства
331
Злочини у банківській сфері
58
Злочини у сфері обігу протиправного контенту і телекомунікацій
36

Додаток Г

ЗАТВЕРДЖУЮ

Начальник Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України, генерал поліції третього рангу

Юрій ВИХОДЕЦЬ

10 2023 року

АКТ

впровадження результатів дисертаційного дослідження Куліуша Вячеслава Миколайовича на тему «Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору», поданого на здобуття наукового ступеня доктора філософії за спеціальністю 081-Право у практичну діяльність Департаменту кіберполіції Національної поліції України

Комісія у складі:

1) першого заступника начальника Департаменту кіберполіції (міжрегіональний територіальний орган) Національної поліції України полковника поліції А.П. Шаронова;

2) т.в.о. заступника начальника Департаменту кіберполіції – начальника 2-го управління (організаційно-аналітичної роботи за забезпечення діяльності) (міжрегіональний територіальний орган) Національної поліції України полковника поліції С.М. Березюка;

3) заступника начальника Департаменту кіберполіції - начальника 1-го управління (оперативного реагування) (міжрегіональний територіальний орган) Національної поліції України полковника поліції О.Д. Заворотнього;

- склала цей акт з приводу того, що результати дослідження викладені у наукових публікаціях за результатами дисертаційного дослідження Куліуша Вячеслава Миколайовича **«Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору»** використовуються у практичній діяльності Департаменту кіберполіції НП України під час проведення занять із особовим складом та здійснення оперативно-розшукової роботи та розслідування злочинів, які вчиняються у кіберпросторі.

У практичній діяльності також використовуються методичні матеріали дисертаційного дослідження В.М. Куліуша. Зокрема, у практичній діяльності

використовуються результати наукового дослідження викладені у таких наукових публікаціях:

1. Куліуш В.М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. № 2. С. 190-193.

2. Куліуш В.М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178-183.

3. Куліуш В.М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. № 1. С. 80-84.

4. Куліуш В. Взаємозв'язки між окремими формами злочинної діяльності у сфері економіки та функціонуванням кіберпростору. *Юридичний вісник*. 2023. № 2. С. 156-163.

5. Куліуш В.М. Обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали Міжнародної науково-практичної конференції. м. Дніпро, 14-15 січня 2022 р. Дніпро : 2022. С. 92-94.

6. Куліуш В.М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнародної науково-практичної конференції. м. Львів, 18-19 лютого 2022 р. Львів, 2022. С. 14-17.

Члени комісії:

Перший заступник начальника
Департаменту кіберполіції
(міжрегіональний територіальний орган)
Національної поліції України
полковник поліції **Андрій ШАРОНОВ**

Т.в.о. заступника начальника Департаменту кіберполіції –
начальник 2-го управління (організаційно-аналітичної
роботи за забезпечення діяльності)
(міжрегіональний територіальний орган)
Національної поліції України
полковник поліції **Сергій БЕРЕЗЮК**

Заступник начальника Департаменту кіберполіції –
начальник 1-го управління (оперативного реагування)
(міжрегіональний територіальний орган)
Національної поліції України
полковник поліції **Олег ЗАВОРОТНИЙ**

14730/38/100/01-2023
31.10.2023

ЗАТВЕРДЖУЮ
Проректор з навчальної роботи
Національного університету
«Одеська юридична академія»,
доктор юридичних наук, професор

Галина УЛЬЯНОВА

«6» березня 2023 року

АКТ
впровадження в освітній процес Національного університету «Одеська юридична академія» результатів дисертаційного дослідження Куліуша Вячеслава Миколайовича на тему «Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору», поданого на здобуття наукового ступеня доктора філософії за спеціальністю 081-Право

Комісія у складі:

1) начальника навчально-методичного відділу Л. Кузнецової;

2) завідувача кафедри криміналістики, доктора юридичних наук, професора В.Тіщенка;

3) доцента кафедри криміналістики, доктора юридичних наук, професора Д. Цехана

склала цей акт з приводу того, що результати дослідження, викладені у наукових публікаціях за результатами дисертаційного дослідження Куліуша Вячеслава Миколайовича на тему «Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору» використовуються в освітньому процесі Національного університету «Одеська юридична академія» під час викладання навчальних дисциплін: «Криміналістика», «Методика і тактика розслідування злочинів». Студентам у вигляді методичних матеріалів під час підготовки до практичних занять рекомендуються опубліковані автором наукові статті, а саме:

1. Куліуш В.М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. № 2. С. 190-193.

2. Куліуш В.М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178-183.

3. Куліуш В.М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. № 1. С. 80-84.

4. Куліуш В. Взаємозв'язки між окремими формами злочинної діяльності у сфері економіки та функціонуванням кіберпростору. *Юридичний вісник*. 2023. № 2. С. 156-163.

5. Куліуш В.М. Обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали Міжнародної науково-практичної конференції. м. Дніпро, 14-15 січня 2022 р. Дніпро : 2022. С. 92-94.

6. Куліуш В.М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнародної науково-практичної конференції. м. Львів, 18-19 лютого 2022 р. Львів, 2022. С. 14-17.

7. Куліуш В.М. Окремі аспекти оперативного (ініціативного) пошуку ознак злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Актуальні питання кримінального провадження у сучасних умовах* : матеріали міжнародної науково-практичної конференції, м. Одеса, 31 травня 2023 р. Одеса : ОДУВС, 2023. С. 137-139.

Крім цього, результати дисертаційного дослідження Куліуша Вячеслава Миколайовича використовуються під час визначення напрямів наукових пошуків і тем дисертацій викладачів, аспірантів і здобувачів Національного університету «Одеська юридична академія».

Члени комісії:

Начальник навчально-методичного відділу Національного університету «Одеська юридична академія» — **Людмила КУЗНЕЦОВА**

Завідувач кафедри криміналістики Національного університету «Одеська юридична академія», доктор юридичних наук, професор — **Валерій ТІЩЕНКО**

доцент кафедри криміналістики Національного університету «Одеська юридична академія», доктор юридичних наук, професор — **Дмитро ЦЕХАН**

ЗАТВЕРДЖУЮ
Перший проректор Національної академії внутрішніх справ,
доктор юридичних наук, професор

Станіслав ГУСАРЄВ

2023 р.

АКТ
про впровадження результатів дисертаційного дослідження аспіранта кафедри криміналістики та судової медицини Національної академії внутрішніх справ Куліуша Вячеслава Миколайовича на тему «Виявлення та розслідування злочинів економічної спрямованості, вчинених із використанням кіберпростору» у освітній процес Національної академії внутрішніх справ

Комісія у складі: професора кафедри криміналістики та судової медицини, доктора юридичних наук, професора **Ю.М. Чорноус** (*голова комісії*), т.в.о. завідувача кафедри кримінального процесу, кандидата юридичних наук, доцента **О.Ю. Хабло** та заступника навчально-методичного відділу, кандидата юридичних наук **Б.Ю. Бистрицького** склала цей акт про те, що наукові роботи, підготовлені Куліушом Вячеславом Миколайовичем, використовуються у освітньому процесі Національної академії внутрішніх справ.

Отримані в результаті дослідження висновки, пропозиції та рекомендації відображені в опублікованих автором працях, основними з яких є:

1. Куліуш В.М. Формування та реалізація криміналістичних комплексів на початковому етапі розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Юридичний науковий електронний журнал*. 2022. № 2. С. 190-193. URL : http://www.lsej.org.ua/2_2022/42.pdf
2. Куліуш В.М. Взаємозв'язки між окремими формами злочинної діяльності в сфері економіки та функціонування кіберпростору. *Південноукраїнський правничий часопис*. 2022. № 3. С. 178-183. URL : http://www.sulj.oduvs.od.ua/archive/2022/3/29.pdf
3. Куліуш В.М. Характеристика структурних елементів злочинної діяльності економічної спрямованості, яка здійснюється із використанням кіберпростору. *Південноукраїнський правничий часопис*. 2023. № 1. С. 80-84. URL : http://www.sulj.oduvs.od.ua/archive/2023/1/14.pdf
4. Куліуш В. Взаємозв'язки між окремими формами злочинної діяльності у сфері економіки та функціонуванням кіберпростору. *Юридичний вісник*. 2023. № 2. С. 156-163. URL : http://yurvisnyk.in.ua/v2_2023/20.pdf

5. Куліуш В.М. обшук як інструмент збирання доказів під час розслідування злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Сучасні наукові дослідження представників юридичної науки – прогрес законодавства України майбутнього* : матеріали Міжнародної науково-практичної конференції, (м. Дніпро, 14-15 січня 2022 р.). Дніпро : 2022. С. 92-94.

6. Куліуш В.М. Особливості виявлення протиправної діяльності Інтернет-магазинів. *Право як ефективний суспільний регулятор* : матеріали Міжнародної науково-практичної конференції, (м. Львів, 18-19 лютого 2022 р.). Львів, 2022. С. 14-17.

7. Куліуш В.М. Окремі аспекти оперативного (ініціативного) пошуку ознак злочинної діяльності економічної спрямованості, вчиненої із використанням кіберпростору. *Актуальні питання кримінального провадження у сучасних умовах* : матеріали міжнародної науково-практичної конференції, (м. Одеса, 31 травня 2023 р.). Одеса : ОДУВС, 2023. С. 137-139. URL : https://dspace.oduvs.edu.ua/server/api/core/bitstreams/391cb1b2-076a-4807-8a7f-e1475032c703/content

Члени комісії дійшли висновку, що надані матеріали свідчать про належний науковий та практичний рівень розробки теми дослідження, грунтуються на достатній кількості опрацьованих Куліушем В.М. законодавчих, наукових та емпіричних джерелах, використовуються під час підготовки лекцій, посібників, методичних рекомендацій, тестових завдань і дидактичних матеріалів з криміналістики, кримінального права, кримінального процесу, оперативно-розшукової діяльності, а також при проведенні різних видів занять із відповідних дисциплін у процесі підготовці бакалаврів та магістрів за спеціальністю 081 «Право» та в системі підвищення кваліфікації працівників системи МВС України.

Голова комісії: **Юлія ЧОРНОУС**

Члени комісії: **Оксана ХАБЛО**

Богдан БИСТРИЦЬКИЙ