Олена Самойленко

докторка юридичних наук, доцентка,
професорка кафедри криміналістики
Національного університету
“Одеська юридична академія”
(Одеса, Україна)
ORCID ID: https://orcid.org/0000-0002-8925-4116
samoilenko_elena@ukr.net

DOI: 10.33498/louu-2021-08-131

УДК 343.3

ПРОТИДІЯ КРИМІНАЛЬНИМ ПРАВОПОРУШЕННЯМ, УЧИНЕНИМ У КІБЕРПРОСТОРІ, ЯК НОВИЙ НАПРЯМ КРИМІНАЛІСТИКИ

Анотація. Діяльність із розслідування кримінальних правопорушень потребує реалізації широкого кола завдань правоохоронних органів, серед яких одним з основних завдань визнається протидія кримінальним правопорушенням. Сьогодні середовищем вчинення більшості останніх є кіберпростір. Телекомунікаційна мережа, комп’ютерна інформація та інші елементи такого середовища будуть предметом, знаряддям та/або засобом широкого кола злочинних посягань – від сфери національної безпеки до відносин власності. Десятиліттями в криміналістиці приділялася увага проблемам розслідування лише тих діянь, які докладно описані як кіберзлочини в Конвенції про кіберзлочинність, що, звісно, не відповідало умовам часу.

Метою статті є дослідження протидії кримінальним правопорушенням, учиненим у кіберпросторі, як нового напряму криміналістичної науки.

У статті визначені й описані складнощі, що виникають на шляху успішності теоретичних розробок, і перспективи дослідження окремих структурних одиниць визначеного наукового напряму.

Встановлено, що структурно науковий пошук учених у цьому напрямі можна активізувати для вирішення двох груп завдань: 1) формування концептуальних засад протидії таким правопорушенням; 2) визначення структурних одиниць вказаного напряму, зокрема напрямів формування методик розслідування кримінальних правопорушень, учинених у кіберпросторі; відповідно, розроблення останніх.

У результаті аналізу криміналістичної діяльності з протидії злочинності та на підставі наявних розробок у галузі філософії, кібернетики та телекомунікаційних технологій конкретизовані вихідні загальнотеоретичні положення у досліджуваному науковому напрямі криміналістики. По-перше, виокремлено два рівня злочинної діяльності у кіберпросторі, зокрема: 1) сукупність одиничних злочинів, що мають взаємозв’язок за розвитком; 2) злочинні технології. По-друге, криміналістичну класифікацію цієї множини правопорушень визнано підґрунтям розроблення комплексної методики (теоретико-методичних засад) розслідування кримінальних правопорушень, учинених у кіберпросторі. По-третє, обґрунтовано, що полімотивованість злочинної діяльності у кіберпросторі є принциповим підходом при розв’я-

занні питань оптимізації протидії відповідній категорії правопорушень. По-четверте, спільний аналітичний підхід до процесу протидії кібрзлочинам уповноважених на це суб'єктів і ситуаційну обумовленість визнано ключовими аспектами побудови та реалізації тактичних операцій при розслідуванні кримінальних правопорушень, учинених у кіберпросторі.

Ключові слова: кіберпростір; кримінальне правопорушення; напрям; протидія; розслідування; технологія.

В умовах сучасного інформаційного суспільства кримінальне правопорушення є динамічним соціальним явищем. Зв'язки між складовими його структури відбуваються в умовах об'єктивної реальності – середовища, яким сьогодні для вчинення більшості різноманітних злочинів стає кіберпростір – телекомунікаційна мережа, комп'ютерна інформація та інші елементи такого середовища слугують предметом, знаряддям та/або засобом широкого кола злочинних посягань – від сфери національної безпеки до відносин власності.

У цій галузі криміналістики увага здебільшого приділялася проблемам розслідування кіберзлочинів (П. Біленчук, А. Білоусов, В. Бутузов, А. Волобуєв, В. Гавловський, В. Голубєв, М. Гуцалюк, М. Карчевський, О. Мотлях, І. Осика, Л. Паламарчук, Д. Пашнєв, А. Реуцький, М. Салтевський, С. Самойлов, Є. Скулиш, К. Тітуніна, В. Хахановський та багато інших науковців). Утім, враховуючи сучасну правову регламентацію, діяльність із розслідування кримінальних правопорушень потребує реалізації широкого кола завдань правоохоронних органів. Відповідно до ч. 1 ст. 2 Закону України "Про Національну поліцію" до кола основних завдань відноситься, зокрема, протидія злочинності[1]. Соціопсихологічний підхід до аналітики дії та протидії свідчить про те, що реальна протидія суб'єктів може розгортатися лише в площині діяльності при наявності конфліктів інтересів цих суб'єктів[2]. Тож основою протидії є конфлікт інтересів, що зазвичай є нормою у кримінально-процесуальних відносинах, адже останні виникають у зв'язку з пошуком і залученням до кримінальної відповідальності конкретної особи та припускають настання відносно неї покарання. Так, працівник оперативного підрозділу має своїм безпосереднім завданням пошук і фіксацію фактичних даних про кримінальні правопорушення у кіберпросторі; слідчий – здійснення досудового розслідування таких правопорушень, під час якого прагне встановити приховувані у цифровому середовищі факти й обставини та подолати опір із боку незацікавлених в успішному розслідуванні справи осіб; злочинець-користувач – уникнути кримінальної відповідальності або покарання, виконуючи для цього різні дії. Наявність протилежних

[1] Про Національну поліцію України: Закон України від 2 липня 2015 р. № 580-VIII <https://zakon.rada.gov.ua/laws/show/580-19> (дата звернення: 26.08.2021).

[2] Л Герасіна, М Требін, В Воднік та інші, *Конфліктологія: навчальний посібник* (Право 2012) 9.

цілей працівника оперативного підрозділу та слідчого зі злочинцем-користувачем і обумовлює конфліктну ситуацію, у якій переважно відбувається виявлення та розслідування злочинної діяльності, пов'язаної із кіберпростором.

Метою дослідження є вивчення протидії кримінальним правопорушенням, учиненим у кіберпросторі, як нового напряму криміналістичної науки.

Напрям у загальному значенні тлумачиться як 'лінія руху або лінія розміщення кого-, чого-небудь; шлях діяльності, розвитку кого-, чого-небудь; спрямованість якоїсь дії, явища; спрямованість думок, інтересів'[3]. Сучасна тенденція в розвитку нових напрямів криміналістики зумовлюється ускладненням тих форм діяльності, що є об'єктом дослідження криміналістичної науки[4]. Діяльність із протидії злочинності в умовах сьогодення потребує використання більш широкого кола джерел доказової інформації – це різноманітні носії цифрової інформації: моноблоки, мобільні пристрої (мобільні телефони, планшетні комп'ютери), цифрові камери, роутери, маршрутизатори, комп'ютерні мережі, глобальна мережа Інтернет, звуко- та відеозаписи тощо. При цьому електронні пристрої можуть розміщуватися або на місці проведення розслідування, або бути територіально дуже віддалені, що пояснюється інтенсивним розвитком децентралізованої технології обміну й зберігання інформації, технологіями анонімізації доступу до ресурсів мережі Інтернет. Це має своїм наслідком, з одного боку, необхідність вивчення комплексу злочинів якісно нового рівня організації злочинної діяльності, а з другого – розроблення та використання сучасних засобів і форм роботи з інформацією. Вказані завдання можливо реалізувати в результаті всебічного використання досягнень сучасної науки і техніки. Відзначимо, що В. Шепітько обґрунтовано диференціює завдання криміналістики на два основних рівні: 1) завдання, спрямовані на вдосконалення теорії криміналістики; 2) завдання, спрямовані на вдосконалення правозастосовної практики[5]. З огляду на викладене вважаємо, що дослідження протидії кримінальним правопорушенням, учиненим у кіберпросторі, спрямовуватиметься на: 1) формування концептуальних засад протидії таким правопорушенням; 2) визначення структурних одиниць вказаного напряму, зокрема напрямів формування методик розслідування кримінальних правопорушень, учинених у кіберпросторі; відповідно, розроблення останніх.

Аналіз наукових праць із досліджуваної проблематиці свідчить про відсутність лаконічної пропорції між теоретичним і прикладним рівнями

[3] *Великий тлумачний словник сучасної української мови* (Бусел Т уклад і голов ред, Перун 2002) 576.

[4] В Тіщенко, 'Технологічний підхід як новаційний напрям у розвитку криміналістичної науки' в Тіщенко В, *Вибрані праці* (Гельветика 2017) 68.

[5] В Шепитько, 'Криминалистика в системе юридических наук и ее роль в глобальном мире' в *Криміналістика та судова експертиза: наука, навчання, практика: збірник наукових праць, т 1* (2014) 150.

розробок питань протидії кримінальним правопорушенням, учиненими у кіберпросторі. Десятиліттями криміналісти розробляли розрізнені методики розслідування та засоби протидії окремих видів кіберзлочинів у розумінні Конвенції про кіберзлочинність[6], зокрема як діянням, об'єктом злочину яких є комп'ютерні дані або системи, або за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину (зокрема, передбачені статтями 176, 185, 190, 200, 229, 231, 232, 300, 301, 361–363[1] Кримінального кодексу України (далі – КК України)[7]). Це пояснюється тим, що тривалий час центральне місце в Україні в механізмі правового регулювання боротьби з кримінальними правопорушеннями, учиненими в кіберпросторі, займали норми вказаної Конвенції, окремі положення якої вже не відповідають умовам часу. Через регламентацію на національному законодавчому рівні альтернативних їй складів кримінальних правопорушень і розширення у середньостроковій перспективі безпекових гарантій та спроможностей України лише протягом останніх п'яти років простежується тенденція вивчити та розкрити закономірності діяльності з протидії злочинності у кіберпросторі. Концептуальним у криміналістичній науці стає визнання окремими криміналістами кіберпростору середовищем злочинної діяльності й одночасно об'єктом криміналістичних досліджень[8].

По суті кіберпростір можна розглядати у двох значеннях: а) середовище, окремі елементи (телекомунікаційна мережа, комп'ютерна інформація, інформаційні технології тощо) якого можуть використовуватись як знаряддя злочину (властиво безпосередньо кіберзлочинам – конвенційним кримінальним правопорушення); б) специфічне середовище для слідоутворення, наприклад, щодо злочинів проти основ національної безпеки України (статті 109–114 КК України), у сфері охорони державної таємниці (статті 328, 330); проти виборчих прав і свобод (ст. 157, 158, 159, 159[1] КК України); проти власності (ст. 185, 189, 191); у сфері господарської діяльності (статті 206, 209, 231, 232 КК України); пов'язаних із тероризмом (статті 258, 258[2], 258[3], 258[5] КК України); у сфері незаконного обігу наркотичних засобів (статті 307, 311 КК України); придбання чи

[6] Конвенція про кіберзлочинність від 11 листопада 2001 р. <https://zakon.rada.gov.ua/laws/show/994_575#Text> (дата звернення: 14.07.2021).

[7] Кримінальний кодекс України: Закон України від 5 квітня 2001 р. № 2341-III <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 14.07.2021).

[8] В Мещеряков, *Преступления в сфере компьютерной информации: основы теории и практики расследования* (Воронеж гос ун-т, 2002) 407; 'Crime scene cyberspace. Globe' (2012. No. 3). Sept. <https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/documents/news2012/ETHglobe_ZISC_SEP2012.pdf> (accessed: 26.08.2021); В Динту, 'Місце кіберпростору в системі обстановки злочину' [2016] 2 (3) Науковий вісник Херсонського державного університету 72–5; О Стрільців, О Тарасенко, І Курилін та інші, *Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами: методолічні рекомендації* (2017) 44; О Самойленко, 'Природа кіберпростору як об'єкта криміналістичного дослідження' [2018] 63 (1) Криміналістика і судова експертиза 174–84.

збут зброї, бойових припасів або вибухових речовин, аналогічних дій і використання спеціальних технічних засобів отримання інформації (статті 263, 359 КК України) тощо.

Звичайно, вказані групи кримінальних правопорушень характеризуються різноманітністю їх кримінально-правових ознак, однак використання інформаційно-комунікаційних технологій (кібертехнологій), що забезпечує інтерактивну взаємодію способів підготовки, вчинення та приховування злочинів, а також досягнення кінцевої злочинної мети, зумовлює ступінь складності останніх, особливу концентрацію та організацію зусиль правоохоронних органів щодо протидії кримінальним правопорушенням, учиненим у кіберпросторі. Сукупність органічно пов'язаних явищ і процесів свідчить про можливість сформувати теоретичну побудову щодо протидії вказаній категорії правопорушень.

Р. Бєлкін доводив, що у межах окремих теоретичних положень пізнання може дійти до знання окремих закономірностей предмета дослідження; об'єктивний же зв'язок цих закономірностей, тобто знання закономірностей більш поглибленої сутності, – це вже рівень окремої криміналістичної теорії[9]. Спираючись на висновки і положення, обґрунтовані сучасними розробками в галузі філософії, кібернетики та телекомунікаційних технологій, а також у результаті аналізу криміналістичної діяльності з протидії злочинності можна представити такі методологічні положення стосовно досліджуваного напряму криміналістики[10].

По-перше, використання системно-структурного методу для аналізу злочинної діяльності забезпечує виокремлення двох її рівнів у кіберпросторі: 1) сукупність одиничних злочинів, що мають взаємозв'язок за розвитком (способи їх вчинення мають тенденцію до вдосконалення; кіберпростір слугує середовищем, яке містить сліди взаємопов'язаного за розвитком комплексу злочинів); 2) комплекс технологічно взаємопов'язаних злочинів, в якому злочини, передбачені розділом XVI КК України, слугують обов'язковою умовою досягнення злочинного результату (злочинні технології).

По-друге, предмет доказування у наведених вище комплексах злочинів є значно ширшим, що, зі свого боку, зумовлює розроблення комплексної методики (теоретико-методичних засад) розслідування кримінальних правопорушень, учинених у кіберпросторі. Підґрунтям для її розроблення є криміналістична класифікація досліджуваних злочинів, адже розмежування усіх термінологічних конструкцій у межах наук кримінально-правового циклу здійснюється із застосуванням методу класифікації. Функціональною спрямованістю криміналістичної

[9] Р Белкин, *Курс криминалистики: учебник* (3-е изд, доп, Закон и право 2001) 285.
[10] О Самойленко, *Основи методики розслідування злочинів, вчинених у кіберпросторі* (Волобуєв А ред, ТЕС 2020).

класифікації таких кримінальних правопорушень буде визначення їхніх взаємозв'язків, уникнення повторів однакових правопорушень у межах кваліфікаційних груп, а також розроблення і конкретизація різних видів (рівнів) методик їх розслідування.

По-третє, полімотивованість злочинної діяльності у кіберпросторі є принциповим підходом при розв'язанні питань оптимізації протидії вказаної категорії правопорушень. Використання кіберпростору забезпечує досягнення злочинної мети, в кожному конкретному випадку злочину. Досягнення мети злочину означає, що спонукання діяння мотивом закінчилося і певна потреба задовольнилася[11]. Мета досягається певним мотивом, на думку А. Савченко, у цьому саме й полягає їхній зв'язок. Мотив злочину – це ті внутрішні спонукання, якими керувався винний, вчиняючи злочин. Основний мотив при вчиненні комплексу злочинів у кіберпросторі по суті виконує роль вектору всієї злочинної діяльності особи в середовищі кіберпростору, проходить крізь причинний зв'язок між злочинними діяннями та кінцевим наслідком, дає змогу встановити взаємозв'язки між злочинами злочинної сукупності у кіберпросторі. Під час її розслідування перед слідчим постає завдання – встановити всю множину кримінальних правопорушень, учинюваних особою в середовищі кіберпростору. Додатковий же мотив має системоутворююче значення щодо певної злочинної технології, забезпечуючи досягнення кінцевої злочинної мети, відповідно, зумовлює певний комплекс злочинів у технології злочинної діяльності, склад організованої групи, особливості обрання певного предмета посягання. Отже, з позицій технологічного та комплексного характеру злочинної діяльності у кіберпросторі мотив є категорією, що має особливе криміналістичне значення.

Так, мотив ми можемо використовувати для цілей класифікації правопорушень у кіберпросторі. Мотив має виражене соціально-психологічне значення, від чого походить безліч класифікацій мотивів у психології чи юридичних науках[12]. Кіберпростір як середовище вчинення злочину також характеризується соціальними чинниками через можливість задовольняти потреби конкретної людини у певній сфері суспільних відносин. Беручи до уваги традиційні сфери суспільного життя суб'єктів кіберпростору, класифікуємо мотиви вчинення злочинів на такі групи: 1) корисливі мотиви, пов'язані з фінансово-економічною сферою відносин суб'єктів у кіберпросторі; 2) соціально-економічні мотиви, пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі; 3) політичні мотиви, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі; 4) ідейні мотиви, пов'язані зі світоглядною сферою жит-

[11] А Савченко, *Мотив і мотивація злочину* (Атіка 2002) 22.
[12] Б Волков, *Проблема воли и уголовная ответственность* (Изд-во Казан ун-та 1965); М Бажанов, *Уголовное право Украины. Общая часть* (Пороги 1992).

тя суб'єктів відносин у кіберпросторі. Відповідно, класифікуються й кримінальні правопорушення, учинені в кіберпросторі, на чотири групи: 1) злочини, вчинені з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі; 2) злочини, вчинені з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі; 3) злочини, вчинені з політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі; 4) злочини, вчинені з ідейних мотивів, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

Технологія злочинної діяльності (що пов'язана з додатковим мотивом) використовується для виділення підгруп злочинів всередині основних класифікаційних груп. Це створює теоретичне підґрунтя для визначення у подальшому структурних одиниць певного наукового напряму, адже компоненти будь-якої структури не існують ізольовано один від одного, певним чином мають бути впорядковані. За допомогою паралельного застосування методу емпіричного узагальнення можна відзначити перспективність розроблення окремих проблематик, наприклад, інтенсивне впровадження в Україні технологій електронного урядування поставило на порядок денний завдання щодо протидії службовим злочинам, вчиненим у кіберпросторі, розроблення методики розслідування кіберзлочинів, учинених у складі організованих груп і злочинних організацій.

По-четверте, ключовим аспектом побудови та реалізації тактичних операцій при розслідуванні кримінальних правопорушень, учинених у кіберпросторі, є не тільки їхня ситуаційна обумовленість, а й спільний аналітичний підхід до процесу протидії кіберзлочинам уповноважених на це суб'єктів. Цей процес розпочинається у момент викриття правопорушення та активно здійснюється під час розслідування і судового розгляду. Тому в наукових дослідженнях визначеного напряму слід враховувати роль оперативних підрозділів різних відомств, форми та засоби організації взаємодії слідчого із ними (під час оцінки матеріалів первинної перевірки інформації, реалізації ним методичної функції в момент викриття злочину та слідчої діяльності), а також специфіку поєднання слідчих (розшукових) і негласних слідчих (розшукових) дій у процесі формування тактичних операцій.

Як справедливо наголошує В. Шевчук, саме тактичні операції активізують та організовують процеси взаємодії правоохоронних органів, слугують засобом реалізації методів розслідування, вирішення окремих тактичних завдань[13]. Враховуючи зміст вирішуваних слідчим спільно з оперативним підрозділом тактичних завдань щодо розслідування кримінальних правопорушень, учинених у кіберпросторі, вважаємо за потрібне побудову та реалізацію таких тактичних операцій, як "Персо-

[13] В Шевчук, *Криміналістика: традиції, новації, перспективи: добірка наукових праць* (Право 2020) 150.

налізація відомостей про особу/осіб злочинця/злочинців", "Встановлення кінцевого мотиву злочинної діяльності в кіберпросторі", "Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи", "Встановлення технології злочинної діяльності з використанням кіберпростору". Їхня внутрішня структура також визначатиметься аналітичним підходом у питанні поєднання слідчих і негласних слідчих (розшукових) дій, що проявлятиметься через спільне розв'язання суб'єктами протидії кіберзлочинам комплексу стандартних завдань з урахуванням практичних аспектів оперативно-розшукової та слідчої діяльності.

Зазначені загальнотеоретичні положення слід вважати вихідними для досліджуваного наукового напряму, такими, що дають змогу здійснювати подальші криміналістичні напрацювання засобів, прийомів і методів протидії кримінальним правопорушенням, учиненим у кіберпросторі.

На шляху успішності розроблення вказаного напряму існують і певні труднощі, пов'язані з недосконалістю правової та, відповідно, емпіричної баз. Широке коло питань в Україні досі вимагає детальної правової регламентації.

По-перше, щодо цивільного обігу віртуальних активів (криптовалют). Відповідно до Закону України "Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового ураження" віртуальним активом є цифрове вираження вартості, яким можна торгувати у цифровому форматі або переказувати, та яке може використовуватися для платіжних або інвестиційних цілей[14]. Для того щоб об'єкт вважався віртуальним активом, він має відповідати трьом критеріям: 1) наявність вартості; 2) можливість до обігу в цифровому форматі; 3) можливість до його обміну на інші об'єкти цивільного права. Перевага злочинців при злочинних посяганнях, пов'язаних із обігом криптовалюти, зумовлена технологією *DLT* (системою розподіленого реєстру, блокчейн), її нейтральністю щодо власника, а також абсолютною законодавчою неврегульованістю діяльності осіб на віртуальних криптовалютних біржах (ринках збуту криптовалюти).

По-друге, щодо використання слідчим міждержавних контактних пунктів 24/7, електронних системи Інтерполу I-24/7 або захищеного каналу зв'язку Європолу "*SIENA*". Декларуючи цей аспект взаємодії слідчого з оперативними підрозділами в окремих відомчих актах, ні держава, ні наукова спільнота не прописують механізми ефективного й оператив-

[14] Про запобігання та протидію легалізації (відмиванню) доходів, одержаних злочинним шляхом, фінансуванню тероризму та фінансуванню розповсюдження зброї масового ураження: Закон України від 6 грудня 2019 р. № 361-IX <https://zakon.rada.gov.ua/laws/show/361-20#Text> (дата звернення: 26.08.2021).

ного застосування можливостей міжнародних поліцейських організацій із метою протидії злочинам у кіберпросторі.

По-третє, щодо впровадження у практику правоохоронних органів інформаційно-аналітичних комплексів. Згідно із нещодавно схваленою Кабінетом Міністрів України Концепцією розвитку штучного інтелекту в Україні штучний інтелект – це організована сукупність інформаційних технологій, із застосуванням якої можливо виконувати складні комплексні завдання за допомогою використання системи наукових методів досліджень і алгоритмів обробки інформації, отриманої або самостійно створеної під час роботи, а також створювати та використовувати власні бази знань, моделі прийняття рішень, алгоритми роботи з інформацією та визначати способи досягнення поставлених завдань[15]. Серед напрямів впровадження технологій штучного інтелекту в сфері кібербезпеки значиться розроблення та впровадження у практику правоохоронних органів інноваційних систем кібербезпеки, які широко застосовують технології штучного інтелекту для автоматичного аналізу та класифікації загроз і автоматичного вибору стратегії їх стримування і запобігання. Сьогодні активно впроваджується у практику роботи Національної поліції відеоаналітичні платформи й інтелектуальні системи кримінального аналізу. Однак досить складним питанням для науковців залишається збір практичного матеріалу з таких джерел інформації. Законодавчо закріплена можливість їх використання суттєво вплинула б на якість криміналістичних рекомендацій, апробацію результатів прикладних наукових досліджень за напрямом протидії кримінальним правопорушенням, учиненим у кіберпросторі.

Висновки. З урахуванням наведеного вище можна констатувати перспективність дослідження у криміналістичній науці проблематики протидії кримінальним правопорушенням, учиненим у кіберпросторі. Структурно науковий пошук учених у цьому напрямі можна активізувати для вирішення двох груп завдань: 1) формування концептуальних засад протидії таким правопорушенням; 2) визначення структурних одиниць вказаного напряму, зокрема напрямів формування методик розслідування кримінальних правопорушень, учинених у кіберпросторі; відповідно, розроблення останніх. Незважаючи на наявність окремих складнощів на шляху теоретичних розробок вказаного напряму, їхнє здійснення вже суттєво збагатило науку, а в перспективі забезпечить вирішення важливих проблем криміналістичної тактики та методики, загалом підвищить ефективність правозастосовної практики правоохоронних органів.

[15] Про схвалення Концепції розвитку штучного інтелекту в Україні: Розпорядження Кабінета міністрів України від 2 грудня 2020 р. № 1556-р <https://zakon.rada.gov.ua/laws/show/1556-2020-%D1%80#Text> (дата звернення: 26.08.2021).

REFERENCES

Bibliography

Authored books

1. Bazhanov M, *Ugolovnoe pravo Ukrainy. Obshhaja chast* (Porogi 1992) (in Russian).
2. Belkin R, *Kurs kriminalistiki: uchebnik* (3-e izd, dop, Zakon i pravo 2001) (in Russian).
3. Cavchenko A, *Motyv i motyvatsiia zlochynu* (Atika 2002) (in Ukrainian).
4. Meshherjakov V, *Prestuplenija v sfere komp'juternoj informacii: osnovy teorii i praktiki rassledovanija* (Voronezh gos un-t 2002) (in Russian).
5. Volkov B, *Problema voli i ugolovnaja otvetstvennost* (Izd-vo Kazan un-ta 1965) (in Russian).

Edited books

6. Herasina L, *Trebin M, Vodnik V ta in, Konfliktolohiia: navchalnyi posibnyk* (Pravo 2012) (in Ukrainian).
7. Samoilenko O, *Osnovy metodyky rozsliduvannia zlochyniv, vchynenykh u kiberprostori* (Volobuiev A red, TES 2020) (in Ukrainian).
8. Shepytko V, 'Krymynalystyka v systeme yurydycheskykh nauk y ee rol v hlobalnom myre' v *Kryminalistyka ta sudova ekspertyza: nauka, navchannia, praktyka: zbirnyk naukovyh prats, t 1* (2014) (in Russian).
9. Shevchuk V, *Kryminalistyka: tradytsii, novatsii, perspektyvy: dobirka naukovyh prats* (Pravo 2020) (in Ukrainian).
10. Striltsiv O, Tarasenko O, Kurylin I ta inshi, *Rozsliduvannia zlochyniv, pov'iazanykh z nezakonnym rozpovsiudzhenniam u merezhi Internet nediinoho kontentu provaideramy prohramnykh posluh ta Internet-provaideramy: metodychni rekomendatsii* (2017) (in Ukrainian).
11. Tishchenko V, 'Tekhnolohichnyi pidkhid yak novatsiinyi napriam u rozvytku kryminalistychnoi nauky' v Tishchenko V, *Vybrani pratsi* (Helvetyka 2017) (in Ukrainian).
12. *Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy* (Busel T uklad i hol red, Perun 2002) (in Ukrainian).

Journal articles

13. Dyntu V, 'Mistse kiberprostoru v systemi obstanovky zlochynu' [2016] 2 (3) Naukovyi visnyk Khersonskoho derzhavnoho universytetu 72–5 (in Ukrainian).
14. Samoilenko O, 'Pryroda kiberprostoru yak ob'iekta kryminalistychnoho doslidzhennia' [2018] 63 (1) Kryminalistyka i sudova ekspertyza 174–84 (in Ukrainian).

Websites

15. 'Crime scene cyberspace. Globe' (2012. No. 3). Sept. <https://www.ethz.ch/content/dam/ethz/special-interest/infk/inst-infsec/information-security-group-dam/documents/news2012/ETHglobe_ZISC_SEP2012.pdf> (accessed: 26.08.2021) (in English).

Olena Samoilenko

A NEW DIRECTION IN FORENSICS – RESISTANCE TO CRIMES THAT ARE COMMITTED IN CYBERSPACE

Abstract. Activities on the investigation of criminal offenses today require the implementation of a wide range of tasks of law enforcement agencies. Among these tasks, the main task is considered to be the fight against modern crime. Cyberspace is the setting for most of the various crimes today. These are situations of committing crimes in conditions when the telecommunications network, computer information and other elements of such an environment are the subject or means of criminal encroachments from various types, both in the field of national security and in the field of protection of private property. For decades, forensic science has paid attention to the problems of investigating only those actions that are called crimes in the Council of Europe Convention on Cyber Crime. This does not meet the conditions of the time.

The purpose of the article is to study a new area of forensic science – activities to counter criminal offenses that are committed in cyberspace.

It has been established that the structurally scientific research of scientists in this direction can be activated to solve several groups of tasks: 1) the formation of conceptual foundations of counteraction to such offenses; 2) determination of the structural units of the specified direction, in particular, the directions for the formation of methods for the investigation of criminal offenses that are committed in cyberspace; accordingly, the development of these techniques. As a result of the analysis of forensic activities in combating crime and on the basis of the available developments in the field of philosophy, cybernetics and telecommunication technologies, the initial general theoretical provisions in the investigated scientific direction of forensic science were concretized. First, there are two levels of criminal activity in cyberspace, in particular: 1) a set of isolated crimes, which have a relationship with development; 2) criminal technologies. Thirdly, it is substantiated that the totality of motives for criminal activity in cyberspace is a principled approach when solving the issues of optimizing the counteraction of offenses in cyberspace. Fourth, situational conditioning and a joint analytical approach of all participants in the counteraction are recognized as key aspects of the design and implementation of tactical operations in the investigation of criminal offenses committed in cyberspace.

Empirically identified and described the difficulties that arise on the path to the success of theoretical developments. The prospects for the study of individual structural units of this scientific direction are also concretized.

Keywords: cyberspace; criminal offense; direction; counteraction; investigation; technology.

ПРАВО УКРАЇНИ • 2021 • № 8 • 131-141