МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ «ОДЕСЬКА ЮРИДИЧНА АКАДЕМІЯ»

Самойленко Олена Анатоліївна

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Монографія

За редакцією доктора юридичних наук, професора А.Ф. Волобуєва

Одеса
ТЕС
2020

УДК 343.346.8:004
С178

Рецензенти:

Шепітько Валерій Юрійович, доктор юридичних наук, професор, академік Національної академії правових наук України, завідувач кафедри криміналістики Національного юридичного університету імені Ярослава Мудрого;

Тіщенко Валерій Володимирович, доктор юридичних наук, професор, член-кореспондент Національної академії правових наук України, завідувач кафедри криміналістики Національного університету «Одеська юридична академія»;

Чорноус Юлія Миколаївна, доктор юридичних наук, професор, професор кафедри криміналістики та судової медицини Національної академії внутрішніх справ

Рекомендовано до друку Вченою радою Національного університету «Одеська юридична академія» від 26 грудня 2019 року (протокол № 3)

Самойленко О. А.

С178 Основи методики розслідування злочинів, вчинених у кіберпросторі [Текст] : монографія / О. А. Самойленко; за заг. ред. А. Ф. Волобуєва. – Одеса :ТЕС, 2020. – 372 с.

У монографії висвітлено основи методики розслідування злочинів, вчинених у кіберпросторі. Розглянуто елементи криміналістичної характеристики злочинів, що зумовлені специфікою кіберпростору як обстановки злочину. Увагу акцентовано на проблемних аспектах початку кримінального провадження, визначено специфіку використання спеціальних знань підчас розслідування злочинів, вчинених у кіберпросторі, типізовано слідчі ситуації й тактичні операції їх розслідування.

Монографія призначена для практичних працівників правоохоронних органів (оперативних і слідчих підрозділів), практиків-юристів, науковців, викладачів, здобувачів закладів вищої освіти.

УДК 343.346.8:004

ISBN 978-617-7711-57-4

ЗМІСТ

ПЕРЕДМОВА

Стратегія розвитку інформаційного суспільства в Україні передбачає гармонізацію національного рівня його розвитку із загальносвітовим до 2020 року шляхом реалізації комплексу напрямів інтеграції національного і всесвітнього інформаційного простору[1]. Водночас для повноправного користування благами інформаційного суспільства Україна повинна бути готова й до негативних наслідків його розвитку – змін традиційних механізмів вчинення кримінальних правопорушень. У діяльності злочинців усе частіше спостерігається отримання, опрацювання та створення інформації, яка виконує роль предмета посягання чи інструмента злочинної діяльності в інформаційному середовищі, яке отримало назву кіберпростору.

Наразі в кіберпросторі вчиняються посягання на різноманітні правовідносини: від сфери національної безпеки до відносин власності. Механізм і динаміка таких злочинів вказують на те, що правоохоронні органи і суди зіштовхуються зі значними труднощами в проведенні їх розслідування. Згідно даних Департаменту організаційно-аналітичного забезпечення Національної поліції України щодо злочинів, вчинених з використанням високих інформаційних технологій, у 2014 р. у провадженні знаходилося 4883 матеріали (справи), у 2015 р. – 6026, у 2016 р. – 6219, у 2017 р. – 10 872, у 2018 р. – 11 131. Але на тлі загального зростання рівня кіберзлочинності показник розкриття таких злочинів має тенденцію до зниження: у 2014 р. слідчі Національної поліції України склали 797 обвинувальних актів; у 2015 р. – 756; у 2016 р. – 453; у 2017 р. – 764; у 2018 р. – 666. Видається, що така тенденція свідчить про недостатню готовність правоохоронних органів протидіяти не лише проявам кіберзлочинності, але й традиційній «технологічно оновленій» злочинності. Таким чином, враховуючи, що при вчиненні різних злочинів все активніше використовуються інформаційні технології та обстановка кіберпростору, наявною є потреба у розробленні

[1] Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки : Закон України від 9 січ. 2007 р. № 537-V. URL: https://zakon.rada.gov.ua/laws/show/537-16; Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 трав. 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80

відповідної методики їх розслідування, яка б передбачала застосування єдиних методів, засобів і прийомів вирішення типових завдань розслідування.

Проблеми виявлення та розслідування злочинів, вчинених у кіберпросторі, досліджували в своїх роботах вітчизняні науковці: П. Д. Біленчук, А. С. Білоусов, В. М. Бутузов, С. А. Буяджи, А. Ф. Волобуєв, І. О. Воронов, В. Д. Гавловський, В. О. Голубєв, М. В. Гуцалюк, Д. В. Дубов, С. В. Демедюк, М. В. Карчевський, О. І. Котляревський, М. О. Кравцова, О. М. Лепеха, М. Ю. Літвінов, О. В. Манжай, В. В. Марков, А. І. Марущак, О. І. Мотлях, І. М. Осика, Л. П. Паламарчук, Д. В. Пашнєв, А. В. Реуцький, С. М. Рогозін, Б. В. Романюк, М. В. Салтевський, С. В. Самойлов, Є. Д. Скулиш, К. В. Тітуніна, Д. М. Цехан, В. С. Цимбалюк, І. Ф. Хараберюш, В. Г. Хахановський, В. П. Шеломенцев, В. В. Чернєй, С. С. Чернявський, а також іноземні спеціалісти (В. Б. Вехов, Р. І. Дрімлюга, Д. А. Іллюшин, В. Є. Козлов, С. В. Кригін, В. В. Крилов, О. М. Лепехін, А. Л. Осипенко та інші). Констатуючи значний внесок вчених у розробку зазначеної проблематики, слід відзначити, що вони зосереджували увагу переважно на окремих видах кіберзлочинності, а наразі достатньо чітко постала проблема розроблення та застосування єдиних методів, засобів і прийомів вирішення типових завдань розслідування всіх злочинів у кіберпросторі. При цьому потрібно врахувати й оновлення кримінального процесуального законодавства останніх років і трансформації системи правоохоронних органів, їх підрозділів та компетенцій, що й зумовлює актуальність представленого монографічного дослідження.

Методологічним підґрунтям для розроблення методики розслідування злочинів, вчинених у кіберпросторі, стали теоретичні напрацювання провідних фахівців у галузі криміналістики (Ю. П. Аленіна, Л. І. Аркуші, В. П. Бахіна, Р. С. Бєлкіна, Г. П. Власової, І. О. Возгріна, А. Ф. Волобуєва, В. І. Галагана, Ю. П. Гармаєва, Л. Я. Драпкіна, М. В. Даньшина, В. А. Журавля, Н. С. Карпова, І. І. Когутича, В. О. Коновалової, А. М. Кустова, О. Ф. Лубіна, В. В. Лисенка, В. Г. Лукашевича, Є. Д. Лук'янчикова, Г. А. Матусовського, В. О. Мещерякова, Д. Й. Нікіфорчука, В. Т. Нора, О. В. Одерія, М. В. Салтевського, М. О. Селіванова, Д. Б. Сергєєвої, В. В. Тіщенка, П. В. Цимбала, В. Ю. Шепітька, А. В. Шмоніна, М. Г. Щербаковського, Б. В. Щура, М. П. Яблокова), кримінального процесу (Л. М. Лобойка, О. Р. Михайленка, М. М. Михеєнко,

О. Ю. Татарова, Л. Д. Удалової, М. І. Хавронюка, Ю. М. Чорноус), оперативно-розшукової діяльності (В. І. Гончаренка, М. Л. Грібова, В. П. Захарова, С. С. Кудінова, А. В. Мовчана, М. А. Погорецького, О. О. Подобного, В. В. Шендрика) та інших юридичних наук (Р. А. Калюжного, Б. А. Кормича, А. Л. Осипенка, А. В. Савченка).

Сучасне монографічне дослідження методики розслідування злочинів, вчинених у кіберпросторі, буде корисним як для теоретиків під час сучасних наукових розробок окремих криміналістичних методик, так і для практичних працівників правоохоронних органів, насамперед – оперативних та слідчих підрозділів. Воно сприятиме розв'язанню практичних проблем планування й організації розслідування кримінального провадження щодо злочину, елементи механізму вчинення якого зумовлені специфікою кіберпростору, його інформаційною сутністю.

Автор висловлює щиру подяку за допомогу та підтримку науковому консультанту – доктору юридичних наук, професору А. Ф. Волобуєву, рецензентам й усім, хто долучився до підготовки та видання цієї монографії.

Під час написання роботи було використано матеріали Національної поліції України (Департаменту кіберполіції, Головного слідчого управління, Департаменту організаційно-аналітичного забезпечення), Генеральної прокуратури України та прокуратур окремих областей. Автор висловлює вдячність практичним працівникам підрозділів цих правоохоронних органів за сприяння в збиранні емпіричного матеріалу, а також читачам за майбутні відгуки, зауваження та пропозиції.

СПИСОК УМОВНИХ ПОЗНАЧЕНЬ

АКБ – Акціонерний комерційний банк

АС – автоматична система

ГП – Генеральна прокуратура України

ГСУ – Головне слідче управління

Держспецзв'язок – Державна служба спеціального зв'язку та захисту інформації України

ДКІБ – Департаменту контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України

ДКП – Департамент кіберполіції Національної поліції України

ДНДЕКЦ – Державного науково-дослідного експертно-криміналістичний центр Міністерства внутрішніх справ України

ДФС – Державна фіскальна служба України

ЕОМ – електронно-обчислювальна машина

ЄРДР – Єдиний реєстр досудових розслідувань

ІСТЕ – Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України

КБ – Комерційний банк

КК – Кримінальний кодекс України (ред. 2001р.)

КПК – Кримінальний процесуальний кодекс України (ред. 2012 р.)

КТЕ – комп'ютерно-технічна експертиза

МВС – Міністерство внутрішніх справ України

НКРЗІ – Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації

НП – Національна поліція України

НС(Р)Д – негласна слідча (розшукова) дія

ОЗГ – організована злочинна група

ООН – Організація об'єднаних націй

ОРД – оперативно-розшукова діяльність

ОРЗ – оперативно-розшуковий захід

ПАТ – публічне акціонерне товариство

СБ – Служба безпеки України

США – Сполучені Штати Америки

ТЕД – технічна експертизи документів

ТОВ – товариство з обмеженою відповідальністю

РОЗДІЛ 1
КІБЕРПРОСТІР ТА ЗЛОЧИНИ ЯК ОБ'ЄКТ КРИМІНАЛІСТИЧНОГО ДОСЛІДЖЕННЯ

1.1. Особливості кіберпростору як об'єкта криміналістичного дослідження

Специфічні особливості злочинів, які вчиняються в кіберпросторі, обумовлені, перш за все, тією обстановкою, яка існує в названому середовищі. Такі злочини згідно Довідника № 9 до Положення про порядок ведення Єдиного реєстру досудових розслідувань реєструються в Україні, як «вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж»[1], тобто у їх найменуванні акцент робиться на засобах вчинення – інформаційних технологіях і телекомунікаційних мережах. Видається, що більш адекватним у цьому аспекті є використання терміну «кіберпростір», яким акцент робиться на середовищі вчинення злочинів, яке містить низку факторів, що обумовлюють як вибір способів злочинної діяльності, так і специфіку утворення її слідів. А відтак вони ж обумовлюють й особливості виявлення і розслідування таких злочинів.

У результаті узагальнення розгорнутих фабул кримінальних правопорушень, обліковуваних Національною поліцією України в період з 30 листопада 2012 року до 1 листопада 2018 року (без урахування закритих за пп. 1, 2, 4, 6 ч. 1 ст. 284 КПК України), що відповідно позначені в обліку як «вчинені з використанням високих інформаційних технологій і телекомунікаційних мереж», констатовано, що вони охоплювали види злочинних проявів, кваліфовані за такими статями КК України:

– ст. 176 (порушення авторського права і суміжних прав);

– ст. 185 (крадіжка);

– ст. 190, ч. 3, 4 (шахрайство);

[1] Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 6 квіт. 2016 р. № 139. URL: https://www.gp.gov.ua/ua/pd.html?_m=publications&_t=rec&id=110522.

– ст. 200 (незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення);

– ст. 229 (незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару);

– ст. 231 (незаконне збирання з метою використання або використання відомостей, що становлять комерційну чи банківську таємницю);

– ст. 301, ч. 3, 4, 5 (ввезення, виготовлення, збут і розповсюдження порнографічних предметів);

– ст. 361–363-1 (Розділ XVII «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж та мереж електрозв'язку»).

Будь-який процес злочинної діяльності, що передбачає використання кіберпростору, з плином часу технологічно ускладнюється. І це пов'язано не лише із закономірним удосконаленням комп'ютерних технологій. У криміналістичному аспекті це зумовлено підвищенням професійного рівня самого злочинця. Обравши певний профіль злочинної діяльності в кіберпросторі, злочинець, власне, отримує «дорожню карту» вдосконалення своєї діяльності. Соціальні мережі, форуми, чати та інші способи комунікацій у кіберпросторі разом із персональною здатністю до навчання таких злочинців дозволяють не лише систематично вчиняти злочин певного виду, а й ускладнювати механізм його вчинення, змінювати профіль злочинної діяльності, використовувати ту саму технологію злочинної діяльності для злочинів різної кримінально-правової кваліфікації, розробляти власну або запозичувати чиюсь технологію вчинення злочинів. Більшість науковців схиляється до думки, що серед таких кваліфікованих злочинців доцільно виокремлювати неординарну особу, котра опанувала технології розроблення програмних засобів, вільно аналізує чужі програми, здатна виявити в них прогалини – хакера[1]. Такий фахівець доволі нечасто

[1] Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М., 1996. С. 36; Рогозин В. Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук : 12.00.09. Волгоград, 1998. С. 13–14; Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посіб. Харків, 2000. С. 14.

потрапляє в коло уваги кримінального судочинства, оскільки для вчинення злочину використовує нетиповий, постійно вдосконалюваний, специфічний набір операцій у комп'ютерних мережах, часто діє в складі організованої групи, забезпечуючи якісно новий рівень злочинної діяльності останньої.

Саме зазначеним зумовлене сучасне реформування в Україні правоохоронних органів та створення підрозділів боротьби з кіберзлочинністю. На підставі Постанови Кабінету Міністрів «Про утворення територіального органу Національної поліції» від 13 жовтня 2015 року за № 831 створено Департамент кіберполіції. Наказом Національної поліції від 10 листопада 2015 року № 85 було затверджено Положення про Департамент кіберполіції Національної поліції України (ДКП НП України), проведено атестацію відповідних співробітників.

В результаті аналізу офіційних звітів про результати роботи ДКП НП України можна визнати, що підрозділи Департаменту беруть участь у розкритті фактів вчинення кримінальних правопорушень різноманітної кримінально-правової кваліфікації – як традиційних Інтернет-шахрайств, так і службових злочинів, незаконного поводження зі зброєю, бойовими припасами або вибуховими речовинами, доведення до самогубства, торгівлю наркотиками тощо. Так, наприклад, правоохоронці Запоріжжя розслідують доведення до самогубства жінки, яка вчинила суїцид після тривалого спілкування в одній з популярних соціальних мереж Інтернету з одним із користувачів. Родичка загиблої наголошує на тому, що до вчинення самогубства той підштовхував і її, детально описуючи, як зробити петлю на зашморзі. Коли йому не вдалося досягти своєї мети, зловмисник розповів, що за такі смерті отримує гроші. З лютого 2017 року в Києві проводиться розслідування щодо діяльності адміністраторів суїцидальних соціальних груп Інтернет-мережі за назвами «Синие киты» або «Розовые феи». Підозрювані, які є студентами одного з медичних університетів України, дають показання про те, що шляхом використання мережі експериментували зі свідомістю людей.[1]

[1] У Києві відпустили адміністраторів груп смерті. URL: https://tsn.ua/kyiv/u-kiyevi-vidpustili-administratoriv-grup-smerti-yaki-viyavilisya-studentami-medikami-zmi-887068.html.

Тож, не дивлячись на різну кримінально-правову кваліфікацію, злочини, вчинені у кіберпросторі, мають спільну і суттєву для розслідування ознаку – в механізмі їх вчинення як знаряддя використовується телекомунікаційна система, мережа та комп'ютерна інформація, а предметом можуть виступати об'єкти інтелектуальної власності, платіжні засоби, матеріальні цінності, об'єкти, нормальне функціонування яких безпосередньо забезпечується кібепростором.

Створення кіберпростору є новітнім досягнення людства, що змінило свідомість сучасної людини, яка вже не уявляє свого існування без задоволення своїх потреб через системи електронних платежів, продажу та придбання товарів через Інтернет, спілкування в соціальних мережах та інших сфер життя. На 15-тому Глобальному симпозіумі для регуляторних органів у м. Лібревіль у червні 2015 року професор Оксфордського інституту Інтернету І. Браун надав прогноз розвитку мережевих технологій: через стрімке падіння цін на різні датчики, обробку даних і комп'ютерну техніку до 2020 року до Інтернету буде підключено приблизно 20–50 мільярдів «речей», як-от: пристрої рухомого зв'язку, паркувальні лічильники, термостати, кардіомонітори, автопокришки, дороги, автомобілі, полиці супермаркетів, будинки і багато інших видів об'єктів і пристроїв[1]. Отже, кіберпростір не існує окремо від фізичного світу, заснованого на пересічних географічних категоріях. Усі дії, пов'язані з використаням кіберпростору, мають цілком реальні наслідки. Цей факт відповідним чином детермінував сучасну злочинність, яка пристосувалася до нової обстановки традиційних сфер життєдіяльності суспільства: дистанційного спілкування та освіти, електронних торгівлі, благодійності, комерції, інформаційних війн тощо. Можливості кіберпростору породжують нові та вдосконалюють наявні форми кримінальних правопорушень.

Таким чином, ***кіберпростір нині створює специфічну обстановку вчинення злочинів різних видів***, що безперечно зумовлює необхідність привернення уваги до нього в криміналістичних дослідженнях.

[1] Проблемы регулирования Интернета вещей: 15-й Глобальный симпозиум для регуляторных органов (Либревиль, 8–10 июня 2015 г.). *Itunews*. 2015. № 4. URL: https://itunews.itu.int/Ru/Note.aspx?Note=6060.

Обстановка є обов'язковим елементом криміналістичної характеристики злочинів, оскільки будь-який злочин вчиняється в умовах об'єктивної реальності, що справляють суттєвий вплив на поведінку злочинця і механізм слідоутворення[1]. Для криміналістів обстановка злочину – це система різного роду взаємодіючих між собою до вчинення злочину, в момент вчинення та після вчинення злочину об'єктів, явищ і процесів, які характеризують місце, час, речовинні, природно-кліматичні, виробничо-побутові та інші умови навколишнього середовища, особливості поведінки непрямих учасників протиправного діяння, психологічні зв'язки між ними та інші фактори об'єктивної реальності, що визначають можливість, умови та обставини вчинення злочину[2]. Таким навколишнім середовищем злочину постає кіберпростір. Аналогічну думку висловлювали й інші вітчизняні та закордонні науковці (В. А. Динту, С. П. Кушніренко, В. А. Мещеряков, Є. С. Шевченко)[3]. У закордонних публікаціях з проблем кіберзлочинності автори часто ототожнюють кіберпростір та обстановку вчинення злочину, використовуючи англійський вислів «crime scene cyberspace»[4], що дослівно перекладається як «обстановка кіберпростору» або «кіберпростір як місце злочину».

Втім в Україні через недосконалість термінологічного блоку чинної правової бази досі відсутнє чітке визначення науково-правового поняття «кіберпростір». У літературі юридичного спрямування в значенні такого використовують також інші терміни

---

[1] Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса, 2014. С. 3.

[2] Криминалистика / под ред. Н. П. Яблокова, В. Я. Колдина. М., 1990. С. 329.

[3] Шевченко Е. С., Михайлюченко Н. Н. Киберпространство как элемент обстановки совершения преступлений. *Академический юридический журнал*. 2015. № 1. С. 52-59; Динту В. А. Місце кіберпростору в системі обстановки злочину. *Науковий вісник Херсонського державного університету*. 2016. Вип. 2. Т. 3. С. 72-75; Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. 407 с.; Осипенко А. Л. Информационное пространство глобальных сетей как объект криминологичского изучения. *Современное право*. 2009. № 5. С.110-114.

[4] Crime scene cyberspace. *Globe*. 2012. No. 3. Sept. URL: https://www1.ethz.ch/zisc/events/ETHglobe_ZISC_SEP2012.pdf.

(віртуальне, інформаційне або Інтернет-середовище). Водночас у практиці слідчої діяльності останнім часом найбільшого поширення набувають терміни саме з префіксом «кібер», наприклад: кіберзлочинність, кіберполіція, кібербезпека, кіберпростір. У англійській мові «cyber» також не є самостійною лексемою – це префікс, який змінює лексичне значення слова.

Поняття кіберпростору (англ. c*yberspace)* вперше запровадив Вільям Гібсон у п'єсі «Le Neuromancer». У 1984 році письменник-фантаст назвав кіберпростір місцем, що поєднує всю наявну у світі інформацію, яку може відвідувати безтілесна свідомість[1]. Власне, йдеться про «всесвітню павутину» мережі Інтернет. Але трактування кіберпростору В. Гібсоном ще не вповні відповідає дійсності. Адже у світі величезна кількість локальних комп'ютерних мереж закритого типу, доступ до яких дозволений лише конкретним користувачам.

На нашу думку, досліджуючи термін «кіберпростір», доречно звернутися до кібернетики. Засновники цієї науки А.-М. Ампер та Б. Трентовський визначали її з філософських позицій – як теорію управління людьми[2]. Зрештою, лексема «кібернетика» походить від грецького «κοβερνω» – об'єкт управління, що містить людей (наприклад військова частина, корабель з командою та пасажирами). Від цього терміна існує багато похідних у різних мовах: англ. gouvernement – уряд; франц. governor – керуючий; рос. губернатор – представник державної влади[3]. Однак автори запропонували лише філософську концепцію управління, уникаючи положень щодо практичного застосування.

Кібернетику як теорію управління в живому та неживому світі розглядав Н. Вінер, праці якого спрямовані на найбільш «хворобливі» проблеми управління. Наприкінці 40-х років XX ст. вибухнула «криза надлишку інформації». Суспільство могло бути «задушене» інформацією, якби не сталося винайдення комп'ютера. Вінерівська ж кібернетика була орієнтована саме на інформаційні проблеми. Дослідник визнавав, що теорія інформації є основою цієї науки[4].

[1] Gibson W. Count Zero. An Ace Science Fiction Book. New York, 1986. URL: http://www.onread.com/fbreader/1414365/.

[2] Поваров Г. Н. Ампер и кибернетика. М., 1977. 95 с.

[3] Бранислав Трентовский и возникновеник кибернетики: из наследия Н. Н. Моисеева. *Экология и Жизнь*. 2007. № 8 (69). С. 15-19.

[4] Там само. С. 18.

Сучасна кібернетика є міжгалузевою наукою про загальні закономірності процесів управління й передавання інформації в машинах, живих організмах і суспільстві[1]. З огляду на це, кіберпростір дуже часто ототожнюють з інформаційним простором.

Аналіз праць з питань інформаційного права дає можливість стверджувати, що зміст терміна «інформаційний простір» є ширшим за «кіберпростір» та містить останній як визначальну складову[2]. Адже формування інформаційного суспільства є сучасною переважною тенденцією розвитку-впровадження людства в глобальний інформаційний простір на базі інформаційно-комп'ютерних технологій, Інтернету, засобів масової інформації тощо[3].

Правники, політологи неодноразово вдавалися до спроб надати визначення поняття «кіберпростір», але одностайності щодо сутності кіберпростору навіть у науках кримінального циклу досягти не вдалося[4]. Джон Барлоу – автор праці «Декларація незалежності кіберпростору» – зазначав, що електронний інформаційний простір має два рівні: 1) обмін інформацією у формі програмних кодів, який здебільшого й створює кіберпростір; 2) віртуальні життя, створювані внаслідок обміну інформацією між аватарами[5] (так традиційно називають користувачів мережі).

---

[1] Толковый словарь русского языка С. И. Ожегова. URL: http://slovariki.org/tolkovyj-clovar-ozegova/11579.

[2] Кормич Б. А. Інформаційне право : підручник. Харків, 2011. 334 с.; Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. Київ, 2007. 531 с.; Бачило И. Л. Информационное право: основы практической информатики : учеб. пособие. М., 2001. 352 с.

[3] Дюжев Д. В. Інформаційне суспільство: соціально-правова парадигма суспільного розвитку : автореф. дис. … канд. філос. наук : 09.00.03. Донецьк, 2004. 18 с.

[4] Білєнький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльно-правове дослідження) : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2016. 20 с.; Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ, 2014. 328 с.; April Mara, Norm Origin and Development in Cyberspace: Models Of Cybernorm Evolution. *Washington University Law Quarterly.* 2000. No. 78. P. 59–80; Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2000. С. 50-53.

[5] Barlow J. P. A Declaration of the Independence of Cyberspace. URL: https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

Тож, кіберпростір утворюється в результаті взаємодії між людьми шляхом обміну інформацією в електронній цифровій формі. Тому для розуміння сутності кіберпростору як специфічної обстановки вчинення кримінального правопорушення необхідно дослідити його подвійну природу: технічну та соціальну.

Технічна природа кіберпростору. Розвиток глобального електронного простору розпочався із замовлення Управління перспективних досліджень Міністерства оборони США у 1969 році на побудову мережі, здатної забезпечити обмін інформацією між користувачами за умов ядерної війни. Наприкінці 80-х років XX ст. мережа поєднувала комп'ютери не лише в США, а й по всьому світу, хоча інформація, що надходила каналами зв'язку, на екранах моніторів мала вигляд текстових символів. З 1992 року було задіяно так звану «WWW» (з англ. «word» – «світ», «wide» – «широко», «web» – «павутиння»), або «Всесвітню павутину», створену як інформаційну технологію Тімом Бернесом-Лі – фахівцем Європейського центру ядерних досліджень у м. Женева. Власне, це засіб доступу до інформаційних ресурсів Інтернет, тобто мережі пов'язаних між собою сторінок, що є веб-вузлами всього світу з гіпертекстовими посиланнями[1]. Таким чином, Тім Бернерс-Лі, запропонувавши протоколи передавання графічної інформації, започаткував розгалужену гіпермедіасистему *World Wide Web* (*WWW*)[2].

Закцентуймося на окремих термінах інформатики. Системоутворювальний комплекс засобів телекомунікацій, що надає територіально розгалуженим об'єктам можливість інформаційної взаємодії шляхом обміну сигналами (радіо, електричними або оптичними), називають телекомунікаційною мережею. Методи і способи накопичення, обробки, зберігання, відображення, пошуку й забезпечення цілісності інформації отримали назву інформаційних технологій. Автономні інформаційно-обчислювальні системи досить швидко трансформувалися в децентралізовані, призначені для розподіленої обробки інформації за допомогою комп'ютерів,

[1] Антонов В. М. Інтернет: енциклопедичне видання : навч.-метод. посіб. Київ, 2008. С. 75.

[2] Гуцалюк М. В. Проблеми протидії комп'ютерній злочинності в глобальній інформаційній мережі Internet. *Вісник Центру дослідження комп'ютерної злочинності*. 2005. № 4. URL: http://www.crime-research.org/library/Gucal.htm.

об'єднаних телекомунікаційною мережею, що, відповідно, мають назву «інформаційні мережі»[1]. У технічному сенсі мережа Інтернет становить глобальну сукупність інформаційних ресурсів і систем, з'єднаних за допомогою електрозв'язку, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів. Власники Інтернет-ресурсів мають змогу розміщувати власну інформацію або інформацію третіх осіб за допомогою різноманітних інформаційних технологій, а користувачі мають можливість одержувати цю інформацію різними методами, серед яких переважають доступ до інформаційних ресурсів (сайтів) у мережі Інтернет і використання електронної пошти[2].

Провідним органом у світі, що здійснює регулювання мережі Інтернет, є Internet Society (ISOC) – недержавна громадська організація, фінансовим базисом діяльності якої є внески учасників і пожертви спонсорів. ISOC проводить щорічні конференції (INET), випускає інформаційні матеріали (Internet Society News), забезпечує підтримку інформаційних серверів[3]. Також функціонують технічні комітети, що підтримують системи стандартів, на яких базується вся мережа. Створення й розвиток інформаційних ресурсів і систем у мережі Інтернет, а також поширення інформації відбуваються винятково в межах узгоджених міжнародних технічних стандартів і протоколів, чим зумовлена висока значущість технічних норм для регулювання зазначених відносин.

Інтернет є основним, але не єдиним засобом створення кіберпростору. З урахуванням комп'ютерної складової електронного обміну інформацією, *кіберпростір утворюють усі телекомунікаційні мережі, комп'ютерні системи й пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача*.

---

[1] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за заг. ред. С. О. Довгого. 2-ге вид., доповн. Київ, 2013. С. 33-36.

[2] Козьяков Д. Масова інформація в мережі Інтернет: правові аспекти. *Вісник Національної Академії прокуратури України*. 2010. № 1. С. 120-123.

[3] Андреев Б. В., Вагонова Е. А. Право и Интернет : учеб. пособие. М., 2001. С. 17.

У сучасній юридичній літературі широкого вжитку набув термін «віртуальний простір», який найчастіше використовують як синонім поняття «кіберпростір» та визначають як модельований за допомогою комп'ютера інформаційний простір, де містяться дані про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному чи будь-якому іншому вигляді, що перебувають у процесі руху локальними і глобальними комп'ютерними мережами, або ж це відомості, що зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою, а також іншого носія, спеціально призначеного для їх зберігання, обробки й передавання[1]. На нашу думку, таке трактування понять може спричинити плутанину під час досліджень у науках кримінально-правового циклу, зокрема щодо криміналістичних методик розслідування окремих видів злочинів, вчинених у кіберпросторі.

Етимологічно «віртуальний» походить від лат. virtus – римляни вживали його для позначення таких якостей воїна, як мужність, хоробрість, рішучість[2]. Віртуальність (від лат. virtus – потенційний, можливий) – вигаданий, уявний (можливо, з певною метою) об'єкт, суб'єкт, категорія, ставлення, дія тощо, відсутній на цей момент у реальному світі, а створений лише грою людської уяви або зімітований за допомогою інших об'єктів[3]. Застосуванню терміна «віртуальний» в комп'ютерній галузі сприяло його використання відносно об'єктів, яких не існує у фізичному світі, що не мають чіткої просторової форми.

Однак у науках кримінально-правового циклу в аспекті розроблення та вдосконалення засобів боротьби зі злочинністю кіберпростір не можна розглядати як віртуальний, адже злочинці, котрі використовують його для вчинення злочину, не можуть бути віртуальними. До того ж, інформація в електронній цифровій формі, що має криміналістичне значення, за своєю фізичною природою є доступною безпосередньому сприйняттю через використання програмно-технічних засобів. Унаслідок впливу (знищення,

[1] Кіпа О. Правопорушення в мережі Інтернет. *Часопис Київського університету права*. 2010. № 4. С. 346-349.

[2] Волинець В. О. Віртуальна реальність: поняття та сутність. *Питання культурології.* 2014. Вип. 30. С. 35-41.

[3] Глазычев В. Игры цивилизаций. *Век XX и мир.* 1994. № 11–12. С. 102-118.

модифікації, копіювання, блокування тощо) комп'ютерної інформації шляхом доступу до неї утворюються певні відомості, які в криміналістиці називають «нетрадиційними», або інформаційними слідами[1]. Їх можуть зберігати на матеріальному носії постачальники Інтернет-послуг (провайдери), користувачі. Для їх виявлення та вилучення необхідне застосування відповідних технічних засобів[2].

Сучасний користувач комп'ютерних мереж має можливість здійснювати різноманітні дії в модельованому комп'ютером електронному просторі в реальному часі (наприклад, під час комп'ютерних ігр у мережі, спілкування в соціальних мережах). Ці дії створюють так звану «віртуальну реальність» або «реальну вертуальність». Це система, в якій реальність як така (матеріальне або символічне існування людей) повністю занурена у віртуальні образи, вигаданий світ, у якому зображення не просто перебуває на екрані, через який передається досвід, але й саме стає досвідом[3]. У сучасних словниках поняття «віртуальна реальність» подано у вузькому й широкому сенсі[4]. У вузькому розумінні – це ті ігрові або необхідні в технічному плані «штучні реальності», які виникають унаслідок впливу комп'ютера на свідомість, коли, наприклад, на людину одягають «електронні окуляри» й «електронні рукавички». У широкому – це будь-які змінені стани свідомості, як-от: шизофренічні марення, наркотичне чи алкогольне сп'яніння, гіпнотичний стан, ігроманія. Шляхом використання різних комп'ютерних аудіовізуальних технологій людина може реалізовувати свою комунікативну функцію, контактувати не лише з іншими людьми, а й зі штучними персонажами, створеними іншими особами, з метою використання цих образів для

[1] Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя, 2003. 250 с.; Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. 328 с.

[2] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж, 2002. С. 74-76.

[3] Кормич Б. А. Інформаційне право : підручник. Харків, 2011. С. 22; Кастельс М. Информационная эпоха: экономика, общество, культура / пер. с англ. ; под науч. ред. О. И. Шкаратана. М., 2000. С. 351.

[4] Heim M., Helsel Ed. S. K., Roth J. P. The Metaphysics of Virtual Reality. *Virtual Reality: Theory, Practiceand Promise.* London, 1991. P. 27-33; Носов Н. А. Словарь виртуальных терминов. Труды лаборатории виртуалистики. *Труды Центра профориентации*. М., 2000. Вып. 7. 69 с.

подальшого вчинення злочину. Тож, віртуальність – це одна з ознак кіберпростору, особливість, яка приваблює злочинців для його використання в механізмі вчинення злочину.

Іншою особливістю функціонування кіберпростору є те, що Інтернет провайдери як головні суб'єкти глобальної мережі, що забезпечують доступ до інформації та надають відповідні послуги, не здатні контролювати весь обсяг розміщеної в Інтернеті інформації, оскільки фактично її може бути розміщено на комп'ютері – www-сервері, розташованому в будь-якій частині світу[1]. Зобов'язання щодо здійснення такого контролю має для суспільства як позитивні, так і негативні наслідки.

Так, з одного боку, визнання на державному рівні (у Російській Федерації, Китаї, Ірані та деяких інших країнах) суверенного права держави регулювати комунікаційні можливості в Інтернеті призводить до технічних помилок електронного зв'язку через надмірну обережність провайдерів. Також це зумовлює негативний ефект відносно загального права на свободу слова, спричиняючи певні обмеження.

З іншого боку, незабезпечення державою належної правової охорони відносин у кіберпросторі, неузгодженість чинних законів конкретної держави є обставинами, що приваблюють особу, котра має намір віддалено від себе (дистанційно) отримати реальний злочинний результат. Адже правоохоронні органи стикаються зі значними труднощами, коли під час розслідування вдається встановити факт перебування під юрисдикцією іншої держави телекомунікаційної мережі, використаної для вчинення злочину, або власника інформаційного продукту, якого необхідно захищати від протиправного посягання.

Зрештою, однією з особливостей кіберпростору як складної технічної системи є можливість користувачів здійснювати обмін інформацією в електронній цифровій формі. Такому обміну притаманна оперативність створення, поширення, модифікації або знищення інформації Саме тому в процесі вчинення окремих видів злочинів використання кіберпростору значно прискорює досягнення злочинної мети, а також сприяє якісному приховуванню фактів їх

[1] Городенко Л. Правові взаємини електронних видань та держави. *Наукові записки Інституту журналістики*. 2005. Т. 20. С. 11-17.

вчинення. Тому для ефективної боротьби зі злочинами, вчиненими у кіберпросторі, необхідно враховувати як особливості вчинення злочину певної кримінально-правової кваліфікації, так і можливості, які створює кіберпростір для їх вчинення, вплив останніх на методику розслідування окремих видів злочинів. У механізмі такої злочинної діяльності кіберпростір як обстановка злочину є передумовою більш ефективного та швидкого досягнення злочинного результату, порівняно з традиційною речовинною обстановкою вчинення злочину.

Соціальна природа кіберпростору. Згідно з першим законом технологій М. Крацберга, виведеним дослідником під час вивчення розвитку технологій та їх взаємодії з соціокультурними змінами, «сама по собі технологія є ні гарною, ні поганою, але й нейтральною її не назвеш»[1]. Дійсно, результати використання нових технологій залежать від мети суб'єкта їх застосування. Однак саме технології стають визначальним чинником у формуванні стилю життя, цінностей, інститутів та інших елементів сучасного суспільства. Тому, виникши як суто технічний спосіб передавання інформації, кіберпростір перетворився на важливе соціальне явище, пов'язане з комунікаційною складовою Інтернет-технологій.

Комунікаційні технології кіберпростору (електронна пошта, скайп, чати, форуми, вебінари, відеоконференції, соціальні мережі) слугують для формування взаємозв'язків зі значними масами населення, впливу на них або взаємодії з ними, інформаційного захоплення чи тиражування інформаційного продукту[2]. Користувачі можуть здійснювати один з двох типів доступу до інформаційного простору: а) *on line* доступ, що дозволяє використовувати мережу в режимі реального часу; б) *off line* доступ – коли підготовка завдання для мережі відбувається заздалегідь, а з'єднання необхідне лише для передавання чи прийому підготовлених даних.

Учасники комунікації в кіберпросторі взаємодіють між собою з певною мотивацією: діловою (отримання або надання послуг, ведення бізнесу); комунікаційною (спілкування з однодумцями, участь у

[1] James R. Hansen Technology and the History of Aeronautics: An Essay. URL: http://www.centennialofflight.net/essay/Evolution_of_Technology/Tech-OV1.htm.

[2] Остапенко Г. Комунікація та комунікативна активність суспільства в добу Інтернет-технологій: соціальний аспект. *Вісник Книжкової палати*. 2013. № 9. С. 48.

визначеній загальними інтересами спільноті); пізнавальною (отримання освіти); розважальною (інтерактивні ігри, перегляд телебачення) тощо. Тож, кіберпростір слугує альтернативою реальному матеріальному світові. Своєю чергою, користувачі мережі є учасниками суспільних відносин, що набули поширення в сучасному інформаційному суспільстві, утворили визначені за певним критерієм соціальні групи.

Існує безліч визначень поняття «соціальна група», проте всі соціологи впевнені в тому, що такою групою можна назвати визначену кількість людей, яка відрізняється від інших за характерними соціальними ознаками[1]. У межах кіберпростору діє аналог соціальної групи, так звана «соціальна мережа» – Інтернет-співтовариство користувачів, об'єднаних за будь-якою ознакою на базі одного сайту[2]. Головним чинником об'єднання користувачів у соціальну мережу також є певна актуальна на окремий момент спільна ознака – фінансове становище, стать, приналежність до тієї чи іншої раси, національності, мовної групи, віросповідання, професії або ж інтереси (спорт, ігри, інші зацікавленості) тощо. Група в соціальній мережі кіберпростору відрізняється від звичайної соціальної групи неважливістю такого критерію, як просторова близькість її учасників, та здатністю постійно перебувати в комунікаційному процесі (що забезпечують технології *on line* доступу).

Нині соціальні мережі створили безмежні можливості для об'єднання віддалених одна від одної (часто безпосередньо не знайомих) осіб з метою спільної злочинної діяльності – у кримінологічному сенсі, для ефективної діяльності утворених організованих злочинних угруповань – у кримінальному. Адже скоєння терористичних актів, незаконний обіг наркотичних засобів, поширення порнографії; піратства та інших транснаціональних злочинів потребує технічного, матеріального й організаційного супроводження, що повною мірою забезпечують можливості кіберпростору. Тому організована злочинність активно використовує обстановку кіберпростіру для досягнення злочинної мети.

Зрештою, такі соціальні мережі стали величезним структурованим масивом відомостей про реальне життя конкретної

[1] Герасимчук А. А., Палеха Ю. І., Шиян О. М. Соціологія : навч. посіб. 4-те вид., випр. і доповн. Київ, 2004. 246 с.

[2] SEO Словник : соц. мережа. URL: http://igroup.com.ua/seo-articles/sotsialna-merezha.

людини, її вподобання, пересування, коло спілкування, робочі функції тощо. За необхідності цю базу може бути вміло використано для вчинення злочину проти неї.

З огляду на зазначене, ***кіберпростір*** слід розуміти як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій, що вміщує Інтернет, інші телекомунікаційні мережі, комп'ютерні системи та пристрої, обмін інформацією в яких здійснюється на базі єдиної системи стандартів і протоколів, що забезпечують процес перетворення вихідної інформації на інформаційний продукт для іншого користувача. Проведений нами вище аналіз використання кіберпростору зі злочинною метою, узагальнення матеріалів судово-слідчої практики дозволяють визначити певні *особливості кіберпростору,* які злочинець використовує з метою досягнення злочинного результату:

1) віддаленість (дистанційність) доступу до предмета посягання з використанням кіберпростору, що забезпечує транскордонну складову такої злочинної діяльності, яка викликає необхідність вирішення слідчим питань територіальної юрисдикції;

2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі, що є предметом злочинного посягання або слідом злочину – це сприяє значному прискоренню та якісному приховуванню злочинної діяльності;

3) віртуальність, що забезпечує відносну конфіденційність інформації про особу злочинця та можливість упливати на свідомість певної категорії осіб;

4) комунікативність, яка уможливлює створення злочинних груп та ефективну діяльність уже наявної організованої злочинності;

5) недосконаліть забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що надає злочинцю можливість уникати кримінальної відповідальності за вчинений злочин.

З урахуванням технічної та соціальної складової такого змісту кіберпростору, останній накладає суттєвий відбиток на механізм цього правопорушення. В цьому аспекті кіберпростір в криміналістичних дослідженнях може розглядатися як:

а) середовище (обстановка), в якому окремі його елементи (телекомунікаційна мережа, комп'ютерна інформація тощо) могли 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, в яку були внесені зміни в результаті правопорушення (його сліди), які можуть виступати джерелами доказів у кримінальному провадженні.

Використана для досягнення злочинного результату обстановка кіберпростору, маючи притаманні лише їй подвійні чинники технічної та соціальної природи, зумовлює необхідність застосування оновлених методів, засобів і прийомів вирішення практичних завдань розслідування такої злочинної діяльності

1.2. Правові основи боротьби зі злочинами, що вчиняються в кіберпросторі

Кіберпростір, як і будь-яке соціальне середовище, використовуване зі злочинною метою, неможливо уявити без чинників регуляторного характеру. Основним засобом регулювання тих чи інших суспільних відносин суб'єктів кіберпростору постає відповідне право: інформаційні відносини підлягають регулюванню інформаційним правом; відносини з приводу інтелектуальної власності – інтелектуальним правом; майнові та особисті немайнові відносини – цивільним, господарським правом; відносини, що виникають унаслідок вчинення злочину та відкриття відповідного кримінального провадження – кримінальним правом та кримінальним процесуальним правом.

Відправним пунктом для розуміння правових засад у сфері боротьби зі злочинами, вчиненими в обстановці кіберпростору, є норми міжнародного права, імплементовані у внутрішнє законодавство України з міжнародних договорів, учасницею яких вона є. Зокрема, це стосується численних багатосторонніх і двосторонніх угод, універсальних, регіональних та локальних договорів із питань боротьби зі злочинами у кіберпросторі. Тому з метою з'ясування сутності злочинів, вчинених у кіберпросторі, вважаємо за доцільне розглядати питання нормативно-правового регулювання сфери боротьби з такими злочинами через призму кореляції відповідного міжнародного та національного законодавства.

Системоутворювальним для України міжнародним актом у сфері боротьби зі злочинами, вчиненими у кіберпросторі, можна вважати прийняту європейськими державами в м. Будапешт 23 листопада 2001 року Конвенцію Ради Європи про кіберзлочинність, до якої Україна приєдналася із застереженнями шляхом ратифікації 7 вересня 2005 року[1].

Ця Конвенція, власне, стала визначальним моментом установлення сучасного світового правопорядку та співробітництва у сфері боротьби зі злочинами такого виду, адже станом на листопад 2017 року була ратифікована 58 державами, серед яких усі держави-члени Ради Європи (за винятком Російської Федерації) й такі, що не входять до європейської спільноти, зокрема Канада, Ізраїль, США, Японія та країни південної Америки[2]. Конвенція про кіберзлочинність – це договір, згідно з яким держави, що до неї приєдналися, узяли на себе зобов'язання відносно зближення між собою внутрішньодержавних положень кримінального права щодо кіберзлочинів та створення можливостей для застосування ефективних засобів розслідування таких правопорушень. Тому Конвенцією прямо передбачено заходи, що мають здійснюватися на національному рівні в матеріальному кримінальному праві (ч.1 розділ 2) й кримінально-процесуальному (так званому «процедурному») праві (ч. 2 розділ 2), а також систему міжнародного співробітництва (розділ 3) та питання юрисдикційного характеру (ч. 3 розділ 2)[3].

Зі змісту міжнародного акту можна зрозуміти, що автори Конвенції, розробляючи її, виходили з необхідності уніфікування національних кримінальних законів, що надасть змогу не просто декларувати у світовій спільноті боротьбу зі злочинами, вчиненими у кіберпросторі, а й уможливить реальне міжнародне переслідування злочинців та розслідування кіберзлочинів. Підтвердженням того є

[1] Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV. URL: http://zakon3.rada.gov.ua/laws/show/2824-15.

[2] Таблица подписей и ратификации договора Совета Европы № 185 «Convention on Cybercrime». URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dfS8PM6Z.

[3] Конвенція про кіберзлочинність : міжнар. док. від 23 лисопт. 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11.

докладний розподіл у Конвенції (з урахуванням прийнятого до неї 2003 року додаткового Протоколу) кіберзлочинів на п'ять груп, зокрема:

1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем: незаконний доступ (ст. 2); незаконне перехоплення (ст. 3); втручання в дані (ст. 4); втручання в систему (ст. 5); зловживання пристроями (ст. 6);

2) правопорушення, пов'язані з комп'ютерами: підробка, пов'язана з комп'ютерами (ст. 7); шахрайство, пов'язане з комп'ютерами (ст. 8);

3) правопорушення, пов'язані зі змістом: правопорушення, пов'язані з дитячою порнографією (ст. 9);

4) правопорушення, пов'язані з порушенням авторських і суміжних прав; ст. 10 Конвенції містить детальне роз'яснення, які саме дії з розповсюдження дитячої порнографії підлягають переслідуванню, зокрема: виробництво дитячої порнографічної продукції з метою поширення через комп'ютерну систему; пропозиція або надання в користування дитячої порнографії через комп'ютерну систему; розповсюдження або передача дитячої порнографії через комп'ютерну систему; придбання дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією, що міститься в комп'ютерній системі або на носіях комп'ютерних даних;

5) дії расистського та ксенофобного характеру, вчинені через комп'ютерні системи (Додатковий протокол до Конвенції[1]): поширення расистського та ксенофобного матеріалу через комп'ютерні системи (ст. 3); погроза з расистських і ксенофобних мотивів (ст. 4); образа з расистських і ксенофобних мотивів (ст. 5); заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства (ст. 6); пособництво та підбурювання (ст. 7).

Утім, незважаючи на докладний опис на міжрегіональному рівні конкретних складів кіберзлочинів, сутність та перелік правопорушень, пов'язаних із обстановкою кіберпростору, в національних правових системах різняться. Не становить винятку й Україна, що вимагає зіставлення відповідних норм Конвенції з чинними нормами КК України.

[1] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 лип. 2006 р. № 23-V. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687.

По-перше, з огляду на те, що Конвенцію було ратифіковано із застереженнями, Україна залишила за собою право не визнавати кримінально караними окремі конвенційні види злочинів, що стосуються таких діянь:

1) виготовлення, придбання для використання, надання для використання іншим чином пристроїв, включаючи комп'ютерні програми, створених або адаптованих, з метою вчинення будь-якого зі злочинів проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (ст. 6);

2) виготовлення і придбання для використання комп'ютерних паролів, кодів доступу чи аналогічних даних, за допомогою яких можна отримати доступ до всієї або частини комп'ютерної системи (ст. 6);

3) здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи; володіння дитячою порнографією в комп'ютерній системі чи на комп'ютерному носії інформації (п. d, e, ч. 1 ст. 9)[1].

З часом у ст. 361-1 КК України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут» було частково втілено норму ст. 6 Конвенції щодо зловживання пристроями в частині розповсюдження або збуту шкідливих програмних чи технічних засобів. При цьому п. d, e, ч. 1 ст. 9 Конвенції щодо криміналізації здобуття дитячої порнографії за допомогою комп'ютерних систем для себе чи іншої особи або володіння нею в комп'ютерній системі чи на комп'ютерному носії інформації досі залишається неімплементованими у національні кримінально-правові норми.

По-друге, за змістом Конвенції, усі інші запропоновані нею склади кримінальних правопорушень утілено в КК України з урахуванням особливостей національної кримінальної політики.

Так, окрема частка правопорушень, визначених у Конвенції, набула закріплення в спеціальних нормах, які об'єднано в Розділі XVI «Злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». В ст. 361 КК України «Несанкціоноване втручання в роботу ЕОМ (комп'ютерів),

[1] Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824- IV. URL: http://zakon3.rada.gov.ua/laws/show/2824-15.

автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку»[1] криміналізовано більшість конвенційних правопорушень проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, зокрема: незаконний доступ (ст. 2); незаконне перехоплення (ст. 3); втручання в дані (ст. 4); втручання в систему (ст. 5). Варто уваги, що, попри термінологічну розбіжність у формулюванні зазначених національної та міжнародної норм, їх семантичний зміст повністю ідентичний. Відмінність у тому, що автори Конвенції у формулюванні об'єктивної сторони складів правопорушень акцентують на процесі вчинення злочину, а вітчизняний законодавець – на його наслідках, прописуючи в диспозиції певний злочинний результат, як-от: «призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації».

Іншу ж кількість конвенційних правопорушень зафіксовано в статтях КК України, якими регламентовано використання для вчинення злочину електронно-обчислювальної техніки, мереж, систем, інших апаратних та програмних засобів, а саме як *елемент об'єктивної сторони* (ст. 200 КК України – незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима; ст. 176 – порушення авторського права і суміжних прав; ст. 300 – ввезення, виготовлення або розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію), як *кваліфікуюча ознака* (ч. 3 ст. 190 – шахрайство із використанням електронно-обчислювальної техніки; ч. 4 ст. 301 – ввезення, виготовлення, збут і розповсюдження порнографічних предметів у частині щодо творів, зображень або інших предметів порнографічного характеру, що містять дитячу порнографію).

У цьому контексті акцентуємо, що передбачені Додатковим протоколом до Конвенції[2] дії расистського та ксенофобного

[1] Кримінальний Кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: http://zakon2.rada.gov.ua/laws/show/2341-14.

[2] Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 лип. 2006 р. № 23-V. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687.

характеру, вчинені через комп'ютерні системи, не визначено в КК України з прямою вказівкою на використання для їх вчинення кіберпростору. Причому щодо злочинів расистського та ксенофобного характеру передбачено склади досить широкої інтерпретації об'єктивної сторони, зокрема: ст. 161 – порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками; ч. 2 ст. 129 – погроза вбивством у частині вчинення цього з мотивів расової, національної та релігійної нетерпимості; ч. 2 ст. 442 – геноцид у частині публічних закликів до геноциду, а також виготовлення матеріалів із закликами до нього з метою їх розповсюдження або розповсюдження таких матеріалів. Це дозволяє констатувати наявність криміналізації зазначеної групи конвенційних кіберзлочинів у національному законодавстві.

По-третє, КК України містить кримінальні правопорушення, що є альтернативними правопорушенням, визнаним Конвенцією про кіберзлочинність, тобто вчинювані у кіберпросторі, але в цьому міжнародному акті про них взагалі не йдеться. До таких спеціальних норм відносимо такі правопорушення, визначені в розділі XVI КК України:

– несанкціоновані дії з інформацією, обробка якої відбувається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, котра має право доступу до неї (ст. 362);

– порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, оброблюваної в них, яких припустилася особа, відповідальна за їх експлуатацію, якщо цим заподіяно значної шкоди (ст. 363);

– перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1).

Диспозиція окремих статей КК України дозволяє виокремити й інші альтернативні Конвенції склади злочинів, для вчинення яких використовують обстановку кіберпростору, зокрема: порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через

комп'ютер (ст. 163); зайняття гральним бізнесом (ст. 203-2); розголошення комерційної або банківської таємниці (ст. 232); незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376); пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436, 436-1); незаконне придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів (ст. 307, 311); публічні заклики до вчинення терористичного акту (ст. 258-2); злочини у сфері охорони державної таємниці (ст. 328, 330).

На підставі наведених вище позицій та за об'єктивного впливу фактору часу можна погодитися з тими науковцями, які наголошують на недосконалості самої Конвенції про кіберзлочинність[1].

Так, Конвенцією ООН проти транснаціональної організованої злочинності державам рекомендовано криміналізацію злочинів проти принципів суверенної рівності й територіальної цілісності держав, а також принципу невтручання у внутрішні справи інших держав, відмивання доходів від злочинів, участі в організованій злочинній групі, корупції, перешкоджання здійсненню правосуддя, вчинених за таких умов: 1) у більш ніж одній державі; 2) в одній державі, але істотний етап підготовки, планування, керівництва або контролю відбувається в іншій державі; 3) в одній державі, але за участю організованої злочинної групи, яка здійснює злочинну діяльність у більш ніж одній державі; 4) в одній державі, але істотні наслідки відбуваються в іншій державі. У п. 29 цієї Конвенції наведено про програми підготовки персоналу правоохоронних органів у аспекті «методів, використовуваних у боротьбі з транснаціональними організованими злочинами, які вчиняються з використанням комп'ютерів, телекомунікаційних мереж та інших видів сучасних технологій»[2]. Наприклад, з появою технології криптографічних валют

[1] Хахановський В. Кіберзлочинність: застосування сучасних технологій при вчиненні злочинів – проблеми досудового розслідування та міжнародної співпраці. *Правова інформатика.* 2007. № 1 (13). С. 68–73; Столяр О. Міжнародно-правові проблеми визначення та класифікації кіберзлочинів. *Национальный юридический журнал* (науч.-практ. правов. изд-во Респ. Молдова). 2017. IULIE. С. 185-188.

[2] Конвенції ООН проти транснаціональної організованої злочинності : міжнар. док. від 15 листоп. 2000 р. URL: http://zakon3.rada.gov.ua/laws/show/995_789.

(так званих електронних грошей), створення та обіг яких базується на методах криптографічного захисту інформації, корупційні дії, відмивання доходів від злочинів шляхом застосування таких взаєморозрахунків стали невідслідковуваними для правоохоронних органів. Адже в процесі обігу таких валют не існує єдиного керівного суб'єкта, ця технологія дозволяє зберігати інформацію про обіг валюти розокремлено на комп'ютерах у всьому світі[1]. Це лише один з прикладів можливостей, які надає кіберпростір для вчинення зазначених злочинів. Тому в Конвенції про кіберзлочинність було би доцільним зазначити про використання технологій кіберпростору для вчинення публічних закликів чи розповсюдження матеріалів із закликами щодо посягання на територіальну цілісність і недоторканність держави; фінансування дій, вчинених з метою насильницького змінення чи повалення конституційного ладу або захоплення державної влади, змінення меж території або державного кордону; державної зради; диверсії; шпигунства; легалізації доходів від злочину та інших транснаціональних організованих видів кримінальних правопорушень.

На окрему увагу заслуговує питання відносно можливості використання кіберпростору для вчинення терористичного акту та інших злочинів, що пов'язані з ним, щодо відповідного віднесення універсальним міжнародним актом наведених правопорушень до категорії кіберзлочинів. Кібертероризм як явище та способи протидії йому стали предметом дослідження багатьох науковців (В. М. Бутузова, С. Б. Гавриша, С. О. Гнатюка, В. А. Голубєва, Д. В. Дубова, О. Г. Корченко, В. А. Ліпкана, В. П. Шеломенцева, С. Хилдрета й ін.). Утім проблеми боротьби з кібертероризмом у міжнародному законодавчому полі відображено лише у вигляді проектів актів або локальних, двосторонніх міжнародних договорів з питань процедурного права. Країни Європейського Союзу обговорюють міжрегіональний проект Clean IT, метою якого є організація оперативного реагування у разі виникнення загрози акту кібернетичного тероризму[2]. В Україні цю сферу боротьби з тероризмом зачіпають двосторонні договори, укладені з

[1]Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение. *Наука, техника, образование.* 2017. № 32. С. 61-64.

[2] Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications. 2012. 21 sep. URL: https://edri.org/cleanit.

США, Республікою Словенія, Чорногорією, Королівством Бельгія, Королівством Нідерланди.

Аналогічна проблема стосується не регламентованих окремо як злочини в Конвенції про кіберзлочинність крадіжки, передавання та використання персональних даних. Одні країни виокремлюють злочини такого виду як самостійну категорію, інші вважають, що ці діяння підпадають під кілька статей кримінального законодавства[1]. На думку К. С. Шахбазян, поширення інформації комп'ютерними мережами може спричинити як масові порушення прав людини (наприклад, пропаганда геноциду, поширення ідеї расової нерівності), так і неповагу до прав окремих осіб. Тому поширення інформації комп'ютерними мережами, що спричиняє масові порушення прав людини, можливо розглядати як міжнародний злочин, що має наслідком виникнення міжнародно-правової відповідальності держав та індивідів[2]. У кримінально-правовій сфері України це питання є вельми актуальним.

Тож у результаті окремого й порівняльного аналізу положень Конвенції про кіберзлочинність та українського кримінально-правового законодавства ми дійшли висновку, що, зрештою, більшість конвенційних кіберзлочинів в Україні є криміналізованими. Імплементаційний процес положень Конвенції у кримінальне законодавство України досі триває.

Водночас процес правового регулювання у сфері боротьби зі злочинами, вчиненими у кіберпросторі, характеризується певними чинниками.

Перший чинник полягає в тому, що національна кримінально-правова охорона тих чи інших прав і свобод людини залежить від наявності суспільної потреби в цьому. Так, наприклад, в Україні переведення коштів із банківських рахунків клієнтів банку на рахунки комерційних структур або фізичних осіб з подальшим їх зняттям готівкою досить часто виконує оператор банку чи інша службова особа[3]. Тому

[1] Незалежна Асоціація банків України «Антикібер»: Кіберзлочинність: проблеми боротьби і прогнози. URL: http://anticyber.com.ua/article_detail.php?id=140.

[2] Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет : дис. ... канд. юрид. наук : 12.00.11. Київ, 2009. С. 71.

[3] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. С. 54–57.

доцільним було запровадження норм кримінального закону України, що містять опис складів кіберзлочинів зі спеціальним суб'єктом – особою, яка має право доступу до інформації, обробка якої здійснюється в кіберпросторі (ст. 362); особою, яка відповідає за експлуатацію комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 363).

Другий чинник стосується того, що процес імплементації положень Конвенції у кримінальне законодавство України супроводжується приєднанням України до інших багатосторонніх міжнародних угод в цій сфері. Україною визнано обов'язковість норм не лише Конвенції про кіберзлочинність, а й інших багатосторонніх міжнародних угод, що стосуються питання боротьби зі злочинами, вчиненими у кіберпросторі.

Стандарти окремих з таких договорів безпосередньо визнані Конвенцією про кіберзлочинність. Зокрема, в тексті Конвенції міститься посилання на такі міжнародні акти, ратифіковані Україною:

– в частині визначення державою меж дотримання права людини на інформацію, що є складовим елементом права особи на свободу вираження поглядів, – на Конвенцію Ради Європи про захист прав людини і основних свобод 1950 року[1] та Міжнародний пакт ООН про громадянські й політичні права 1966 року[2];

– в частині забезпечення захисту персональних даних, що зберігаються у файлах даних для автоматизованої обробки, та запобігання несанкціонованим доступу, їх зміненню або поширенню – на Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних 1981 року[3];

---

[1] Європейська Конвенція про захист прав людей та основоположних свобод : міжнар. док. від 4 листоп. 1950 р. URL: http://zakon5.rada.gov.ua. laws/show/995_004?nreg=995_004&find=1&text=%F1%EA%E0%F0&x=12&y=7#n150 ; Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 р. Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції : Закон України від 17 лип. 1997 р. № 475/97-ВР. URL: http://zakon3.rada.gov.ua/ laws/show/ru/475/97-%D0%B2%D1%80.

[2] Міжнародний пакт про громадянські й політичні права : міжнар. док. від 16 груд. 1966 р. URL: http://zakon3.rada.gov.ua/laws/show/995_043; Про ратифікацію Міжнародного пакту про економічні, соціальні і культурні права та Міжнародного пакту про громадянські й політичні права : Указ Президії ВР УСРС від 19 жовт. 1973 р. № 2148-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2148-08.

[3] Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнар. док. від 28 січ. 1981 р. URL: http://zakon5.rada.gov.ua/laws/show/994_326; Про ратифікацію Конвенції про захист

– в частині забезпечення захисту дитини від усіх форм сексуальної експлуатації та сексуальних розбещень – на Конвенцію ООН про права дитини 1989 року[1], Конвенцію Міжнародної організації праці про заборону та негайні заходи щодо ліквідації найгірших форм дитячої праці[2];

– в частині запитів про взаємну допомогу, переданих телекомунікаційними шляхами – на Європейську Конвенцію про взаємодопомогу у кримінальних справах[3];

– в частині захисту інтелектальнх прав – на Бернську Конвенцію про захист літературних та художніх творів (Паризький Акт від 24 липня 1971 року, змінений 2 жовтня 1979 року)[4], Угоду про торговельні аспекти прав інтелектуальної власності[5]; Угоду Всесвітньої організації інтелектуальної власності про авторське право за

осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 лип. 2010р. № 2438-VI. URL: http://zakon5.rada.gov.ua/laws/show/2438-17.

[1] Конвенція про права дитини : міжнар. док. від 20 листоп. 1989 р. (зі змінами, схваленими резолюцією 50/155 Генеральної Асамблеї ООН від 21 груд. 1995 р.). URL: http://zakon5.rada.gov.ua/laws/show/995_021; Про ратифікацію Конвенції про права дитини : постанова ВР УССР від 27 лют. 1991 р. № 789-XII. URL: http://zakon5.rada.gov.ua/laws/show/789-12.

[2] Про ратифікацію Конвенції Міжнародної організації праці № 182 про заборону та негайні заходи щодо ліквідації найгірших форм дитячої праці : Закон України від 5 жовт. 2000 р. № 2022-III. URL: http://zakon3.rada.gov.ua/laws/show/2022

[3] Додатковий протокол № 2 до Європейської Конвенції про взаємодопомогу у кримінальних справах від 20 квітня 1959 р. : міжнар. док. від 8 листоп. 2001 р. URL: http://zakon5.rada.gov.ua/laws/show/994_518/page?text=%E5%EB%E5%EA%EE%EC; Про ратифікацію Другого додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах : Закон України від 1 черв. 2011 р. № 3449-VI. URL: http://zakon5.rada.gov.ua/laws/show/3449-17.

[4] Бернська Конвенція про захист літературних та художніх творів (Паризький акт від 24 лип. 1971 р., змінений 2 жовт. 1979 р.) : міжнар. док. від 24 лип. 1971 р. URL: http://zakon3.rada.gov.ua/laws/show/995_051/page; Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 лип. 1971 р., зміненого 2 жовт. 1979 р.) : Закон України від 31 трав. 1995 р. № 189/95-ВР. URL: http://zakon3.rada.gov.ua/laws/show/189/95-%D0%B2%D1%80.

[5] Угоди про торговельні аспекти прав інтелектуальної власності : міжнар. док. від 15 квіт. 1994 р. URL: http://zakon5.rada.gov.ua/ laws/show/981_018; Про прийняття Протоколу про внесення змін до Угоди ТРІПС : Закон України від 3 лют. 2016 р. № 981-VIII. URL: http://zakon5.rada.gov.ua/laws/show/981-19/paran2#n2.

Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція)[1];

– в частині забезпечення рівності людей перед законом і рівний захист від усякої дискримінації та від усякого підбурювання до дискримінації – на Міжнародну конвенцію про ліквідацію всіх форм расової дискримінації[2];

– в частині процедурних аспектів переслідування злочинців – на Європейську Конвенцію про видачу правопорушників[3].

Іншими міжнародними договорами в кримінальному законодавстві України було передбачено відповідальність за певні дії, вчинені у кіберпросторі, що відповідно до положень Конвенції про кіберзлочинність не є злочином у кіберсфері. Так, 12 грудня 2003 року на п'ятому пленарному засіданні Всесвітньої зустрічі на вищому рівні з питань інформаційного суспільства, що відбувалася в Женеві (Швейцарія), на підставі рішення Ради Міжнародного союзу електрозв'язку (МСЕ) і резолюцій 56/183 і 57/238 Генеральної Асамблеї ООН, вповноваженими від 103 держав, включно й України, одноголосно було прийнято Декларацію принципів[4]. Її п. 37 закріплено: «спам представляє для користувачів, мереж і загалом для

---

[1] Угоди ВОІВ про авторське право за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція) : міжнар. док. від 26 жовт. 1961 р. URL: http://zakon3.rada.gov.ua/laws/show/995_763; Про приєднання України до міжнародної конвенції про охорону інтересів виконавців, виробників фонограм і організацій мовлення : Закон України від 20 верес. 2001 р. № 2730-III. URL: http://zakon3.rada.gov.ua/laws/show/2730-14.

[2] Міжнародна конвенція про ліквідацію всіх форм расової дискримінації : міжнар. док. від 4 січ. 1969 р. URL: куhttp://zakon3.rada.gov.ua/laws/show/995_105

[3] Про ратифікацію Європейської конвенції про видачу правопорушників : міжнар. док. від 13 груд. 1957 р. URL: http://zakon3.rada.gov.ua/laws/show/995_033; Про ратифікацію Європейської конвенції про видачу правопорушників 1957 р., Додаткового протоколу 1975 р. та Другого додаткового протоколу 1978 р. до Конвенції : Закон України від 16 січ. 1998 р. № 43/98. URL: http://zakon3.rada.gov.ua/laws/show/43/98-%D0%B2%D1%80.

[4] Письмо Постоянного представителя Швейцарии при ООН от 7 окт. 2004 г. на имя Генерального секретаря с Приложением Отчета о Женевском этапе всемирной встречи на высшем уровне по вопросам информационного общества, Женева Palexpo, 10–12 дек. 2003 года. URL: http://www.un.org/ru/documents/ods.asp?m=%20A/C.2/59/3.

Інтернету серйозну проблему, масштаби якої зростають. Питання, що стосуються спаму й кібербезпеки, слід розглядати на відповідному національному й міжнародному рівнях». Відповідно, через рік, 23 грудня 2004 року, КК України був доповнений ст. 363-1 «Перешкоджання роботі ЕОМ (комп'ютерів), АС, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку», якою, власне, було передбачено кримінальну відповідальність за розсилання спаму, що стало причиною порушення або припинення роботи комп'ютерів, АС, комп'ютерних мереж чи мереж електрозв'язку. Згідно зі ст. 3 Правил надання та отримання телекомунікаційних послуг, терміном «спам» позначено електронні, текстові та/або мультимедійні повідомлення, які без попередньої згоди (замовлення) споживача умисно масово надсилаються на його адресу електронної пошти або кінцеве обладнання абонента, крім повідомлень оператора, провайдера щодо надання послуг[1]. Злочинці досить вдало використовують спам-повідомлення для несанкціонованого проникнення до електронної системи користувача, викрадення або модифікації інформації, поширення вірусів з різною злочинною метою. Для цього в листах розміщують шкідливі вкладення, у момент завантаження або переходу яких за відповідними вкладеними посиланнями шкідливі програми починають діяти відповідним чином.

Третім чинником щодо правого регулювання сфери боротьби зі злочинами, вчиненими у кіберпросторі, слід вважати паралельне формування національного галузевого законодавства у сфері забезпечення національної кібербезпеки. Однією із загроз національній безпеці є саме кібернетична загроза. У березні 2016 року Указом Президента України було введено в дію Рішення Ради національної безпеки і оборони України «Про Стратегію кібербезпеки України». Метою Стратегії кібербезпеки України є створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави[2]. Визначальними позиціями в Стратегії є шляхи

[1] Про затвердження Правил надання та отримання телекомунікаційних послуг : постанова Кабінету Міністрів від 11 квіт. 2012 р. № 295. URL: http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF/page?text=%F1%EF%E0%EC#w11.

[2] Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96/2016. URL: http://zakon2.rada.gov.ua /laws/show/96/2016/paran11#n11.

розв'язання питань консолідації зусиль у розслідуванні та запобіганні кіберзлочинам різних суб'єктів забезпечення кібербезпеки, зокрема Міністерства оборони України, Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Національної поліції України, Національного банку України, розвідувальних органів. Щороку Кабінет Міністрів України своїм розпорядженням затверджує План заходів з реалізації Стратегії, зазначаючи конкретних виконавців і терміни виконання. 5 жовтня 2017 року Верховна Рада України прийняла Закон «Про основні засади забезпечення кібербезпеки України». Не дивлячись на те, що у ньому лише частково враховано висловлені раніше зауваження Комітету Верховної Ради України з питань інформатизації та зв'язку та Головного юридичного управління, цей закон став відправною точкою для протидії кібератакам, актам кібертероризму та іншим злочинним проявам у куіберпрострі. Тому вважаємо, для України стало актуальним питання доповнення окремих статей КК України кваліфікаційною ознакою стосовно використання обстановки кіберпростору для вчинення відповідних видів злочинів, зокрема проти основ національної безпеки України (ст. 109–114 КК України), у сфері охорони державної таємниці (ст. 328, 330); проти виборчих прав і свобод (ст. 157, 158, 159, 159-1); проти власності (ст. 185, 189, 191); у сфері господарської діяльності (ст. 206, 209, 231, 232); пов'язаних з тероризмом (ст. 258, 258-2, 258-3, 258-5); у сфері незаконного обігу наркотичних засобів (ст. 307, 311); придбання чи збут зброї, бойових припасів або вибухових речовин, аналогічних дій та використання спеціальних технічних засобів отримання інформації (ст. 263, 359).

Таким чином, правові основи боротьби зі злочинами, що вчиняються у кіберпросторі, визначаються, перш за все, Конвенцією Ради Європи про кіберзлочинність від 23 листопада 2001 року до сьогодні триває процес узгодження норм КК України та Конвенції.

Сучасний стан правового регулювання боротьби зі злочинами, вчиненими у кіберпросторі, характеризується відносною цілісністю системи актів у цьому напрямку на національному рівні при дезорганізованості системи нормативно-правових актів на міжнародному рівні регулювання. Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми Конвенції Ради Європи про

кіберзлочинність від 23 листопаду 2001 року, Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року, загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору. Іншими складовими національної системи правового регулювання боротьби з такими злочинами виступають норми галузевого законодавства, зокрема у сфері забезпечення національної, економічної та кібернетичної безпеки, захисту суспільства, дітей, інформації, авторських та суміжних прав.

Порівняльне дослідження українського та міжнародного сегментів кримінально-правових норм, якими регламентовано відповідальність за кіберзлочини та злочини, вчинені з комп'ютерів, АС і мереж, дає можливість визначити у КК України альтернативні Конвенції про кіберзлочинність кримінальні правопорушення, що можуть бути вчинені у кіберпросторі (ст. 163, 203-2, 232, 258-2, 362, 363, 363-1, 376, 436, 436-1 КК України). При цьому допоки в кримінально-правовому законодавстві питання криміналізації вчинення у кіберпросторі традиційних злочинів залишається невирішеним, у боротьбі з такими кримінальними правопорушеннями особливого значення набувають теоретичні засади їх розслідування, що дозволить мінімізувати труднощі збирання, дослідження, оцінки та використання доказів, правильно планувати та організувати їх розслідування

1.3. Криміналістична класифікація злочинів, вчинених у кіберпросторі

Класифікація об'єкта пізнання спрощує його вивчення, забезпечує ефективність системного підходу до пізнання множини об'єктів, дає можливість визначити її внутрішні закономірності й істотні ознаки. З філософської позиції класифікація розглядається як природній метод пізнання[1]. С. С. Розова пише про класифікацію як принцип побудови системи повних знань, що є необхідним посередником при практичному або пізнавальному використовуванні

[1] Розова С. С. Научная классификация и ее виды. *Вопросы философии*. 1964. № 8. С. 68–79

неповних знань[1]. Класифікація – це упорядкування об'єктів за їх схожістю, а об'єктом можна назвати все, включаючи процеси і дії (усе, що можна описати за допомогою визначників властивостей)[2].

В науках кримінального циклу розподіл множини злочинів, як об'єкта пізнання, на класи, види і категорії є однією з умов зручності та ефективності такого пізнання. В теорії кримінального права науково-теоретичні класифікації злочинів за ступенем тяжкості, за об'єктом посягання стали підґрунтям законодавчої типологізації злочинів в Україні. В практичному сенсі, на думку Л. М. Кривоченко це, є першим етапом індивідуалізації відповідальності, на якому законодавець встановлює її межі[3].

Кримінологічна класифікація злочинів підпорядкована завданню їх попередження – ціле (злочинність) розчленовується на частини (види, групи) за різними підставами і ознаками. Наприклад, на перше місце ставляться особливості особистості злочинця і виділяються такі види, як жіноча злочинність, злочинність неповнолітніх, військовослужбовців. Такі знання в практичному значенні стають основою для виборчого, цілеспрямованого, адресного застосування заходів кримінологічної профілактики[4].

Криміналістична класифікація пройшла еволюційний шлях свого становлення і набуває все більш поширеного застосування. Як зазначає В. А. Журавель криміналістична класифікація – це засіб упорядкування окремих категорій злочинів за їх криміналістично-значущими ознаками[5].

На думку В. Ю. Шепітько криміналістична класифікація злочинів – це їх диференціація (або систематизація) за криміналістично значущими підставами, що сприяє формуванню криміналістичних характеристик злочинів і розробленню окремих

---

[1] Розова С. С. Методологические основы психологии : учеб. пособие. *Новосибирский государственный университет.* Новосибирск, 2013. Ч. 1 : Теория познания С. 79.

[2] Сокал Р. Р. Кластер-анализ и классификация: предпосылки и основные направления. *Классификация и кластер*. М., 1980. С. 7.

[3] Кривоченко Л. М. Класифікація злочинів за ступенем тяжкості у Кримінальному кодексі України : монографія. Київ, 2010. С. 78.

[4] Алексеев А. И. Криминология : курс лекций. М., 1999. С. 175.

[5] Журавель В. А. Криміналістична класифікація злочинів: засади формування та механізм застосування. *Вісник Академії правових наук*. 2002. № 3 (30). С. 162.

методик розслідування[1]. О. В. Пчеліна змістовно аналізуючи етимологію поняття «класифікація» приходить до думки, що криміналістична класифікація – це метод пізнання, який полягає в систематизації злочинів за криміналістичнозначущими ознаками відповідно до законів логіки задля задоволення потреб слідчої практики[2]. На думку В. В. Тіщенка криміналістична класифікація злочинів спрямована на систематизацію, вдосконалювання і розвиток методик розслідування окремих видів злочинів, сприяючи деталізації і з'ясуванню особливостей їх криміналістичної характеристики[3].

Наведені положення вказують на те, що прагматична роль криміналістичної класифікації злочинів полягає у тому, що вона створює відповідне підґрунтя для формування криміналістичної характеристики злочинів окремих видів і груп та вироблення найбільш наближених до потреб практики цілеспрямованих наукових рекомендацій з розслідування, що й утворює певну методику розслідування.

Класифікація – це, в першу чергу, система розміщення предметів за класами на підставі схожості цих предметів у середині класу та їх відмінності від предметів інших класів[4]. Тому основною проблематикою криміналістів стали підстави для побудови класифікаційних систем злочинів, а відповідно й методик їх розслідування. Вивчення цієї проблеми дає можливість конкретизувати три наукових підходи до виділення критеріїв класифікації злочинів/методик їх розслідування.

1. В основу класифікації злочинів/методик покладають кримінально-правові ознаки (критерії), що визначають нормативну суть класифікації, передбаченої законом. Р. С. Бєлкін свого часу запропонував класифікувати злочини за елементами складу злочину, наприклад, як-от злочинів, пов'язаних із суб'єктом злочину, що поділяються, на: одноособово і групою; вперше і повторно; особами, що перебувають в особливих відносинах з безпосереднім предметом

[1] Шепітько В. Ю. Криміналістика : підручник. Київ, 2010. С. 324.

[2] Пчеліна О. В. Криміналістична класифікація злочинів. *Право і суспільство.* 2014. № 6-1. Ч. 2. С. 308.

[3] Тіщенко В. В. Теоретичні і практичні основи методик розслідування злочинів : монографія. Одеса, 2007. С. 29.

[4] Словник української мови : в 11 т. / за ред. І. К. Білодіда. Київ : Наук. думка, 1970–1980. Т. 4. С. 175.

посягання, та такими, що не перебувають у таких відносинах; дорослими злочинцями і неповнолітніми; чоловіками і жінками[1]. Г. Ю. Жирний систему окремих криміналістичних методик уявляв через структуру Особливої частини КК України[2]. З цього приводу В. А. Журавель справедливо резюмує, що йдеться тільки про окремі криміналістичні методики певних категорій злочинів, які розрізняються за двома критеріями: 1) щодо кримінально-правової класифікації; та 2) за ступенем спільності (рівнем конкретизації) методичних рекомендацій (групові, видові, підвидові)[3].

2. В основу криміналістичної класифікації злочинів/методик покладають криміналістичний критерій, що враховує особливості предмета посягання, обстановки злочину, його механізму та способів, типології особи злочинця, мети та мотивації злочинних дій тощо[4]. Так, В. В. Тіщенко класифікує корисливо-насильницькі злочини за елементами криміналістичної характеристики: 1) за особою злочинця: за кількістю учасників; за ступенем організованості; за віком; за статтю; за місцем роботи, навчання, роду занять, захоплень; за зв'язком злочинця з жертвою тощо; 2) за об'єктом (особою потерпілого і предметом посягання); 3) за обстановкою їх вчинення: залежно від місця їх здійснення; за часом; за іншими елементами обстановки; 4) за способом підготовки, вчинення і приховування; 5) за результатом і наслідками[5]. В контексті розроблення криміналістичних методик виділяє: базові, допоміжні, споріднені, побічні, нетипові злочини[6].

3. В основу криміналістичної класифікації злочинів/методик у сучасних наукових розробках з тематики методик розслідування

---

[1] Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 3 : Криминалистические средства, приемы и рекомендации. С. 326.

[2] Жирний Г. Ю. До питання про класифікацію окремих криміналістичних методик. *Актуальні проблеми криміналістики :* матеріали Міжнар. наук.-практ. конф. (Харків, 25–26 верес. 2003 р.). Харків, 2003. С. 105.

[3] Журавель В. А. Криміналістична класифікація злочинів: засади формування та механізм застосування. *Вісник Академії правових наук.* 2002. № 3 (30). С. 163.

[4] Криминалистика : учебник / [Б. Е. Богданов и др.] ; отв ред. А. Н. Васильєв. М., 1971. С. 425.

[5] Тіщенко В. В. Теоретичні і практичні основи методик розслідування злочинів : монографія. Одеса, 2007. С. 32–38.

[6] Там само. С. 44.

злочинів покладено два взаємопов'язаних критерії: кримінально-правовий та криміналістичний[1]. Як слушно зазначає В. А. Журавель, сучасний етап розвитку криміналістики, активізація її прогностичної функції обумовлюють можливість застосування іншого напрямку, за яким методики розслідування певних категорій злочинів створюються на підставі наукових розробок[2]. В цьому контексті автор веде мову про ускладнені (групові) методики – родові, міжродові, комплексні, визнаючи, що у цих випадках наука випереджає практику, компенсує відсутність необхідного емпіричного матеріалу або узагальнює існуючі рекомендації за типовими ознаками, що притаманні не одному виду злочинів, а цілій їх групі[3]. Саме при розробленні таких методик спостерігається злиття криміналістичних та кримінально-правових знань, що в умовах сучасної інформаційної невизначеності на початку досудового розслідування якісно розширює можливості слідчого у встановленні об'єктивної дійсності події злочину.

Видається, що найбільш продуктивно класифікаційний підхід був використаний стосовно побудови методик розслідування економічних злочинів. Як зазначив Г. А. Матусовський, в побудові класифікацій злочинів і практиці їх застосування можна відзначити певну ієрархію, де серед кримінально-правової, кримінологічної і криміналістичної класифікацій, які використовуються для вирішення певних завдань, приорітетною є кримінально-правова класифікація. Тому при побудові криміналістичної класифікації злочинів потрібно враховувати як різний ступінь суспільної небезпечності (загальна частина кримінального права), так і систему різних родових об'єктів складу злочину. Названий вчений вважав доцільним розглядати криміналістичну класифікацію економічних злочинів як систему їх

[1] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. ... д-ра юрид. наук : 12.00.09. Харків, 2011. 407 с.; Яблоков Н. П. Научные основы методики расследования. *Криминалистика* : учебник. М., 1995. 708 с.; Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. дис. … д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с.

[2] Журавель В. А. Криміналістична класифікація злочинів: засади формування та механізм застосування. *Вісник Академії правових наук*. 2002. № 3 (30). С. 163

[3] Журавель В. А. Технології побудови окремих криміналістичних методик розслідування злочинів. *Науковий вісник Львівської комерційної академії.* 2015. Вип. 2. С. 305–315. (Серія «Юридична»).

груп і видів, які передбачені відповідними нормами кримінального кодексу, розподілених за сферами соціальних відносин (власності, виконання бюджету, фінансових відносин, підприємництва, обслуговування населення та ін.)[1].

Розглядаючи економічні злочини, як корисливі діяння, вчинені особами з використанням легальних форм господарської діяльності чи повноважень з контролю за цією діяльністю в різних соціальних сферах, А. Ф. Волобуєв запропонував класифікувати ці злочини на дві групи: 1) основні (предикатні) злочини; 2) підпорядковані злочини. Основою для такої класифікації було використано поєднання різних видів злочинів (за кримінально-правовою класифікацією) єдиним задумом спрямованим на заволодіння чужим майном або отримання іншої матеріальної вигоди. До основних (предикатних) економічних злочинів були віднесені ті, котрі безпосередньо спрямовані на заволодіння чужим майном чи одержання іншої незаконної вигоди: шахрайство (ст. 190 КК України); заволодіння чужим майном шляхом зловживання службовим становищем (ч. 2 ст. 191 КК України); ухиляння від сплати податків, зборів, інших обов'язкових платежів (ст. 212 КК України); шахрайство з фінансовими ресурсами (ст. 222 КК України). До підпорядкованих злочинів віднесені злочини, які виступають формою, способом чи необхідною умовою вчинення основного злочину: незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200 КК України); фіктивне підприємництво (ст. 205 КК України); легалізація (відмивання) грошових коштів та іншого майна, здобутих злочинним шляхом (ст. 209 КК України) та ін. Поєднання основних і підпорядкованих злочинів для досягнення тієї чи іншої корисливої мети визначалося вказаним автором, як певні технології злочинної діяльності, стосовно яких і потрібно розробляти комплексні методики розслідування [2].

Прямо або опосередковано через обрання певного складного за структурою злочину як об'єкта дослідження комплексна методика серед ускладнених методик справедливо вважається найбільш

[1] Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков, 1999. С. 29–30; 42–43.

[2] Волобуєв А. Ф. Економічні злочини: поняття та проблеми розробки методик розслідування. *Актуальні проблеми держави і права.* 2003. Вип. 21. С. 37–39.

оптимальною для розв'язання завдань слідчого[1]. На думку А. Ф. Волобуєва, А. В. Шмоніна, Б. В. Щура комплексна методика спрямована на розслідування комплексу злочинів, між якими існують взаємозв'язки. Сьогодні такі злочини вчиняються часто організованими групами, посягають на різні предмети, при цьому кваліфікуються за різними статтями різних розділів Особливої частини КК України. У кримінальному праві дана проблема визначається як множинність злочинів, яка виявляється в різних формах, установлення яких за допомогою криміналістичних методів та засобів складає одне з найважливіших завдань [2].

Криміналістика покликана сприяти слідчому у розкритті та розслідуванні злочинів сучасними криміналістичними рекомендаціями. Поява та інтенсивний розвиток децентралізованої технології обміну й зберігання інформації, «хмарних обчислень», технологій анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій, або англ. Virtual Private Network) інших засобів-анонімайзерів) має наслідком вчинення комплексу злочинів якісно нового рівня організації злочинної діяльності, яка має ознаки технологічного процесу.

І. О. Возгрін підкреслював існування «технології злочинної діяльності», яку розумів як певний зміст та динаміку процесів, що

[1] Журавель В. А. Технології побудови окремих криміналістичних методик розслідування злочинів. *Науковий вісник Львівської комерційної академії.* 2015. Вип. 2. С. 309. (Серія «Юридична»); Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. ... д-ра юрид. наук : 12.00.09. Харків, 2011. С. 127; Волобуєв А. Ф. Комплексна методика розслідування економічних злочинів. *Вісник прокуратури*. 2003. № 6 (24). С. 53–56; Корнилов Г. А. Расследование преступлений, совершаемых в финансово-кредитной сфере. М. ; Якутск, 2002. 252 с.; Ищенко Е. П. Расследование преступлений, связанных с профессиональной деятельностью. М., 2009. 352 с.; Тищенко В. В. Теоретичні і практичні основи методик розслідування злочинів : монографія. Одеса, 2007. 260 с. Матусовский Г. А. Экономические преступления: криминалистический анализ : монография. Харьков, 1999. С. 129.

[2] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. ... д-ра юрид. наук : 12.00.09. Харків, 2011. С. 128.

складають механізм і спосіб вчинення злочину[1]. А. Ф. Лубін названим терміном визначав сукупність всіх процесів, що складають злочинну діяльність, відзначаючи потребу у переосмисленні методологічних підходів до вивчення злочинної діяльності[2]. В. І. Куліков, В. П. Корж, А. Ф. Волобуєв, В. Б. Смелік та багато інших науковців використовували в криміналістиці поняття «технологія злочинної діяльності» щодо вчинення складних, комплексних злочинів[3]. Про використання в криміналістиці поняття «технологія злочинів» наголошував А. В. Шмонін[4]. Тож, злочинна діяльність як будь-який технологічний процес може бути розчленована на певну кількість типових технологічних ланок або операцій, що утворюють певну послідовність, схему діяльності злочинців.

Досягнення злочинного результату у кіберпросторі супроводжується комплексом злочинних дій, реалізація яких забезпечується кібертехнологіями у значенні комплексу методів і процедур, за допомогою яких реалізуються функції збирання, оброблення, зберігання та доведення до користувача інформації в організаційно-управлінських системах з використанням обраного комплексу технічних засобів[5]. Кожну типову технологію злочинної діяльності у кіберпросторі можна охарактеризувати через послідовне

---

[1] Возгрин И. А. Введение в криминалистику: история, основы теории, библиография. СПб., 2003. С. 34–35.

[2] Лубин А. Ф. Методология криминалистического исследования механизма преступной деятельности : дис. … д-ра юрид. наук : 12.00.09. Н. Новгород, 1997. 337 с.

[3] Аверина Н. А., Скрыпников А. И. Раскрытие серийных преступлений против личности и убийств, совершенных по найму : учеб.-метод. пособие. М. : ВНИИ МВД России, 1998. 56 с.; Куликов В. И. Основы криминалистической теории организованной преступной деятельности. Ульяновск : Филиал МГУ, 1994. 256 с.; Корж В. П. Методика расследования экономических преступлений, совершаемых организованными группами, преступными организациями. *Руководство для следователей :* науч.-практ. пособие. Харьков, 2002. 280 с.; Протидія економічній злочинності / [П. І. Орлов, А. Ф. Волобуєв, І. М. Осика та ін.]. Харків : Нац. ун-т внутр. справ, 2004. 568 с.; Смелік В. Б. Кореляційні зв'язки між окремими видами злочинів у сфері підприємництва (проблеми методики розслідування) : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2006. 20 с.

[4] Шмонин А. В. Методология криминалистической методики : монография. М., 2010. С. 164–165.

[5] Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посіб. Київ : КНЕУ, 2003. С. 7.

обрання злочинцем для використання відповідної інформаційно-комунікаційної технології, що впроваджується у інформаційне суспільство з певною суспільнокорисною метою. Наприклад, технології електронної комерції, електронних бірж та аукціонів, електронних депозитаріїв, безготівкових розрахунків, що з метою досягнення злочинного результату застосовуються злочинцем у певній послідовності, створюють безмежні можливості для вчинення економічних злочинів: від звичайних розкрадань майна шляхом обману (шляхом створення фіктивних інвестиційних фірм, ведення фіктивного підприємництва) до легалізації (відмивання) доходів, одержаних злочинним шляхом. В цьому сенсі Л. І. Аркуша пише про взаємопов'язані господарські, посадові, «комп'ютерні» злочини та злочини проти власності як злочинні технології[1].

Використання технологій анонімайзерів дозволяє забезпечувати конфіденційність інформації про користувача з метою отримання останнім доступу до заборонених у локальній мережі веб-сайтів, доступ до яких громадянам певної країни заблокований рішенням державних органів цієї країни. Наприклад, користувач заходить на веб-сайт, що надає послугу анонімайзера, вводить в адресний рядок адресу веб-сторінки, яку користувач бажає відвідати анонімно. Анонімайзер завантажує цю сторінку собі, обробляє її та передає користувачу, але вже від свого (сервера-анонімайзера) імені. В іншому разі технологія TOR (браузер) аналогічно дозволяє отримати анонімний доступ до певних ресурсів Інтернет шляхом так званої «цибулевої маршрутизації». Для передавання інформації використовуються три довільні Інтернет-вузли. Tor-браузер (Tor Browser) відправляє першому вузлу пакет із зашифрованою адресою другого вузла. Перший вузол має ключ для розшифрування адреси та переправляє інформацію на другий вузол. Останній, одержавши пакет, має ключ для розшифрування адреси третього вузла. Таким чином, для правоохоронних органів стає незрозумілим, який саме сайт особа запитувала та відвідала в результаті через вікно Tor-браузера. Ці та аналогічні програмні засоби з мережі Інтернет

[1] Аркуша Л. І. Основи виявлення та розслідування легалізації доходів, одержаних в результаті організованої злочинної діяльності: Интернет : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2011. 496 с.

вільно завантажує будь-який користувач. Використання таких технологій створює безмежні можливості для вчинення злочинів різної тяжкості: від створення ринків збуту товарів, заборонених до цивільного обігу (наркотиків, зброї), поширення порнографії, порушення авторських прав до терористичних актів.

Технологія «хмарних обчислень» і децентралізованих мереж обміну інформацією та засобів зберігання означає, що, незважаючи на можливість ідентифікації місця перебування конкретного засобу комп'ютерної техніки в конкретний момент часу, аналогічні дані можуть існувати у вигляді декількох копій, розповсюджуватися між багатьма пристроями й місцями знаходження та переміщуватися в інший географічний локус за декілька секунд. Організовані злочинні групи використовуватимуть саме такі технології, оскільки останні справляють безпосередній уплив як на вчинення злочину, так і на процес його розслідування. По-перше, якщо постачальник Інтернет-послуг або безпосередньо відомості перебуватимуть поза межами юрисдикції державних органів країни, в якій проводиться розслідування, процес розслідування такої злочинної діяльності буде ускладнений тривалими процедурами надання взаємної правової допомоги. По-друге, інформація в децентралізованих комп'ютерних мережах досить часто є зашифрованою або фрагментованою, це змушує правоохоронні органи звертатися по допомогу до відповідних фахівців, застосовувати заходи примусу відносно постачальників послуг або фізичних осіб, що ускладнює доступ до екстериторіальних джерел інформації.

Тому в криміналістичному аспекті сучасна парадигма злочинів, вчинених у кіберпросторі, є складною, комплексною. Це не елементарна сукупність злочинів або технологія злочинної діяльності. Одні комп'ютерні технології злочинці можуть використовувати для досягнення різного злочинного результату, поєднання інших як типові для досягнення певного злочинного результату, чим вдало користаються організовані злочинні групи. Особливий технологічний, комплексний і транснаціональний характер злочинної діяльності, що передбачає використання обстановки кіберпростору, вимагає розроблення новітньої комплексної методики, що дозволить інтегрувати дані про визначені взаємозв'язки такої множинності злочинів та на їх підставі розробити оптимальну систему

криміналістичних рекомендацій з виявлення та розслідування злочинів визначеної категорії.

Це підтверджується результатами анкетування, адже 80% опитаних практиків НП України вказали на потребу в науково-методичних рекомендаціях з розслідування комплексу злочинів, вчинених у кіберпросторі. Така методика є потребою в першу чергу слідчих органів, що пов'язано із відсутністю на рівні регіонів України спеціалізації слідчих в розслідуванні кримінальних правопорушень вказаної категорії. При відсутності відповідної методики розслідування кримінальні провадження щодо злочинів, вчинених у кіберпросторі, доручаються недосвідченим слідчим, що призводить до неповноти слідства, не встановлення всієї множини злочинів та складу злочинної групи. З аналізованого матеріалу у більше ніж у 80 % кримінальних проваджень фігурують невстановлені під час слідства особи-співучасники злочину.

Вдаючись до фактичного розроблення криміналістичної класифікації злочинів, науковці наголошують на цілі такої класифікації, зокрема необхідності забезпечення потреб криміналістичної науки та практики такою класифікацією[1]. Н. П. Яблоков справедливо вважав, що криміналістичні підстави класифікації злочинів повинні бути відповідно значущими і методично перспективними[2]. Дійсно, якщо пропонується криміналістична класифікація злочинів певного виду з безліччю підстав та класифікаційних систем, виникає питання про доцільність такої класифікації, та про те, чи кожний з запропонованих видів злочинів можна покласти в основу відповідних методичних рекомендацій з їх розслідування. На думку Б. В. Щура не можна обмежуватися у класифікаційних побудовах лише криміналістичними ознаками (критеріями), а необхідно виходити з кримінально-правової класифікації злочинів, яка у цьому плані є базовою[3]. Ми також будемо

[1] Шмонин А. В. Методология криминалистической методики : монография. М., 2010. С. 118; Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса, 2007. С. 44.

[2] Яблоков Н. П. Научные основы методики расследования. *Криминалистика* : учебник. М. : Изд-во БЕК, 1995. С. 486.

[3] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. ... д-ра юрид. наук : 12.00.09. Харків, 2011. С. 166.

виходити з цих позицій при розробленні криміналістичної класифікації злочинів, вчинених у кіберпросторі.

В криміналістичній науці вже були спроби здійснити криміналістичну класифікацію подібних злочинів, але через різний зміст обраного для дослідження поняття, жодна з класифікацій не може задовольнити вимоги практиків. До сьогодні терміносполучення «злочини, вчинені у кіберпросторі» були підмінені поняттями «комп'ютерні злочини», «кіберзлочини», «інформаційні злочини», «злочини у сфері високих інформаційних технологій», «злочини у сфері комп'ютерної інформації». Здавалося би, дефінування конкретного терміна повинно сприяти вирішенню проблеми, втім окреслення понять зводить останні до інших, не визначених основних понять[1]. Тому для нашої мети потрібно спочатку розмежувати зміст означених понять з урахуванням вітчизняних, міжнародних та закордонних теоретико-прикладних досліджень у науках кримінального циклу.

Проаналізувавши публікації щодо тематики змісту терміна «комп'ютерні злочини» й не вдаючись до активної полеміки відносно недоцільності його використання (Ю. М. Батурін, В. В. Крилов)[2] через його фактичне існування, резюмуємо, що зміст терміна залежить від предметної сфери конкретної науки. На цьому справедливо наголошують також В. В. Вехов, М. В. Карчевський та багато інших науковців, які пропонують надавати різні визначення комп'ютерних злочинів з позиції кримінально-правової охорони, а також криміналістичної науки[3]. Традиційним у кримінально-правових дослідженнях стало ототожнення «комп'ютерного злочину» зі «злочинами у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», передбаченими винятково кримінально-правовими нормами однойменного Розділу

[1] Бауэр Ф. Л., Гооз Г. Информатика : в 2 ч. М., 1990. Ч. 1 : Вводный курс. С. 18.

[2] Батурин Ю. М. Проблемы компьютерного права. М., 1991. С. 129; Крылов В. В. Информационные компьютерные преступления : учеб. и практ. пособие. М., 1997. С. 11.

[3] Вехов В. В. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М., 1996. С. 23–24.

XVI КК України[1]. З метою скорочення громіздких терміносполучень цієї тематики у такому значенні термін «комп'ютерний злочин» став використовуватися в кримінально-правовій та окремій криміналістичній літературі (Д. Айкав, Ю. М. Батурин, А. Г. Волеводз, В. О. Голубєв, Р. А. Калюжний, М. В. Карчевський, Н. А. Розенфельд, К. Сейгер, У. Фонсторх та ін.)[2].

У криміналістиці термін «комп'ютерний злочин» має розширене тлумачення. Ним позначають діяння, в яких комп'ютер є предметом, знаряддям або засобом скоєння злочину. М. В. Салтевський, пояснюючи застосування терміна «комп'ютерні злочини», зазначав, що, на відміну від кримінального права, у криміналістиці вид злочину називають навіть не за засобом (знаряддям) вчинення злочину, а за видом злочинної діяльності[3]. На стику XX й XXI століть опубліковано цілу низку праць щодо «комп'ютерного злочину» в такому

[1] Карчевський М. В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину : дис. ... канд. юрид. наук : 12.00.08. Луганськ, 2003. С. 42; Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... д-ра юрид. наук : 12.00.02. Киев, 1992. С. 14; Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. ... канд. юрид. наук : 12.00.09. Запоріжжя, 2008. С. 38.

[2] Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... д-ра юрид. наук : 12.00.02. Киев, 1992. 23 с.; Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М., 1999. 351 с.; Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М., 1991. 157 с.; Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2002. 496 с.; Вертузаєв М. С., Голубєв В. О., Котляревський О. І., Юрченко О. М. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / за ред. О. П. Снігерьова. Запоріжжя, 1998. 316 с.; Карчевський М. В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину : дис. ... канд. юрид. наук : 12.00.08. Луганськ, 2003. 175 с.; Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.08. Київ, 2003. 222 с.

[3] Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посіб. Харків, 2000. С. 4.

трактуванні. Ідеться, зокрема, про криміналістів (П. Д. Біленчук, А. С. Білоусов, В. Б. Вехов, М. А. Зубань, Б. В. Романюк, В. С. Цимбалюк)[1], кримінологів (Р. І. Дрімлюга, Д. В. Добровольський, М. О. Кравцов)[2], процесуалістів (А. І. Журба)[3]. Тому й у більшості джерел чітко визначають дві категорії злочинів, зокрема: 1) коли комп'ютер або інформація в ньому виступає предметом посягання (дії, що кваліфікуються за статтями Розділу XVI КК України); 2) коли комп'ютер є засобом вчинення злочину (традиційно ст. 185, 190, 191 КК України).

На окрему увагу заслуговує терміносполучення «злочини у сфері комп'ютерної інформації», яке в Україні на рівні дисертаційного дослідження 2002 року запровадив Д. С. Азаров. Цей вислів, на думку автора, зумовлений важливістю та значенням об'єкта посягання – комп'ютерної інформації[4]. До таких відносять злочини, передбачені Розділом XVI КК України, а також ч. 3 ст. 190 КК (шахрайство, вчинене шляхом незаконних операцій з використанням електронно-обчислювальної техніки) та ст. 200 КК (використання підроблених електронних засобів доступу до банківських рахунків)[5]. У цьому

[1] Вехов В. В. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М., 1996. 182 с.; Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посіб. Київ, 1994. 72 с. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. Запоріжжя, 2008. 245 с.

[2] Дримлюга Р. И. Интернет-преступность : автореф. дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2007. 23 с.; Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: уголовно-правовые и криминологические проблемы : дис. ... канд. юрид. наук : 12.00.08. М., 2005. 218 с.; Кравцов М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків, 2016. 16 с.

[3] Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. С. 59.

[4] Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08. Київ, 2002. С. 19.

[5] Голубєв В. О., Юрченко О. М. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту / за ред. О. П. Снігерьова, М. С. Вертузаєва. Запоріжжя, 1998. 140 с.; Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук : 12.00.08. Київ, 2002. 18 с.

аспекті В. В. Крилов у криміналістичних дослідженнях уживає поняття «інформаційні злочини», розуміючи їх як суспільно небезпечні діяння, заборонені кримінальним законом під погрозою покарання, вчинені в галузі інформаційних правовідносин[1].

Тож, криміналістична класифікація «комп'ютерних злочинів», «злочинів у сфері комп'ютерної інформації» та «інформаційних злочинів», як правило, здійснювалась за кримінально-правовими ознаками відповідної групи злочинів. Останню розглядали в аспекті «діянь, вчинених у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», кримінальну відповідальність за які передбачено однойменним Розділом XVI КК України, та злочинних діянь, вчинених за допомогою комп'ютера (ст. 190, 200 КК України). Варто зазначити, що законодавство України не містить тлумачення жодного з розглянутих терміносполучень. У ст. 7 Закону України «Про основи національної безпеки України»[2] на позначення основних загроз національній безпеці нашої держави використовується лише вислів «комп'ютерна злочинність та комп'ютерний тероризм». В окремих міжнародних угодах України міститься суто вказівка на термін [3].

Поява у криміналістичних дослідженнях терміносполучень «злочини у сфері високих інформаційних технологій» або «злочини у сфері комп'ютерних технологій» була пов'язана з розвитком наукового знання у сфері високих інформаційних технологій, комп'ютерних технологій зокрема. На цей час абсолютну більшість технологічних та соціальних процесів у державі, галузей виробництва від енергетики до засобів масової інформації виведено на інший наукомісткий рівень саме завдяки високим інформаційним технологіям, що засновані на автоматичній обробці інформації в процесі розв'язання обчислювальних та інформаційних завдань. Комп'ютерні технології є комплексом систематичних та масових

[1] Крылов В. В. Информационные компьютерные преступления : учеб. и практ. пособие. М., 1997. С. 11.

[2] Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV. URL: http://zakon2.rada.gov.ua/laws/show/964-15.

[3] Договір між Кабінетом Міністрів України та Федеральним Урядом Республіки Австрія про співробітництво у сфері боротьби зі злочинністю : постанова Кабінету Міністрів від 17 лип. 2014 р. № 270. URL: http://zakon3.rada.gov.ua/laws/show/040_040.

засобів і прийомів автоматичної обробки інформації, заснованих на перетворенні інформації в числову форму, що забезпечує високу швидкість обробки даних, пошуку інформації, розосередження даних, доступ до джерел інформатизації незалежно від місця розташування[1]. Комп'ютер є лише одним з апаратних засобів комп'ютерних технологій. Тому очевидно помилковою видається попередня практика посилання криміналістів тільки на його використання в перебігу вчинення злочинів.

Застосування будь-яких апаратних та програмних засобів комп'ютерних технологій у вчиненні злочину має наслідком утворення специфічних слідів – змін у специфічному інформаційному середовищі, що зумовлює необхідність використання в процесі розслідування відповідних (спеціальних) прийомів і методів їх виявлення й дослідження. На межі першого й другого десятиріч XXI ст. наукові теми, окремі та комплексні методики розслідування злочинів розробляють саме з урахуванням цієї специфіки злочинної діяльності, зокрема щодо викрадень майна, шахрайств, незаконних дій у кредитно-фінансовій сфері тощо[2]. В основу криміналістичної класифікації покладаються різні криміналістичнозначущі ознаки, зокрема спосіб вчинення злочину, особа злочинця.

Тривала наукова та законодавча невизначеність наведеного соціально-правового явища призвела в країнах СНД до запозичення з міжнародної практики боротьби зі злочинами терміна «кіберзлочин» («cybercrime»). Аналіз сучасних публікацій, тем дисертаційних досліджень та інших джерел інформації дозволяє доволі впевнено

[1] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. С. 18.

[2] Там само. 328 с.; Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2009. 22 с.; Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.; 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.

стверджувати про всезагальне визнання українською науковою спільнотою цього терміна[1].

На нашу думку, запозичення з англійської терміна «кіберзлочин» можна розглядати з двох різнопланових позицій.

По-перше, запозичена конструкція є вдалою щодо предметної сторони криміналістичної науки, у змістовному плані її сформульовано лаконічно, вона проста для розуміння навіть не фахівцем з права. Як уже було доведено в першому підрозділі роботи, термін з префіксом «кібер» дає однозначну відповідь на обстановку вчинення конкретного злочинного явища – це кіберпростір як інформаційний простір взаємодії між людьми за допомогою інфраструктури електронних інформаційних технологій. До того ж, у вітчизняній криміналістичній науці доволі поширеною є практика використання багатьох запозичених з інших мов термінів, наприклад, тактика (гр. taktika – мистецтво шикування військ), криміналістика (лат. Criminalis – злочинний, той, що належить до злочинної діяльності), криміналістична фотографія (гр. photos – світло, гр. grapho – пишу)[2].

По-друге, проблему недостатньої аргументованості й хаотичного подання поняття «кіберзлочин», що властиво розробкам закордонних дослідників та зарубіжним правовим актам, екстрапольовано в національну науку.

Для розуміння особливостей процесу розвитку міжнародної наукової думки щодо змісту терміна «кіберзлочин» доцільно вдатися до аналізу результатів багаторічної роботи такого консультативного органу, як Конгрес ООН з попередження злочинності та поводження з правопорушниками, за Програмою ООН у сфері попередження злочинності та кримінального судочинства, а саме п. 29 Декларації

---

[1] Біленький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України (порівняльно-правове дослідження) : дис. ... канд. юрид. наук : 12.00.08. Одеса, 2015. 230 с.; Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів. *Юридичний часопис Національної академії внутрішніх справ.* 2011. № 1 (1). С. 89–93; Голубев В. А. Аналіз кіберзлочинності у сфері економічної безпеки. *Information Technology and Security.* 2013. № 1. С. 26–32; Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека.* 2014. № 1. С. 85–89.

[2] Радецька В. Я. Мова науки криміналістики : дис. ... канд. юрид. наук : 12.00.09. Київ, 2002. С. 39.

принципів[1]. Перший форум Конгресу відбувся в 1955 році в Женеві. Починаючи з десятого форуму Конгресу (Відень, 2000 рік), жоден (одинадцятий у Бангкоці, 2005 р.; дванадцятий у Сальвадорі, 2010 р.; тринадцятий у Досі, 2015 р.) не оминає теми боротьби з кіберзлочинами.

На Десятому форумі Конгресу термін «кіберзлочин» було подано у двох значеннях[2]. Кіберзлочин у вузькому сенсі (синонім до «комп'ютерний злочин», що використовували окремі доповідачі форуму) є будь-яким протиправним діянням, здійснюваним за допомогою електронних операцій, метою якого є подолання захисту комп'ютерних систем і оброблюваних ними даних. Кіберзлочини в широкому значенні (як синонім до «злочини, пов'язані з використанням комп'ютерів») – це будь-яке протиправне діяння, вчинене за допомогою або з використанням комп'ютерної системи чи мережі, включаючи й такі злочини, як незаконне зберігання, пропозиція або поширення інформації за допомогою комп'ютерної системи чи мережі.

На одинадцятому форумі Конгресу було прийнято так звану Бангкокську декларацію про взаємодію та відповідні заходи – стратегічні союзи (спілки) в галузі попередження злочинності й кримінального правосуддя[3], у п. 16 якої констатовано активізацію та розширення сучасного співробітництва у галузі попередження та розслідування злочинності, пов'язаної з використанням високих технологій і

---

[1] Создание эффективной программы ООН в области предупреждения преступности и уголовного правосудия : междунар. док. от 18 дек. 1991 г. № 46/152. URL: http://base.garant.ru/2565318/#ixzz4xKtuj3dP.

[2] Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничеств : справ. док. / 13 Конгресс ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апр. 2015 г. A/CONF.222/12). С. 23 24. URL: http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf.

[3] Бангкокська декларація про взаємодію і відповідні заходи: стратегічні союзи в галузі попередження злочинності і кримінального правосуддя : резолюція Генеральної Асамблеї ООН № 60/177, додаток 1. URL: http://www /zakon3.rada.gov.ua/laws/show/995_785.

комп'ютерів. У інших пунктах ідеться про тероризм і транснаціональну організовану злочинність, як різновид кіберзлочинності.

У центрі уваги учасників дванадцятого форуму Конгресу були транснаціональний та організаційний аспекти кіберзлочинності, організаційні відмінності підходів у національному законодавстві та інші важливі питання.

Останній форум Конгресу, датований 2015 роком, є надзвичайно важливим у сенсі практичного роз'яснення проблем та шляхів їх вирішення щодо розслідування кіберзлочинів[1]. Наведемо основні тези, що дають можливість визначити міжнародний погляд на зміст терміна «кіберзлочин».

По-перше, визнано, що межа між кіберзлочиністю та звичайною злочинністю стає все менш визначеною. Наприклад, у річному звіті про результати роботи за 2016 рік Управління ООН з наркотиків та злочинності конкретизовано напрями протидії кіберзлочинам (для країн Західної та Центральної Азії), зокрема: створення спеціалізованих підрозділів боротьби з кіберзлочинами; зміцнення регіональної співпраці між правоохоронними й судовими органами в питаннях переслідування кіберзлочинців, проведення розслідувань у «тіньовій мережі» (DarkNet); боротьба з проблемою незаконного використання віртуальних валют; збір і використання електронних доказів[2].

По-друге, до категорії «кіберзлочинність» віднесено такі діяння, об'єктом злочину яких є комп'ютерні дані або системи, а також діяння, за яких використання комп'ютерних або інформаційних систем є невід'ємною складовою способу вчинення злочину. До першої класифікаційної групи відносять отримання незаконного доступу до комп'ютерних даних або систем (іноді їх називають

[1] Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничеств : справ. док. / 13 Конгресс ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апр. 2015 г. (A/CONF.222/12). URL: http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf.

[2] Звіт про результати роботи за 2016 рік Управління ООН з наркотиків та злочинності щодо кіберзлочинності. URL: http://www.unodc.org/documents/rpanc/RP_Annual_Report_RU_31.05.17_low.pdf.

«основними» кіберзлочинами). До другої – використання комп'ютерних даних або систем для шахрайства, розкрадання чи спричинення шкоди іншим особам; злочини, пов'язані з використанням комп'ютерів та інтернет-контенту, включаючи пропаганду ненависті, дитячу порнографію, злочини з використанням особистих даних і продаж заборонених товарів у режимі онлайн.

Цікавим в аспекті розроблення криміналістичної класифікації злочинів, вчинених у кіберпросторі, є те, що міжнародна спільнота резюмувала, що у внутрішньому (національному) законодавстві про кіберзлочинність відповідальність за такі злочини встановлюється на підставі поєднання положень, що стосуються як суто кіберзлочинів, так і загальнокримінальних злочинів. Наведемо фрагмент офіційної публікації результатів форуму: «Кримінальна відповідальність за здійснення «основних», таких як отримання незаконного доступу до комп'ютерних даних і систем, може встановлюватися шляхом ухвалення спеціального законодавчого положення, тоді як діяння, пов'язані із застосуванням комп'ютерів для отримання особистої або фінансової допомоги або спричинення особистої або фінансової шкоди, частіше за все можуть визнаватися кримінальними на підставі положень, що стосуються здійснення загальнокримінальних (не пов'язаних із застосуванням комп'ютерів) злочинів. У деяких випадках внутрішні нормативно-правові засади приймаються у виконання з урахуванням багатобічних документів, які можуть бути обов'язковими або необов'язковими для сторін»[1].

До таких міжнародних документів відносять: Конвенцію про кібербезпеку і захист особистих даних африканського союзу, Угоду про співпрацю держав – членів Співдружності Незалежних Держав у боротьбі зі злочинами у сфері комп'ютерної інформації, Конвенцію Ради Європи про кіберзлочинність, Директиву 2013/40/EU європейського парламенту і Ради Європейського союзу про атаки на

[1] Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничеств : справ. док. / 13 Конгресс ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апр. 2015 г. A/CONF.222/12). С. 15. URL: http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf.

інформаційні системи, Конвенцію про боротьбу зі злочинами в галузі інформаційних технологій арабських держав і Угоду про співпрацю в галузі забезпечення міжнародної інформаційної безпеки Шанхайської організації співпраці. З огляду на таку кількість міжрегіональних нормативних актів, підготовча нарада до тринадцятого Конгресу рекомендувала державам розглянути питання щодо розроблення універсальної конвенції про кіберзлочинність, якої до сьогодні не існує.

Вважаємо, що термін «кіберзлочин» на міжнародній арені виправдано розширений до позначення ним усіх традиційних злочинів, вчинених у кіберпросторі. Утім розкриття змісту через конкретний перелік таких злочинів ми нині не побачимо в жодному нормативному акті чи теоретичній спробі класифікувати кіберзлочини. Це пов'язано з відсутністю універсального міжнародного документа щодо боротьби з кіберзлочинами. Більшість науковців апелює в цьому питанні до міжрегіональних нормативних актів, до яких приєдналася їх держава.

Як ми вже висновували в попередньому підрозділі, Конвенція Ради Європи про кіберзлочини далека від досконалості щодо визначення змісту та видів кіберзлочинів у європейському просторі. Тому, використовуючи дефініцію «кіберзлочин», вітчизняні науковці-правники невиправдано звужують зміст злочину, вчиненого у кіберпросторі. Це призводить до класифікації кіберзлочинів на підстві позицій наведеної Конвенції або криміналістичнозначущої ознаки – способу вчинення суто комп'ютерного злочину, що спричиняє неповноту розроблених методик розслідування.

Криміналістична класифікація злочинів, що вчиняються у кіберпросторі, буде мати практичний сенс, якщо складові системи злочинів будуть виключати повтори традиційних злочинів, оскільки при використанні відповідних рекомендацій з їх розслідування буде спостерігатися тенденція до їх розосередження на декілька складових системи. Тому в основу криміналістичної класифікації досліджуваної категорії злочинів повинен бути покладений один критерій поділу на групи злочинів, який буде мати криміналістичне значення. В межах кожної з груп можна виділити підгрупи, які також мають відповідно один критерій поділу. Останні об'єднують злочини певних кримінально-правових ознак, які вчиняються в кіберпросторі.

Використання кіберпростору забезпечує досягнення злочинної мети, в кожному конкретному випадку злочину. Досягення мети

злочину означає, що спонукання діяння мотивом закінчилось і певна потреба задовольнилась[1]. Розглянемо це твердження більш детально.

Мета досягається певним мотивом, на думку А. В. Савченко в цьому саме й полягає їх зв'язок. Мотив досить вдало піддавався дослідженню у науках кримінально-правового циклу[2], адже мотив в першу чергу є факультативним елементом складу злочину.

У психологічному аспекті мотив є необхідним, невід'ємним і реально існуючим компонентом у структурі будь-якої діяльності суб'єкта[3], тому й криміналісти не обходили увагою мотив вчинення злочину.

І. Ф. Пантелєєв вказував, що елементом криміналістичної характеристики злочинів слугують узагальнені дані щодо найбільш розповсюджених мотивів і цілей їх вчинення[4]. Але наголошувалось, що інформацію щодо них використовують для висунення версій стосовно суб'єкта та суб'єктивної сторони злочину, а також для організації цілеспрямованого пошуку злочинця. А. В. Шмонін, розглядаючи мотив у складі криміналістичної характеристики, писав, що він визначає вибір відповідного предмета посягання, способу впливу на нього[5]. Таке бачення ґрунтується на традиційному розумінні в психології мотиву як чинника, який, відображуючись у свідомості людини, спонукає його до діяльності, спрямовуючи її на задоволення певної потреби[6]. Намагаючись перенести термін «мотив»

---

[1] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 22.

[2] Музюкин А. П. Мотив преступления и его уголовно-правовое значение : автореф. дис. … канд. юрид. наук : 12.00.08. Рязань, 2010. 23 с.; Капинус О. С. Убийства: мотивы и цели. М., 2003. 312 с.; Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. 144 с.; Масол Д. І. Мотиви расової, національної чи релігійної нетерпимості у кримінальному праві України : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2014. 20 с.; Подільчак О. М. Мотив і мотивація злочинів учинених жінками : автореф. дис. … канд. юрид. наук : 12.00.08. Харків, 2004. 20 с.

[3] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 19.

[4] Криминалистика : учебник / под ред. И. Ф. Пантелеева, Н. А. Селиванова. М. : Юрид. лит., 1988. 672 с.

[5] Шмонин А. В. Методика расследования преступлений : учеб. пособие. М., 2006. С. 185.

[6] Общая психология : курс лекций / сост. Е. И. Рогов. М. : ВЛАДОС, 1995. С. 323; Маклаков А. Г. Общая психология. СПб. : Питер, 2000. С. 513.

на юридичнй ґрунт, А. В. Савченко, аналізуючи психологічні концепції визначення мотиву, прийшов до думки, що в цілому під мотивом можна розуміти складний інтегральний (системний) психологічний утвір[1]. Ця складність позначається через розуміння в психології мотиву як поняття, що узагальнює безліч диспозицій: органічних, матеріальних, соціальних, духовних[2]. Отже, кожний науковець, досліджуючи категорію «мотив злочину» апелював до певної психологічної концепції.

В криміналістичних дослідженнях переважає діяльнісний підхід[3]. Дійсно, адже одним з основних загальновизнаних об'єктів дослідження в криміналістиці є діяльність зі скоєння злочинів (злочинна діяльність)[4]. Мотив злочину в таких дослідженнях не можна відривати від злочинної діяльності, адже саме мотив виконує роль вектору злочинної діяльності. Мотив проходить крізь причинний зв'язок між злочинним наслідком і злочинним діянням[5]. Без встановлення такого причинного зв'язку не можна висновувати про наявність події злочину, вини конкретної особи у його вчиненні. При розслідуванні множини злочинів перед слідчим стоїть також завдання встановити весь комплекс злочинів, вчинених певною групою осіб або конкретною особою, визначити взаємозв'язок між злочинами. При цьому при прийнятті рішення про початок кримінального провадження та на початку розслідування злочинів, вчинених у кіберпросторі, слідчий має інформацію лише про злочинний результат, тобто потребу, яка була задоволена в результаті вчинення злочинів, а отже може висновувати про мотиви злочинців, відповідно визначати коло запідозрених осіб, способи вчинення злочину, предмет посягання тощо. Тож, мотив є категорією що безсумнівно має криміналістичне значення та може бути покладена в основу криміналістичної класифікації злочинів, вчинених у кіберпросторі.

---

[1] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 13.

[2] Немов Р. С. Психология : учебник : в 3 кн. 4-е изд. М. : ВЛАДОС, 2003. Кн. 1 : Общие основы психологии. С. 392.

[3] Тіщенко В. В. Теоретичні і практичні основи методик розслідування злочинів : монографія. Одеса, 2007. С. 8.

[4] Криміналістика : навч. посіб. / за ред. А. Ф. Волобуєва. Київ, 2011. С. 14.

[5] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 22.

Через те, що мотив має виражене соціально-психологічне та юридичне значення, існує безліч класифікацій мотивів в психології чи юридичних науках[1]. Для нас самостійне значення має саме соціальна складова мотиву вчинення злочину. Адже при дослідженні мотиву у центрі нашої уваги знаходяться злочини, що вчиняються в кіберпросторі, який характеризується соціальними чинниками через можливість задовольняти потреби конкретної людини.

Людська діяльність здійснювана з приводу того чи іншого матеріального або духовного об'єкта для задоволення соціальних потреб та інтересів нерозривно пов'язана із існуванням різних сфер життя суспільства. Таким чином виникають суспільні відносини (з приводу того чи іншого об'єкта) або соціальні відносини (як особливий вид суспільних, що відображають статус особи і соціальних груп у суспільстві)[2]. У соціології як науці про суспільство загальновизнаним є трактування сфери суспільного життя як певного комплексу стійких відносин між соціальними суб'єктами[3]. Філософи та соціологи умовно виокремлюють чотири таких сфери, зокрема: економічну, політичну, духовну та соціальну[4]. У зарубіжних публікаціях активно поширюється думка про існування аналогічних сфер життя в кіберпросторі, започатковано навіть термін «соціологія Інтернету»[5].

---

[1] Волков Б. С. Проблема воли и уголовная ответственность. Казань, 1965. С. 59; Бажанов М. И. Уголовное право Украины. Общая часть. Днепропетровск, 1992. С. 58; Дагель П. С. Классификация мотивов преступления и ее криминологическое значение. *Некоторые вопросы социологии и права* : материалы науч.-теорет. конф. Иркутск, 1967. С. 272; Герцензон А. А. Уголовное право. Общая часть. М. : РИО ВЮА, 1948. С. 343.

[2] Вербець В. В., Субот О. А., Христюк Т. А. Соціологія : навч. посіб. Київ, 2009. 550 с.

[3] Там само; Лавриненко В. Н., Кафтан В. В., Чернышова Л. И. Философия : учеб. и практикум / под ред. В. Н. Лавриненко. 7-е изд., перераб. и доп. М., 2015. С. 521.

[4] Лариненко В. Н., Кафтан В. В., Чернышова Л. И. Философия : учеб. и практикум / под ред. В. Н. Лавриненко. 7-е изд., перераб. и доп. М., 2015. С. 522; Сферы жизни общества: энциклопедия экономиста. URL: http://www.grandars.ru/college/sociologiya/sfera-obshchestva.html.

[5] Keith N., Hampton, Lauren F. Sessions, Eun Ja Her, Lee Rainie Social Isolation and New Technology. *How the internet and mobile phones impact Americans' social networks.* URL: http://www.pewinternet.org/2009/11/04/social-

В результаті аналізу сучасного контенту Інтернет-простору можна виділити такі умовні сфери суспільного життя суб'єктів відносин у кіберпросторі:

1) фінансово-економічна – пов'язана зі здійсненням розрахункових операцій та укладанням цивільно-правових угод;

2) соціальна – пов'язана з системою соціальних зв'язків між користувачами електронних мереж як суб'єктами кібернетичного соціуму з приводу реалізації ними своїх соціальних потреб (ідеться про організацію людиною свого дозвілля; задоволення освітніх, інтелектуальних та інших потреб, оплатно або безоплатно);

3) державно-політична – пов'язана із запровадженням так званого «електронного уряду», що має забезпечити надання органами влади послуг фізичним та юридичним особам, а також зі створенням централізованих баз даних, заснованих на технології забезпечення електронного документообігу в державних органах, у різних галузях промисловості й економіки, зокрема на підприємствах, що мають стратегічне значення для безпеки держави, під час організації та проведення виборів;

4) світоглядна (ідейна чи духовна) – пов'язана із впливом на масову свідомість система цінностей членів певної групи суспільства (за мовним критерієм, національною, расовою або релігійною приналежністю, іншою ознакою, наприклад, професією).

Мотив злочину кримінологи прямо пов'язують із цими сферами суспільного життя. Так, часто виділяють наступні групи мотивів: 1) політичні; 2) корисливі; 3) насильницько-егоїстичні; 4) анархістсько-індивідуалістичні; 5) легковажно-безвідповідальні та боязливо-малодушні. Або майже не моделюючи їх від сфер життя поділяли мотиви на: 1) суспільно-політичні; 2) соціально-економічні; 3) насильницько-егоїстичні; 4) легковажно відповідальні[1]. А. В. Савченко в кримінально-правовому дослідженні на підставі цих груп висновує про поділ мотивів злочинів залежно від найважливіших сфер життя людини на такі групи: 1) ідейні; 2) політичні; 3) релегійні;

---

isolation-and-new-technology/; Петренко-Лисак А. О. Соціальний простір у міждисциплінарному вимірі : навч. посіб. Київ, 2013. 400 с.

[1] Криминология / под ред. А. И. Долговой. М., 1997. С. 289.

4) націоналістичні[1]. В цих поглядах в одній класифікаційній системі автори намагаються уявити одразу всю сукупність мотивів.

Для цілей основної криміналістичної класифікації злочинів, вчинених у кіберпросторі, на групи потрібно виходити саме з традиційних сфер суспільного життя суб'єктів кіберпростору, класифікуючи 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) антидержавно-політичні мотиви, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі;

4) ідейні мотиви, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі.

Тож, на підставі класифікації мотивів можна класифікувати злочини, вчинені у кіберпросторі, на відповідні 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 антидержавно-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.

Звичайно ці групи злочинів характеризуються різноманітністю їх кримінально-правових ознак, тому виникає питання поділу на підгрупи в межах виділених груп злочинів, які традиційно утворюють визначену множину злочинів в одному акті розслідування. В цьому сенсі важливим є беззаперечне визнання в юридичній літературі наявності у суб'єкта вчинення злочину, крім основного мотиву, також й додаткових мотивів[2].

---

[1] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 31.

[2] Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. С. 31; Тарарухин С. А. Установление мотива и квалификация преступления. Київ, 1977. С. 21; Герцензон А. А. Уголовное право. Общая часть. М. : РИО ВЮА, 1948. С. 15.

З криміналістичної точки зору ці мотиви мають системоутворююче значення в технологіях вчинення злочинів, забезпечуючи досягення кінцевої злочинної мети, відповідно зумовлюють суб'єктний склад організованої групи, відповідний комплекс злочинів, обрання певного предмету посягання. На прикладі злочинів у сфері підприємництва А. Ф. Волобуєв підкреслював, що організовані злочинні групи вчиняють не окремі злочини, а їх комплекси, розробляючи цілі технології злочинної діяльності, які забезпечують їм систематичне одержання кримінального доходу. Комплексність досліджень у криміналістичній методиці, як доводить автор, обумовлюється саме дослідженням злочинних технологій[1].

Аналіз матеріалів судово-слідчої практики дозволяють наступним чином класифікувати злочини, вчинені у кіберпросторі.

1. Злочини, вчинені з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі, поділяються на такі підгрупи:

1.1. *злочини, що порушують встановлений порядок обігу певних речей*: придбання чи збут зброї, бойових припасів або вибухових речовин (ст. 263 КК України); незаконне придбання, збут наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів (ст. 307, 311); незаконні придбання, збут або використання спеціальних технічних засобів отримання інформації (ст. 359);

1.2. *злочини, що спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних розрахунків*: крадіжка (ст. 185 КК України); вимагання (ст. 189); шахрайство (ст. 190); привласнення, розтрата майна або заволодіння ним шляхом зловживання службовим становищем (ст. 191); незаконні дії з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення (ст. 200); зайняття гральним бізнесом (ст. 203-2); легалізація (відмивання) доходів, одержаних злочинним шляхом (ст. 209);

1.3. *злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції*: протидія законній господарській

[1] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 28.

діяльності (ст. 206); незаконне використання знака для товарів і послуг, фірмового найменування, кваліфікованого зазначення походження товару (ст. 229); незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю (ст. 231); розголошення комерційної або банківської таємниці (ст. 232).

2. Злочини, вчинені з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі, поділяються на підгрупи:

2.1. *злочини, пов'язані із насильницько-егоїстичними діями*: доведення до самогубства (ст. 120); погроза вбивством (ст. 129); вербування людини, вчинене з метою її експлуатації (ст. 149); розбещення неповнолітніх (ст. 156); завідомо неправдиве повідомлення про загрозу безпеці громадан, знищення чи пошкодження об'єктів власності (ст. 259); ввезення, виготовлення, збут і розповсюдження порнографічних предметів (ст. 301);

2.2. *інтелектуальне піратство та злочини, пов'язані із комунікаційними діями:* порушення авторського права і суміжних прав (ст. 176); порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер (ст. 163).

3. Злочини, вчинені з антидержавно-політичних мотивів, пов'язані з державно-політичною сферою відносин суб'єктів у кіберпросторі, поділяються на підгрупи:

3.1. *злочини, що пов'язані з антидержавницькими діями*:

3.1.1. злочини проти основ національної безпеки України: дії, спрямовані на насильницьку зміну чи повалення конституційного ладу або на захоплення державної влади (ст. 109); посягання на територіальну цілісність і недоторканність України (ст. 110); фінансування дій, вчинених з метою насильницької зміни чи повалення конституційного ладу або захоплення державної влади, зміни меж території або державного кордону України (ст. 110-1); державна зрада (ст. 111); диверсія (ст. 113); шпигунство (ст. 114);

3.1.2. злочини у сфері охорони державної таємниці (ст. 328, 330);

3.1.3. злочини проти судоустрою: незаконне втручання в роботу автоматизованої системи документообігу суду (ст. 376);

3.2. *злочини політико-ідеологічного спрямування*:

3.2.1. злочини проти виборчих прав і свобод (ст. 157, 158, 159, 159-1);

3.2.2. терористичний акт (ст. 258) та злочини, пов'язані з тероризмом (публічні заклики до вчинення терористичного акту (ст. 258-2); створення терористичної групи чи терористичної організації (ст. 258-3); фінансування тероризму (ст. 258-5);

3.2.3. пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного і націонал-соціалістичного (нацистського) тоталітарних режимів (ст. 436, 436-1).

4. Злочини, вчинені з ідейних мотивів, пов'язані зі світоглядною сферою життя суб'єктів відносин у кіберпросторі, поділяються на підгрупи:

4.1. *злочини, пов'язані із насильницько-дискримінаційними діями:* порушення рівноправності громадян залежно від їх расової, національної належності, релігійних переконань, інвалідності та за іншими ознаками (ст. 161); розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію (ст. 300);

4.2. *злочини, пов'язані із анархістськими діями у кіберпросторі*: злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України).

Остання з наведених підгруп є доволі специфічною через те, що злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можуть вчинятися як самостійно з анархістськими мотивами, так й поєднуватися зі злочинами інших класифікаційних систем. Така злочинна діяльність кваліфікується за сукупністю статей КК України. Саме відносно цієї підгрупи злочинів спостерігається тенденція до їх розосередження на різні групи та підгрупи традиційних злочинів, вчинених у кіберпросторі.

Вивчення матеріалів кримінальних проваджень означеної категорії засвідчує, що особа, котра вчиняє такі злочини, є користувачем, який здатний вільно працювати з програмними засобами комп'ютерної техніки. Вона має певний рівень кваліфікації, відповідний рівень технічної освіти в галузі комп'ютерної техніки, можливість доступу до спеціальної інформації або технологій. Щонайперше, це технічний персонал мереж і систем, які зазнали неправомірного втручання, розробники автоматизованих систем, їх

керівники, оператори, програмісти, інженери зв'язку, фахівці із захисту інформації та ін.[1] Діяльність останніх завжди найчастіше підлягає кваліфікації за сукупністю статей КК України, серед якої присутні статті розділу XVI КК України.

Тож, від обраного злочинцем специфічного набору операцій, які забезпечують існування кіберпростору (технічний чинник) залежить й ступінь складності традиційного злочину в кіберпросторі (вчинюваного з наведених нами мотивів). Розслідування такої злочинної діяльності вимагає особливої концентрації та організації зусиль правоохоронних органів.

Таким чином, при розслідуванні будь-якого традиційного злочину, що вчиняється у кіберпросторі, наприклад, шахрайства або збуту і розповсюдження порнографічних предметів, слідчій водночас повинен перевіряти наявність інших складів, чи то злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України), чи злочинів відповідної класифікаційної підгрупи, стосовно нашого прикладу – серед злочинів, що спрямовані на заволодіння чужим майном, та злочинів, пов'язаних із насильницько-егоїстичними діями в кіберпросторі.

Предмет доказування у такому комплексі злочинів буде значно ширшим, що у свою чергу зумовлює необхідність розроблення комплексної методики розслідування злочинів, вчинених у кіберпросторі. Підґрунтям для її розроблення уявляється криміналістична класифікація досліджуваних злочинів, здійснена з підстав мотивів їх вчинення на першому рівні та злочинної технології на другому рівні.

[1] Мазуров В. А. Компьютерные преступления: классификация и способы противодействия : учеб.-практ. пособие. М., 2002. С. 120.

РОЗДІЛ 2
КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

2.1. Структура криміналістичної характеристики злочинів, вчинених у кіберпросторі

Словом «характеристика» (від др.-грецької «відмітний») позначають опис, визначення істотних, характерних особливостей, ознак будь-чого[1]. Оскільки злочинність вивчається з точки зору різних юридичних наук, протягом розвитку наукової думки категорія «характеристика злочину» використовується з позиції оперативно-розшукової, кримінологічної, кримінально-правової або криміналістичної наук. Але саме «криміналістична характеристика злочину» піддавалась критиці з боку науковців та нерозумінням її значення з боку практиків.

Р. С. Бєлкін з цього приводу писав, що склалося парадоксальне становище: сам по собі комплекс відомостей про злочин, який складає зміст криміналістичної характеристики, нічого нового для науки і практики не надав[2]. Далі автор акцентувався на тому, що комплекс відомостей про злочин, іменований криміналістичною характеристикою, все ж таки набуває практичного значення лише у тих випадках, коли між його складовими встановлено кореляційні зв'язки та залежності. Б. В. Щур в результаті анкетування слідчих говорить про непоінформованість слідчих відносно кореляційних зв'язків багатьох елементів у структурі криміналістичної характеристики[3]. Однак, ця проблема стосується питання якості впровадження криміналістичних розробок у практику конкретних правоохоронних органів, і жодним чином не нівелює значення самої криміналістичної характеристики окремого виду злочинів у відповідній методиці розслідування.

---

[1] Новий тлумачний словник української мови : в 3 т. / уклад.: В. Яременко, О. Сліпушко. Київ : Аконіт, 2006. Т. 3. 926 с.

[2] Белкин Р. С. Криминалистика и проблемы сегодняшнего дня. *Злободневные вопросы российской криминалистики.* М. : НОРМА, 2001. С. 221.

[3] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. С. 199.

Проведений нами аналіз наукових робіт (статей, дисертаційних досліджень, монографій, інших публікацій), дозволяє впевнено констатувати, що в жодному дослідженні з проблем криміналістичної методики науковці не обходять увагою питання криміналістичної характеристики злочинів. І цьому є логічне пояснення.

В теорії пізнання для ефективного впливу на певний об'єкт будь-якій людині потрібні знання загального, що повторюється у безлічі аналогічних предметів або явищ, знання необхідного, що наступає за відповідних умов, нарешті, потрібне знання законів, яким підкоряється функціонування і розвиток об'єкту, його суті через загальне[1]. Ця сторона пізнавального процесу реалізується шляхом застосування в єдності діалектичних методів пізнання, зокрема дедуктивного та індуктивного методів. Перший – це рух в процесі пізнання одиничного від загального до особливого, що здатне забезпечити отримання істинного знання про одиничне; другий – навпаки, від одиничного до загального, що сприяє закріпленню в поняттях тих або інших загальних властивостей, визначенню закономірності зв'язків досліджуваних об'єктів[2].

Злочин виступає об'єктом пізнання слідчого[3]. Слідчий в ході пізнання конкретного акта вчинення злочину повинен з усієї інформації про подію, що пізнається, обрати ту, що набуває особливого значення для встановлення об'єктивної дійсності події, впливає на організацію та планування цієї діяльності. Тому в процесі розслідування важливого значення набувають не лише інтелектуальні та творчі здібності слідчого, а й попередньо накопичені емпіричним шляхом відомості щодо вчинення злочинів аналогічного виду. Застосування індуктивного методу як методу наукового пізнання забезпечуватиме процес розслідування такими відомостями про злочин, тим самим дозволяючи слідчому отримати знання щодо закономірних зв'язків таких відомостей. В криміналістичній науці цей шлях пізнання злочину й окреслюється категорією «криміналістична характеристика злочину».

---

[1] Шептулин А. П. Диалектический метод познания. М. : Политиздат, 1983. С. 103.

[2] Там само. С. 137.

[3] Коновалова В. О., Шепітько В. Ю. Юридична психологія : підручник. 2-ге вид., переробл. і доповн. Харків : Право, 2008. С. 74.

Це поняття, введене у 60-ті роки XX століття криміналістом О. Н. Колесніченком[1], згодом стало одним з основних в криміналістичній методиці. Однак, до його визначення науковці підходять по-різному. О. Н. Колесніченко і В. Є. Коновалова в результаті аналізу наукових поглядів щодо криміналістичної характеристики злочину визначили це поняття як систему відомостей (інформації) про криміналістичнозначущі ознаки злочинів певного виду, яка відбиває закономірні зв'язки між ними і слугує побудові і перевірці слідчих версій в розслідуванні конкретних злочинів[2]. Підтримуючи в цілому таке визначення Л. Я Драпкін, В. П. Бахін та інші криміналісти наголошували також про типовість таких криміналістично значущих ознак певного виду (групи) злочинів[3].

В. І. Шиканов криміналістичну характеристику злочинів представляв як наукову абстракцію, що відображає в основному на статистичному рівні дані про прийоми підготовки і способи вчинення окремих видів (підвидів) злочинів[4]. В цьому контексті справедливо наголошує О. В. Одерій, що абстракція визначається як те, що не має практичного застосування, що не зовсім кореспондує з природою й призначенням розглядуваної категорії[5].

Здійснюючи науковий пошук щодо формування поняття та структури криміналістичної характеристики злочину, В. А. Журавель прийшов до думки, що криміналістична характеристика злочину являє собою інформаційну модель, в якій відбиваються типові ознаки, тобто ті, що притаманні даному масиву злочинів, і специфічні, котрі

[1] Колесниченко А. Н. Научные и правовые основы расследования отдельных видов преступлений : автореф. дис. ... д-ра юрид. наук : 12.00.09. Харьков, 1967. 42 с.

[2] Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. ин-т, 1985. С. 16–20.

[3] Бахін В., Лук'янчиков Б. Склад і призначення криміналістичної характеристики злочинів. *Часопис Донецького університету.* 2000. Вип. 1 (4). С. 40; Драпкин Л. Я. Предмет доказывания и криминалистические характеристики преступлений. *Криминалистические характеристики в методике расследования преступлений.* 1978. Вып. 69. С. 17–18.

[4] Шиканов В. И. Проблемы использования специальных познаний и научно-технических новшеств в уголовном судопроизводстве : автореф. дис. … д-ра юрид. наук : 12.00.09. М., 1980. С. 18.

[5] Одерій О. В. Криміналістична характеристика злочинів проти довкілля: проблеми побудови та використання. *Теорія та практика судової експертизи і криміналістики.* 2012. № 3. С. 53

дозволяють відокремити його від інших груп злочинів[1]. При цьому головною відмінністю цієї моделі науковець вважає те, що всі елементи, які входять до її складу, становлять певну систему і розглядати їх у відриві один від одного недоцільно. З позицій акценту на ролі елементів в цій системі, визначенням типових та специфічних ознак злочину певного виду, автор розширює зміст поняття, наданого М. В. Салтевським, А. В. Старушкевичем та багатьма іншими, які визнавали криміналістичну характеристику інформаційною моделлю лише як якісно-кількісний опис або систему типових ознак виду (групи) злочинів[2] або конкретного злочину[3]. Остання теза щодо криміналістичної характеристики конкретного злочину взагалі справедливо спростовується більшістю науковців (А. Ф. Волобуєвим, В. А. Журавлем, Б. В. Щуром та іншими).

Різноманітність поглядів вчених щодо категорії «криміналістична характеристика злочину» зумовлює відсутність єдності криміналістів у питанні її структури. Майже всі вчені, в коло інтересів яких входили питання методики розслідування злочинів, з власним аргументуванням пропонували той або інший перелік типових елементів криміналістичної характеристики, які різнилися як за кількісними, так й за якісними показниками. С. П. Мітричєв виділяв лише три основні взаємопов'язані елементи: 1) засіб скоєння злочину; 2) сліди, які оставив злочинець на місці скоєння злочину; 3) особа злочинця[4]. Р. С. Бєлкін – 5 типових елементів: 1) типові слідчі ситуації, під якими розуміють характер вихідних даних про злочин; 2)спосіб вчинення та приховування злочину; 3) типові матеріальні сліди злочину і можливі місця знаходження; 4) характеристика особи злочинця; 5) обстановка злочину (місто, час і інші обставини)[5].

---

[1] Журавель В. Криміналістична характеристика злочинів: проблеми формування та застосування. *Вісник Національної академії правових наук.* 2008. № 4. С. 209.

[2] Салтевский М. В Криминалистическая характеристика: структура, элементы. *Специализированный курс криминалистики :* учебник. Киев, 1987. С. 310.

[3] Старушкевич А. В. Криміналістична характеристика злочинів : навч. посіб. Київ : Правник, 1997. С. 12.

[4] Митричев С. П. Методика расследования отдельных видов преступлений : лекции. М. : Б.и., 1973. С. 13–14.

[5] Белкин Р. С. Курс криминалистики : в 3 т. М. : Юрист, 1997. Т. 3 : Криминалистические средства, приемы и рекомендации. С. 312.

Г. А. Матусовський характеризував злочини через шість елементів: 1) особа злочинця; 2) способи готування до злочину; способи вчинення злочину; способи приховування злочину (маскування злочинних дій); 3) особа потерпілого; 4) предмет посягання; 5) обстановка вчинення злочину; 6) наслідки у вигляді будь-яких змін[1]. В. В. Тіщенко – також через шість елементів, але якісно різних: 1) дані про суб'єкта (суб'єктів) злочину (злочинної діяльності); 2) дані про цілі і мотиви злочину; 3) дані про об'єкт злочинного посягання; 4) дані, що характеризують обстановку злочину; 5) дані про механізм (процес) злочинної діяльності; 6) дані про результат і наслідки злочинних дій[2]. О. Н. Колесниченко та В. О. Коновалова – вісім головних елементів криміналістичної характеристики: 1) спосіб злочину; 2) місце та обстановку; 3) час вчинення злочину; 4) знаряддя та засоби; 5) предмет посягання; 6) особу потерпілого; 7) особу злочинця; 8) сліди злочину (у широкому розумінні)[3]. Подібних прикладів структури криміналістичної характеристики можна навести безліч, особливо якщо остання розробляється в контексті окремого виду або групи злочинів. Отже, криміналістична характеристика виду (роду) злочинів – це результат аналізу безлічі одиничних випадків злочинів[4], в результаті якого виділяються конкретні криміналістичнозначущі елементи, враховуючи наявні між ними закономірні зв'язки.

Б. В. Щур зробив спробу систематизувати різні підходи щодо структури криміналістичної характеристики та запропонував наступний елементний склад характеристики будь-якого виду злочину: 1) спосіб злочину (спосіб приготування, спосіб вчинення, спосіб приховування злочину); 2) предмет злочинного посягання; 3) умови вчинення злочину (час, місце, обстановка); 4) знаряддя та засоби вчинення злочину; 5)

[1] Матусовський Г. А. Загальні положення методики розслідування злочинів. *Криміналістика :* підручник / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2001. С. 370–371.

[2] Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. С. 62–84.

[3] Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. ин-т, 1985. С. 22.

[4] Фокина А. А. Роль криминалистической характеристики преступлений в укреплении связи науки криминалистики и практики расследования. *Криминалистика и судебная экспертиза.* 1990. Вып. 41. С. 18.

особа злочинця; 6) особа потерпілого (жертви); 7) сліди злочину[1]. Незважаючи на аналіз більшості існуючих сьогодні поглядів з цієї проблематики, криміналіст не претендує на безапеляційність свого переліку. На думку науковця запропоновані ним найменування мають умовне значення і поєднують певні типові криміналістичнозначущі ознаки.

Абсолютно переконливою нам уявляється позиція А. Ф. Волобуєва, який шляхом визначення об'єкта і предмета криміналістичної методики, по суті, вирішує проблему визначення структури криміналістичної характеристики будь-якої групи або виду злочинів. Чітке визначення об'єкта і предмета дослідження криміналістичної методики є необхідною умовою однозначного тлумачення окремих її наукових положень, структури її змісту[2]. Визначаючи закономірності механізму злочинів окремого виду одним з самостійних предметів криміналістичної методики, А. Ф. Волобуєв пише: «За своїм змістом криміналістична характеристика – це знання (відомості), накопичені в результаті вивчення механізму вчинення злочинів окремого виду, його внутрішніх зв'язків і залежностей. Тому її структура як система знань детермінована структурою механізму вчинення злочинів як об'єкту пізнання. З урахуванням вищевикладеного криміналістична характеристика злочинів може бути визначена як структурний елемент окремої методики розслідування, що являє собою систему відомостей про елементи механізму вчинення злочинів певного виду чи групи, в яких відбиваються закономірні зв'язки між цими елементами і які використовуються для розробки наукових рекомендацій, а також побудови і перевірки версій при розслідуванні конкретних злочинів»[3]. Криміналістична характеристика злочинів окремих видів є відображенням механізму їх вчинення[4]. Тож,

[1] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. С. 201.

[2] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 49.

[3] Там само. С. 49–50.

[4] Волобуєв А.Ф. Механізм злочину та його зв'язок з концептуальними положеннями криміналістики: монографія. Кривий Ріг: Вид. Р. А. Козлов, 2019. - 122 с.

елементами криміналістичної характеристики злочинів автор визнає відомості про елементи механізму їх вчинення.

Більшість криміналістів намагаються визначити типові елементи механізму вчинення злочину шляхом визначення самого поняття «механізм злочину». Так, Р. С. Бєлкін механізмом злочину вважав складну, багатокомпонентну динамічну систему, що утворюється наступними елементами: 1) діями суб'єкта злочину, спрямованими на досягнення певного злочинного результату щодо конкретного об'єкта злочинного посягання; 2) діями потерпілого, поведінкою осіб, які стали випадковими (активними чи пасивними) учасниками події, що відбулася за певних умов і обставин, сукупність яких детермінує спосіб вчинення злочину, зумовлює характер і зміст зв'язків та відносин між суб'єктом злочину й предметом зазіхання, між діями учасників і злочинним результатом, між співучасниками злочину, між учасниками та матеріальним середовищем[1]. П. Д. Біленчук, А. П. Гель, М. В. Салтевський, Г. С. Семаков пишуть, що механізм злочину є системою взаємодій реальних об'єктів матеріального світу і тому охоплює явища, події та реальні факти, людей, моменти часу, ділянки місцевості та простору, предмети, речі, механізми й комп'ютерні системи, тварин, об'єкти рослинного світу тощо, які є його елементами[2]. В. К. Гавло під так званим «криміналістичним механізмом злочину» розуміє взаємодіючу систему елементів криміналістичної характеристики, яка відбиває процес вчинення, утворення його слідів, що мають значення для встановлення істини у справі[3]. А. М. Кустов, узагальнюючи всі наукові підходи, справедливо визнає механізм злочину системою процесів взаємодії учасників злочину, як прямих, так й опосередкованих, між собою та матеріальним середовищем, пов'язаних з використанням відповідних знарядь, засобів

[1] Криминалистика / [Т. В. Аверьянова, Р. С. Белкин, И. А. Возгрин и др.] ; под ред. Р. С. Белкина. М. : Акад. МВД РФ, 1995. Т. 1 : История, общая и частные теории. С. 83.

[2] Біленчук П. Д., Гель А. П., Салтевський М. В., Семаков Г. С. Криміналістика (криміналістична техніка) : курс лекцій. Київ : МАУП, 2001. С. 3.

[3] Гавло В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск : Томск. ун-т, 1985. С. 191.

і інших окремих елементів обстановки[1]. Тож, з позицій бачення такої різноманітності елементів, процесів та чинників, що утворюють механізм злочину, в криміналістиці сформувались два погляди щодо конкретизації співвідношення механізму вчинення злочину з криміналістичною характеристикою.

Перший, по суті, є інформаційним підходом, коли відомості про типовий механізм злочину вказують в ряду інших елементів структури криміналістичної характеристики, як-от відомості про спосіб вчинення злочину, типові сліди, обстановку тощо (Р. С. Бєлкін, І. О. Возгрін, Г. А. Густов, Л. Я. Драпкін та інші), іноді ведеться мова про можливість заміни в цьому переліку «способу вчинення злочину» на «механізм» (А. М. Кустов). Другий є функціональним підходом, коли відомості про елементи механізму його вчинення складають елементи криміналістичної характеристики злочину (А. Ф. Волобуєв, В. І. Гончаренко, Г. А. Кушнір, О. Г. Головін та інші)[2]. Звертаючись до положення системного аналізу щодо первинності функції по відношенню до структури[3], виправданим вважаємо саме останній. До того ж, як справедливо наголошує А. Ф. Волобуєв, криміналістика акцентується саме на функціональному аспекті протиправної діяльності як системи детермінованих діянь і відносин на шляху досягнення злочинної мети (наставання злочинного результату)[4].

---

[1] Кустов А. М. Криминалистика и механизм преступления : цикл лекций. М. ; Воронеж : МОДЭК, 2002. С. 24.

[2] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 420 с.; Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. ин-т, 1985. 92 с.; Головин А. Ю., Берестнев М. А. Современные подходы к пониманию криминалистической характеристики преступлений. *Криміналістика XXI століття :* матеріали Міжнар. наук.-практ. конф. (25–26 листоп. 2010 р.). Харків : Право, 2010. С. 250–254; Гончаренко В. И., Кушнир Г. А., Подпалый В. Л. Понятие криминалистической характеристики преступлений. *Криминалистика и судебная экспертиза :* респ. межведом. науч.-метод. сб. Киев : Вища шк., 1986. Вып. 33. С. 5.

[3] Дивак М. П. Системний аналіз : метод. посіб. Тернопіль, 2004. С. 20; Лузгин И. М. Моделирование при расследовании преступлений. М., 1981. 152 с.

[4] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 48.

Тож, механізм вчинення певного виду (групи) злочинів конкретизується через типові елементи її криміналістичної характеристики, які, знаходячись у взаємозв'язку, утворюють останню як систему типових та специфічних ознак певної групи (видів) злочинів. Останні є найбільш значущими для процесу розслідування виду (групи) злочину, тобто забезпечуватимуть слідчому можливість висунення загальних і окремих версій, планування розслідування, а також цілеспрямованого пошуку слідів злочину, злочинця, потерпілого, сприятимуть дослідженню всіх обставин, що підлягають доказуванню. Прагматичне значення криміналістичної характеристики злочинів зумовлює її розгляд як одного з складових елементів криміналістичної методики розслідування будь-якого виду (групи) злочинів.

Криміналістична характеристика комплексних злочинів, якими визнаємо злочини, вчинені у кіберпросторі, охоплює ознаки множини злочинів, яка визначається певною специфікою – ознаками, що дозволяють відокремити цей комплекс злочинів від інших злочинів.

Використання кіберпростору для вчинення традиційного злочину суттєво детермінує механізм його вчинення. Застосування технологій кіберпростору (телекомунікаційних мереж, комп'ютерних систем й пристроїв), як знарядь досягнення протиправної мети призводить до утворення специфічних змін (слідів в криміналістичному сенсі) в самому кіберпросторі як інформаційному просторі взаємодії людей. Тому ознаки обстановки вчинення злочину та типові його сліди отримують в криміналістичній характеристиці значення *специфічних ознак* злочинів, вчинених у кіберпросторі. Вони зумовлюють схожість всіх класифікаційних груп та підгруп досліджуваної категорії злочинів. Втім, для побудови повної криміналістичної характеристики таких злочинів потрібно визначити закономірні зв'язки між усіма типовими ознаками злочину. Систематизація останніх здійснюватиметься в межах типових елементів механізму вчинення цієї категорії злочинів.

Механізм вчинення злочинів в кіберпросторі не піддавався системному науковому дослідженню, що зумовлено, як ми вже визначали раніше, складністю у визначенні суті цієї категорії злочинів.

З кримінально-правових позицій В. В. Марков, розглядаючи механізм злочинів в кіберпросторі, пише про ознаки об'єктивної сторони окремих видів таких злочинів, зокрема про засоби та способи

вчинення злочину, а також електронну природу предмета посягання[1], що в цілому відповідає розумінню механізму злочину в кримінальному праві.

У криміналістичних колах теж велась мова про механізми вчинення окремих видів злочинів цієї категорії, при цьому обмежувались характеристикою окремих елементів механізму, без спроби отримати системне уявлення про вчинення відповідного злочину. В контексті механізму вчинення комп'ютерних злочинів у одному з перших вітчизняних посібників з цієї тематики науковці визнають неправомірний доступ до автоматизованих систем або мереж початковим етапом вчинення інших злочинів у сфері комп'ютерної інформації та приділяють увагу характеристиці таких елементів механізму: місце вчинення злочину, предмет посягання, спосіб вчинення, особа злочинця та мотив[2]. В. М. Бутузов, В. Д. Павловський. Л. П. Скалозуб, К. В. Тітуніна, В. П. Шеломенцев в результаті узагальнення матеріалів практики та анкетувань висновують про існування «основних елементів криміналістичної характеристики злочинів у сфері використання ЕОМ, систем, комп'ютерних мереж та мереж електрозв'язку», до яких відносять: предмет безпосереднього посягання; спосіб вчинення в широкому розумінні та типову обстановку[3]. В такому розумінні може виникнути питання про існування й додаткових елементів характеристики. Пізніше ці науковці в розширеному авторському колективі роблять наголос на визначенні ними загальних рис (ознак) вчинення злочинів у сфері високих інформаційних технологій, зокрема: транскордонність злочинних діянь; високий рівень латентності; вчинення злочинів у електронному середовищі; унікальність способів вчинення та висока технічна забезпеченість злочинної діяльності; висока гнучкість та

[1] Марков В. В. Про механізм скоєння злочинів у кіберпросторі та особливості їх кваліфікації. *Південноукраїнський правничий часопис.* 2013. № 1. С. 112–115.

[2] Комп'ютерна злочинність : навч. посіб. / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. Київ : Атіка, 2002. С. 179–180.

[3] Документування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за заг. ред. Л. П. Скалозуба, І. В. Бондаренко. Київ, 2010. 245 с.

оперативність кримінальних структур[1]. Таке бачення лише активізує науковий пошук з проблематики визначення типових елементів механізму вчинення досліджуваного виду злочинів.

О. І. Мотлях називає механізм вчинення комп'ютерних злочинів одним з предметів свого дисертаційного дослідження. Про механізм висновує з позицій криміналістичної характеристики як інформаційної моделі, що вміщує типові ознаки наступних елементів: способи скоєння злочинів; слідова картина; особа злочинця, мотиви і мета скоєння злочину; деякі обставини (місце, час, обстановка)[2]. Однак, по суті, механізм вчинення злочину автором не розкривається, адже зовсім не приділяється увага взаємозв'язкам між елементами характеристики злочинів. Нажаль, такий недолік вбачається у багатьох робіт подібної тематики[3].

З кримінально-процесуальних поглядів А. І. Журба звужує механізм вчинення комп'ютерного злочину до розуміння під ним комплексу різноманітних комп'ютерних технології, що зумовлюється свободою дій обвинуваченого у підходах до програмування, у створенні або використанні нових індивідуальних методик та інструментів скоєння злочину[4].

Досить цікавий підхід до визначення механізму злочинної діяльності у сфері комп'ютерної інформації використано у

[1] Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. С. 88–94.

[2] Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. С. 41.

[3] Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2009. 22 с.; 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. Київ, 2004. 214 с.

[4] Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. С. 110.

дисертаційному дослідженні росіянином С. В. Кригіним[1]. Він розглядає криміналістичну характеристику злочинів, вчинених у сфері комп'ютерної інформації, через криміналістичні моделі такої злочинної діяльності, структура і зміст яких обумовлюється можливістю їх обробки математичними методами для висунення версій при розслідуванні конкретних злочинів. Використовуючи метод «дерево класифікацій», виявляє стійкі (закономірні) зв'язки між складовими (елементами) моделі злочинної діяльності, що дає можливість побудувати систему типових криміналістичних версій про подію та особу злочину. Про наявність певної типової моделі злочинної діяльності свідчить сукупність наступних ознак (елементів) типової моделі: мотив; сфера діяльності злочинця; відношення до предмета посягання; організація; час та місце злочину; комп'ютеризація об'єкта; спосіб захисту інформації; спосіб злочину; предмет посягання; принцип дії; наслідки для системи[2]. В основі визначення таких складових моделі знаходиться деталізація автором чотирьох типових елементів злочинної діяльності, зокрема: 1) суб'єкта злочину; 2) ситуації вчинення злочину (по суті, обстановка); 3) способу вчинення злочинних дій; 4) слідів (ознак) злочину[3]. Попри наявність деяких недостатньо обґрунтованих позицій щодо формулювання окремих елементів моделі злочину, в цілому підхід С. В. Кригіна можна визнати достатньо конструктивним. Тому, вважаємо, що в основу криміналістичної концепції механізму вчинення досліджуваної нами категорії злочинів потрібно покласти закономірності функціонування такої злочинної діяльності.

Будь-яка людська діяльність може мати дві форми: теоретичну та предметну (практичну). Остання є активним відношенням суб'єкта до оточуючого середовища, зміст якого складає зміна та перетворення цього середовища відповідно цілі суб'єкта[4]. Різновидом предметної діяльності в кримінально-правовій науці вважається злочинна діяльність. А. Ф. Зелінський, виходячи з обов'язкової доцільності

[1] Крыгин С. В. Расследование преступлений, совершаемых в сфере компьютерной информации : дис. … канд. юрид. наук : 12.00.09. Н. Новгород, 2002. 200 с.

[2] Там само. С. 108–109.

[3] Там само. С. 63.

[4] Юдин Э. Г. Системный подход и принцип деятельности. М., 1978. С. 267.

практичної людської діяльності, приходить до висновку про те, що злочини, вчинені імпульсивно або з необережності, не можуть утворювати злочинну діяльність [1]. На думку А. М. Кустова діяльність – це процес, що спонукається потребою (мотивом) та спрямовується усвідомленою метою[2]. Тож, вмотивованість є обов'язковою ознакою злочинної діяльності.

Особливо складний, технологічний та організований характер злочинів, вчинених у обстановці кіберпростору, дозволяє вважати їх завжди вмотивованими. Також, у попередньому підрозділі роботи доведено, що найбільш значущим критерієм для криміналістичної класифікації таких злочинів є саме мотив їх вчинення. Це дає підстави говорити про злочини, вчинені у кіберпросторі, як злочинну діяльність.

Механізм будь-якої діяльності складається з її мотиву, загальної цілі, програми дій, прийняття рішення, усвідомлення критеріїв успіху та моделі умов діяльності, інформації про результат, рішення щодо корекції поведінки[3]. З таких позицій злочин – це ланка в процесі взаємодії двох систем – людини і навколишнього світу[4]. Матеріальне утворення «навколишній світ» уособлює собою предмет злочинного посягання; дії, спрямовані на досягнення бажаного злочинного результату, зміни (сліди), що утворились в результаті дії; матеріальне утворення «людина» – це, по суті, злочинець або організована група осіб, їх мотиви та цілі вчинення злочину. Взаємодіючи системи утворюють безліч закономірних зв'язків. Тому Ю. М. Антонян, В. П. Бахін, В. П. Голубєв, А. В. Дулов, Г. Х. Єфремова, В. О. Коновалова, А. М. Кустов, А. Р. Ратинов, О. В. Челишева, Ю. В. Чуфаровський, Г. Г. Шиханцов та багато інших криміналістів вказували на структурність злочинної діяльності. Аналіз існуючих наукових позицій свідчить, що використання системно-структурного підходу до визначення змісту злочинної діяльності є виваженим. Загалом виділяють два рівні злочинної діяльності:

---

[1] Зелинский А. Ф. Осознаваемое и неосознаваемое в преступном поведении. Харьков : Вища шк., 1986. С. 120.

[2] Кустов А. М. Криминалистика и механизм преступления : цикл лекций. М. ; Воронеж : МОДЭК, 2002. С. 28.

[3] Зелинский А. Ф. Осознаваемое и неосознаваемое в преступном поведении. Харьков : Вища шк., 1986. С. 121.

[4] Зав'ялов С. М. Способи вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. С. 17.

1) діяльність як сукупність (комплекс) поступових дій, об'єднаних загальним задумом в межах окремого злочину;

2) діяльність як процес поступової заміни дій в межах декількох злочинів, об'єднаних єдиним злочинним замислом[1].

Аналіз матеріалів судово-слідчої практики щодо розслідування злочинів, вчинених у кіберпросторі, дозволяє визначити, що зі змістовної сторони близько половини таких злочинів є одиничними злочинами, що повторюються за способами скоєння та входять до визначених нами класифікаційних підгруп аналізованої категорії злочинів; інша половина злочинів – це комплекс органічно взаємопов'язаних злочинів, в якому злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України) виступають обов'язковою умовою досягнення злочинного результату. Про подібний зв'язок злочинів писав А. Ф. Волобуєв, наголошуючи про наявність між злочинами такого зв'язку, що поєднує їх у єдиний ланцюг злочинної поведінки. Нехтування таким зв'язком не приведе до досягнення наміченого злочинного результату[2].

Вивчення матеріалів кримінальних проваджень дозволяє ствердити, що можливість досягнення кінцевої злочинної мети, прямо не пов'язаної з спричиненням шкоди нормальному функціонуванню кіберпростору, – як-от заволодіння об'єктами інтелектуальної власності, платіжними засобами, матеріальними цінностями, – забезпечуватиметься існуванням типових технологій вчинення злочинів у кіберпросторі. Використання технологій злочинної діяльності є особливо характерним для двох класифікаційних груп злочинів: 1) вчинених із корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі;

[1] Кустов А. М. Криминалистика и механизм преступления : цикл лекций. М. ; Воронеж : МОДЭК, 2002. С. 33. 304 с.; Лубин А. Ф. Механизм преступной деятельности: развитие концепции. *Белкинские чтения «Памяти Учителя».* Н. Новгород, 2001. С. 13–22; Романов С. Ю. Обман як спосіб злочинної діяльності : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків, 1998. 16 с.

[2] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. С. 54.

2) вчинених з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі.

Наведемо приклад однієї з поширених технологій корисливої злочинної діяльності у кіберпросторі[1]. Так, в 2012 році у м. Черкасах гр. К., користуючись послугами інтернет-провайдера ПрАТ «Київстар Дж.Ес.Ем.», інсталював у свій комп'ютер шкідливий програмний засіб, що призначений для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації, шляхом прихованого перехоплення натискань клавіш на клавіатурі, моніторингу буферу обміну, запису знімків екрану монітору (скріншотів), моніторингу відвідуваних веб-сайтів з послідуючим відправленням такої інформації на конкретну електронну скриньку. Достовірно знаючи про шкідливість вказаного програмного засобу, К. налаштував його таким чином, щоб за його допомогою можна було здійснити несанкціоноване втручання в роботу комп'ютерів інших користувачів мережі «Інтернет». Використовуючи свій комп'ютер, розповсюдив вказаний програмний засіб шляхом розміщення в мережі Інтернет під виглядом комп'ютерної програми для викрадення ігрових грошей в он-лайн грі «FG» на спеціально створеному інтернет-сайті домену «.ru». 23 жовтня 2011 р. о 00.59 годині К., реалізуючи свій злочинний умисел, направлений на несанкціоноване втручання в роботу комп'ютера гр. О., діючи умисно, за місцем своєї реєстрації та проживання, використовуючи свій комп'ютер, через мережу Інтернет, за допомогою паролю, який він незаконно отримав внаслідок роботи розповсюдженого ним в мережі програмного засобу, здійснив несанкціоноване проникнення до електронної поштової скриньки гр.О. в результаті чого отримав доступ до відомостей про електронний гаманець гр.О. та його особисту переписку. З метою таємного викрадення, належних О. грошових коштів К. створив в електронній грошовій системі додатковий електронний гаманець, зареєстрував його на своїй електронній поштовій скоринці, після чого, використовуючи свій комп'ютер, через мережу Інтернет здійснив без відома О., незаконний переказ грошових коштів з електронного гаманця О. на свій додатковий електронний гаманець**.** Однак, довести

[1] Вирок Соснівського районного суду м. Черкаси від 19 листоп. 2012 р. Справа № 1-443/12. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/27536021.

до кінця свій злочинний намір, направлений на таємне викрадення чужого майна він не зміг, оскільки О., отримавши повідомлення про переказ, встиг використати можливості сервісної служби «Арбітраж WebMoney», наклавши на переказ «арешт», що унеможливило їх відчуження К. Своїми діями, вчиненими з корисливих мотивів, останній вчинив злочини, передбачені ч.1 ст. 361-1, ч. 2 ст. 361, ч. 1 ст. 185 КК України.

Слід констатувати, що подібну технологію злочинної діяльності використовують й організовані групи, які типово ускладнюють її транскордонним компонентом або створенням фіктивних суб'єктів підприємницької діяльності для легалізації отриманих в результаті злочину грошових коштів. Як приклад можна навести діяльність організованої групи осіб у м. Києві в 2013 році[1]. Згідно з розподіленими злочинними ролями, невстановлені особи несанкціоновано втручалися в роботу комп'ютерів юридичних осіб, на яких було встановлено програмне забезпечення дистанційного доступу до рахунків, відкритих у банківських установах (система «Клієнт-Банк»). Отримавши доступ до інформації, яка на них зберігається й обробляється, злочинці здійснювали перерахування коштів загальною сумою 357 303,44 грн на рахунок фіктивно створеного підприємства. В ході слідства було встановлено лише особу, на яку було відкрито з її відома фіктивне підприємство з метою переведення коштів у готівкову форму.

Дослідження обраної нами категорії злочинної діяльності буде неповним, якщо залишати поза уваги специфіку вчинення одиничних злочинів у кіберпросторі та зв'язки між ними. В цьому сенсі вважаємо, потрібним звернутися до так званого «зв'язку об'єктів за розвитком». Адже для злочинної діяльності також характерним визнається «зв'язок розвитку злочину»[2]. Розвиток – це безповоротна, спрямована, якісна зміна того або іншого об'єкту, що відбувається на певній відносно стійкій основі, що виникла у попередній період[3]. Якщо ж особа систематично вчиняє злочин певного виду, маючи один й той самий

[1] Вирок Колегії суддів Печерського районного суду м. Києва від 24 берез. 2016 р. Справа № 757/27385/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56716129.

[2] Зелинский А. Ф. Осознаваемое и неосознаваемое в преступном поведении. Харьков : Вища шк., 1986. С. 124.

[3] Морозов В. Д. Проблема развития в философии и естествознании: историко-философский очерк. Минск : Вышейшая шк., 1969. С. 6-7.

мотив, то є сенс говорити й про вчинення множини певної групи (підгрупи) злочинів із застосуванням типових способів їх вчинення. Спосіб злочину взагалі найтісніше взаємопов'язаний з властивостями інших елементів злочинної події[1]. Сам спосіб вчинення злочину для одиничних (простих) злочинів у кіберпросторі буде виступати головною якісною характеристикою діяльності злочинця. Наприклад, одним з найпоширених способів вчинення шахрайства у кіберпросторі стало сьогодні розміщення в мережі Інтернет неправдивої інформації про продаж різних товарів з метою заволодіння грошовими коштами імовірних покупців. Так, в Дніпровській області протягом 2014-2015 років М. з використанням комп'ютера, підключеного до глобальної мережі Інтернет, маючи на сайті http://skuters.hol.es/index.php власний Інтернет-магазин, зареєстрований на його ім'я, офіційно займаючись перепродажем двоколісних скутерів за завищеними цінами, реєстрував, використовуючи різні номери мобільних телефонів, оголошення на Інтернет-ресурсі компанії ТОВ «Ємаркет Україна» «Olx.ua» щодо продажу двоколісних скутерів без наміру поставляти останні замовникові. Для заволодіння грошима замовників з призначенням «предоплата» М. використовував карткові рахунки малознайомих осіб та електронні гаманці[2]. Розміщення забороненої інформації у соціальних мережах та адміністрування відповідних груп соціальних мереж здебільше стає типовим способом вчинення різноманітних злочинів з антидержавно-політичних мотивів. Наприклад, розповсюджуються матеріали із закликами про захоплення державної влади, здійснюється вербування агентури для іноземної розвідки, активно сприяють діяльності терористичних організацій.

В практичному плані закономірне ускладнення способів вчинення наступного зі злочинів будуть свідчити про інтелектуальні та професійні здібності злочинців, сприятимуть встановленню під час розслідування всієї сукупності злочинів, вчинених однією особою або групою осіб. Бачення типових способів підготовки, вчинення та

[1] Зав'ялов С. М. Способи вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. С. 19.

[2] Ухвала Колегії суддів судової палати у кримінальних справах апеляційного суду Дніпропетровської області від 10 берез. 2016 р. Справа № 182/3014/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56361518.

приховування одиничних злочинів у кіберпросторі дає змогу розглянути й комплексний злочин не статично, а в динаміці, як процес, що розвивається і відбиває тенденції розвитку технологій злочинної діяльності у майбутньому.

Тож, в основі функціонування злочинної діяльності у кіберпросторі знаходяться зв'язки між наступними елементами, що складають механізм вчинення такої категорії злочинів:

1) предмет посягання (матеріальні цінності, грошові кошти, інформація тощо);

2) особа злочинця, в тому числі у складі організованої групи чи злочинної організації;

3) способи вчинення злочинів у кіберпросторі (підготовки, безпосереднього вчинення та приховування)/ технології вчинення злочинів (сукупність способів, що забезпечують досягнення кінцевої злочинної мети при вчиненні сукупності різних за кримінально-правовими ознаками злочинів);

4) сліди злочину (в матеріальному та електронному середовищах).

Визначення типових та специфічних ознак наведених елементів механізму злочинів, вчинених у кіберпросторі, та зв'язків між цими елементами дозволить отримати повну криміналістичну характеристику досліджуваної категорії злочинів. При цьому конкретизація закономірних зв'язків між типовими ознаками таких злочинів в межах їх класифікаційних груп та підгруп, підкреслить специфіку останніх. Наведені позиції щодо функціонування такої злочинної діяльності вважаємо також орієнтиром для розроблення криміналістичних методик розслідування окремих видів злочинів, вчинених у обстановці кіберпростору.

2.2. Характеристика типових предметів посягання та їх зв'язок з мотивами вчинення злочинів у кіберпросторі

Безпредметних суспільних відносин між суб'єктами не може бути – головною, конституюючою характеристикою будь-якої діяльності, в тому числі й злочинної, є її предметність[1]. Тому зі всіх елементів механізму злочинної діяльності саме предмет посягання першим

[1] Леонтьев А. Н. Деятельность. Сознание. Личность. М. : Политиздат, 1975. С. 39.

потрапляє у поле зору слідчого. Адже процес розслідування як один з проявів кримінально-процесуальних відносин розпочинається за умови встановлення факту посягання на суспільні відносини, які поставлені під охорону закону про кримінальну відповідальність[1].

Слово «посягання» походить від слова «посягати», етимологія якого позначається як «намагатися захопити, привласнити що-небудь, зазіхати»[2]. Тому такі категорії як «предмет посягання», «предмет злочинного посягання», «безпосередній предмет посягання» в криміналістичній науці утворюють синонімічний ряд та використовуються як один з елементів криміналістичної характеристики злочинів. Традиційно криміналісти вказаними категоріями позначають речі матеріального світу, які характеризуються залежно від виду злочину певними фізичними ознаками (матеріальність, кількість, якість, форма, стан, структура тощо).

Виходячи з потреб сучасної практики виявлення та розслідування злочинів, специфіки використання кіберпростору під час здійснення злочинної діяльності, постає завдання розібратися у сутності «предмета посягання» як одного зі складових понятійно-категоріального апарату криміналістичної методики. Для цього вважаємо за потрібне звернутися до кримінально-правової доктрини щодо предмету злочину. Адже, як справедливо писав І. О. Возгрин, саме існування криміналістичної методики розслідування злочинів викликано встановленим законом переліком злочинних дій[3]. Вважаємо, що в основу криміналістичних розробок предмета посягання окремих видів злочинів, по суті, покладаються теоретичне (наукове) та прагматичне (практичне) бачення сутності предмета злочину в кримінально-правовій доктрині.

В теорії кримінального права найчастіше йдеться про так звані «предметні злочини», у яких предмет є ознакою складу злочину та виступає складовою частиною його об'єкта. Останній позбавлений

[1] Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. С. 61.

[2] Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2003. 1440 с. URL: http://sum.in.ua/s/posjaghaty.

[3] Возгрин И. А. Научные основы криминалистической методики расследования преступлении : в 4 ч. СПб. : С.-петерб. юрид. ин-т МВД России, 1992. Ч. 2. С. 18.

фактично ознаки «матеріальності», традиційно визнається суспільними відносинами, яким злочином завдається шкода або створюється загроза заподіяння такої шкоди[1]. Тому з теоретичних позицій в статтях КК України прямо йдеться про посягання на предмет злочину, як матеріальної природи (наприклад, на засоби доступу до банківських рахунків (ст. 200); порнографічні предмети (ст. 301); ЕОМ (комп'ютери), автоматизовані системи, комп'ютерні мережі чи мережі електрозв'язку (ст. 361, 361-1)), так й нематеріальної (відомості, що становлять комерційну чи банківську таємницю (ст. 231, 232), об'єкти авторського і суміжних прав (ст. 176), інформацію, обробка якої відбувається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах (ст. 361-2, 362) тощо).

З цих позицій П. Д. Біленчук, В. К. Лисиченко та деякі інші криміналісти ототожнюють предмет посягання з кінцевим продуктом злочину[2], його наслідком[3]. З поправкою на чинне кримінальне процесуальне законодавство можна перефразувати окремі тези криміналістів, зокрема: предметом посягання виступає результат злочинної діяльності суб`єкта, перед яким опиняється слідчий на момент прийняття рішення про внесення інформації про злочин до Єдиного реєстру досудових розслідувань. Наприклад, при вчиненні шпигунства у кіберпросторі предметами посягання стає електронна інформація у вигляді відомостей, що становлять державну таємницю, та комп'ютерна мережа, в якій циркулювали ці відомості, що піддалася впливу в результаті застосування шкідливого програмного засобу з метою отримання доступу зацікавленої особи до відповідних відомостей. Узагальнення наукових праць, присвячених розслідуванню окремих видів злочинів, вчинених у кіберпросторі, дозволяють визначити, що комп'ютерна (електронна) інформація або

[1] Кримінальне право України. Загальна частина : підручник / [М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.] ; за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ : Юрінком Інтер ; Харків : Право, 2001. С. 89.

[2] Криміналістика : підручник / [П. Д. Біленчук, В. К. Лисиченко, Н. І. Клименко та ін.] ; за ред. П. Д. Біленчука. 2-ге вид., випр. і доповн. Київ : Атіка, 2001. С. 485.

[3] Пособие для следователей: расследование преступлений повышенной общественной опасности / под ред. Н. А. Селиванова, А. М. Дворядкина. М. : Лига разума, 1998. С. 346.

зафіксовані аналогічним способом дані (відомості) майже безапеляційно визнаються предметом злочинного посягання[1]. Іноді ведеться мова про так званий «контент» як будь-яке інформаційно значуще (змістовне) наповнення інформаційного ресурсу (Інтернет-порталу, сайту, веб-сторінки тощо)[2].

З позицій прагматичного бачення предмета злочину останній виступає річчю лише матеріального (реального) світу, яка характеризується певними фізичними ознаками. Для їх позначення часто використовують термін «безпосередній предмет злочину». Такий предмет внаслідок вчинення злочину може знищуватися, псуватися, втрачати свої якості, переміщатися у просторі, змінювати власника, незаконно виготовлятися або вживатися, змінювати свій вигляд тощо[3]. На думку М. Й. Коржанського, предмет злочину – це конкретний матеріальний об'єкт, в якому проявляються певні сторони, властивості суспільних відносин (об'єкта злочину), фізичним чи психічним впливом на який заподіюється суспільно небезпечна шкода у сфері цих суспільних відносин [4]. Тим самим вказуючи або на матеріальну річ (у формі матерії, визначеної в просторі та часі), або на особу потерпілого, які піддаються злочинному впливу.

Криміналістика вивчає практичну діяльність з виявлення і розслідування злочинів з точки зору використання певних способів

[1] Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків : ХНУВС, 2010. 112 с.; Документування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за заг. ред. Л. П. Скалозуба, І. В. Бондаренко. Київ, 2010. 245 с.; Крылов В. В. Расследование преступлений в сфере информации. М. : Городець, 1998. 264 с.; Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рек. / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

[2] Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рек. / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

[3] Бантишев О. Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : монографія. Київ : Нац. акад. СБ України, 2001. С. 110.

[4] Коржанський М. Й. Кримінальне право і законодавство України. Загальна частина : курс лекцій. Київ : Атіка, 2001. С. 173.

(слідчих дій), прийомів та засобів виявлення, фіксації, вилучення і використання слідів злочину як джерел доказів[1]. Серед останніх відповідно до чинних норм КПК України називаються документи та «об'єкти кримінально протиправних дій», що виступають речовими доказами у справі[2]. Сутність речових доказів традиційно підлягає характеристиці шляхом окреслення притаманних їм ознак, серед яких предметність визнається процесуалістами як невід'ємна ознака, що позначає матеріальний характер відомостей, що мають доказове значення (це речі або документи)[3]. Тож, з прагматичних позицій (з метою збирання та дослідження слідів злочину) предмет посягання у криміналістичному сенсі повинен мати фізичну (матеріальну) форму, що придатна для сприйняття слідчому. З цих позицій обґрунтованим уявляється віднесення до предметів посягання грошей, майнових комплексів, апаратних засобів комп'ютерної техніки та інших матеріальних цінностей, а суперечливим – немайнових цінностей як-от комп'ютерної (електронної) інформації, банківської та державної таємниці, персональних даних та інших утворень немайнового характеру, про які як предмети посягання наявна велика кількість публікацій[4].

Отже, сутність предмета посягання у криміналістичній науці є достатньо суперечливою. Колізія полягає у тому, що криміналісти,

---

[1] Криміналістика : підручник / [А. Ф. Волобуєв, О. О. Волобуєва, О. А. Самойленко та ін.] ; за ред. А. Ф. Волобуєва. Київ : КНТ, 2011. С. 15.

[2] Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

[3] Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : монографія. Івано-Франківськ : Супрун В. П., 2017. С. 174.

[4] Ткач О. В. Предмет злочинного посягання як елемент криміналістичної характеристики порушень недоторканності приватного життя. *Юрист України.* 2014. № 4 (29). С. 136–141; Одерій О. В. Предмет посягання як елемент криміналістичної характеристики злочинів проти довкілля: окремі питання. *Ученые записки Таврического национального университета им. В. И. Вернадского.* 2013. № 1. Т. 26 (65). С. 255–259. (Серия «Юридические науки»); Кузьмін С. А. Комп'ютерна (кібернетична) інформація як предмет вчинення злочину (кримінально-правовий аспект). *Інформація і право.* 2012. № 3 (6). С. 159–163; Лужецька О. Р. Предмет посягання в системі криміналістичної характеристики вимагання. *Науковий вісник Національного університету державної податкової служби України.* 2014. № 2 (65). С. 202–207. (Серія «Економіка, право»).

визнаючи в цілому обов'язковість матеріальних властивостей предмета посягання, в окремих методиках розслідування злочинів допускають наявність нематеріальних предметів злочину.

Домінуючою в цьому контексті вважаємо позицію А. Ф. Волобуєва, який визнає, що властивості предмета посягання закономірно пов'язані з своєрідностями умов вчинення злочинів (умов існування предмета)[1]. Описуючи предмет розкрадання, науковець наголошує на тому, що предмет посягання детермінує дії злочинців з підготовки, вчинення і приховування цього злочину, які, в свою чергу, пов'язані з утворенням певних слідів –джерел доказів. Предмети посягання при вчиненні розкрадання він розглядає через призму головної мети розкрадачів – заволодіння фінансовими ресурсами (капіталом), що дає йому підстави відносити до предметів як традиційні матеріальні цінності, так й нетрадиційні, зокрема «електронні» або «банківські» грошові кошти.

Еволюційні процеси технологій кіберпростору призвели до того, що сьогодні інформація отримала значення цінного ресурсу суспільства, який дає можливість задовольнити конкретній людині широкий спектр потреб у фінансово-економічній, соціальній, державно-політичній або духовній сферах її життя. Для цього людина вдається до системи дій, зміст яких визначається сутністю протікання інформаційних процесів у кіберпросторі. Тож, за умови використання останнього у механізмі злочинної діяльності, окремого значення набуває питання природи інформації та інформаційних процесів у кіберпросторі.

Як писав засновник кібернетики Н. Вінер: «Інформація – це не енергія і не матерія, це зміст, отриманий від зовнішнього світу в процесі пристосування до нього»[2]. Традиційно в науках розрізняють семантичний та семіотичний (теорія інформації) підходи до розуміння інформації[3].

---

[1] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 57.

[2] Винер Н. Кибернетика. М., 1983. С. 208.

[3] Аляєв Г. Теорія інформації на тлі історії філософії. *Науковий вісник Чернівецького університету.* 2015. Вип. 754–755. С. 3–8. (Серія «Філософія»).

Семантичний підхід досліджує інформацію з погляду її змісту: інформація обов'язково має певний предмет, який повинен бути інтерпретований у знання певного адресанта цієї інформації. Для цього використовують різні знаки (символи), що дозволяють виразити (представити) інформацію у певній формі: букви, цифри, слова та фрази певного змісту. По суті, це інформація у широкому розумінні як сукупність знань про довкілля, яка є найважливішим ресурсом науково-технічного та соціально-економічного розвитку суспільства[1].

З семіотичного погляду інформація – це кількість, яка вимірюється в «бітах» і визначається як вірогідність частотності символів. Засновниками теорії інформації вважаються Клод Шеннон і Уоррен Уівер, які писали про кібернетичні системи, пристрої керування, повідомлення та сигнали, що було згодом використано з метою налагодження функціонування телекомунікаційних мереж[2]. Для розуміння суті інформації у електронній формі наведемо деякі ключові позиції[3]. Повідомлення – це сукупність знаків, які відображають ту або іншу інформацію. Сигнал – це фізичний процес, що відображає передане повідомлення. У сучасних системах керування та зв'язку найчастіше використовують електричний зв'язок. Фізичною величиною, що визначає такий сигнал, є струм або напруга. На відміну від матеріального та енергетичного ресурсів інформаційний ресурс не зменшується при споживанні, він накопичується, порівняно легко та просто за допомогою технічних засобів обробляється, зберігається та передається на великі відстані.

Вітчизняний законодавець намагається поєднати одночасно вказані два підходи у розумінні інформації, визнаючи у ст.1 Закону України «Про інформацію», останню будь-якими відомостями та/або даними, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді. Втім, науковці, продовжуючи науковий пошук, виділяють «фізичність інформації» як ознаку

[1] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. С. 60.

[2] Колмогоров А. Н. Теория информации и теория алгоритмов. М. : Наука, 1987. 304 с.

[3] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. С. 61.

предмета злочину. М. В. Карчевський під фізичною ознакою комп'ютерної інформації розуміє наявність носія – предмета або сигнала, фізичні, хімічні чи інші властивості яких використовуються для зберігання, передавання та опрацювання інформації, що розпізнається електронно-обчислювальною машиною[1]. Є. В. Лащук пише, що фізичність знаходить свій прояв у можливості людини сприймати органами чуття чи фіксувати спеціальними технічними засобами матеріальні цінності, з приводу яких та (або) шляхом безпосереднього впливу на які вчиняється злочинне діяння[2].

З одного боку інформація дійсно не може існувати без матеріального або так званого фізичного носія. Телекомунікаційні мережі, магнітний, електронний або оптичний носій (накопичувач) інформації (диски різних видів, карти пам'яті, флеш-пам'ять) використовуються для оперування інформацією різного змісту. З іншого боку – інформація піддається злочинному впливу за умови її транспортування, її руху в просторі за допомогою інформаційних (телекомунікаційних) технологій, які виступають способами передачі інформаії. При цьому основним завдання телекомунікаційної мережі є надання якісного транспортного сервісу при перенесенні інформації в просторі[3]. В цьому процесі для користувача інформація виступає результатом задоволення його інформаційних потреб – інформаційним продуктом. Останній є по-суті обов'язковою умовою існування самого кіберпростору.

Засновник теорії особистості психолог А. Н. Леонтьєв писав, що головним у діяльності особистості є те, що потреба стоїть завжди за мотивом, а останній завжди відповідає тій або іншій потребі[4]. На думку науковця предмет діяльності є її дійсний мотив, який може

[1] Карчевський М. В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину : дис. ... канд. юрид. наук : 12.00.08. Луганськ, 2003. 175 с.; Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. 168 с.

[2] Лащук Є. В. Предмет злочину в кримінальному праві : дис. … канд. юрид. наук : 12.00.08. Київ, 2005. С. 59.

[3] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. С. 32.

[4] Леонтьев А. Н. Деятельность. Сознание. Личность. М. : Политиздат, 1975. С. 48.

бути як речовинним, так і ідеальним, як даним в сприйнятті, так і існуючим тільки в уяві, по суті. Тож, поряд з ідеальним мотивом допускається нематеріальний предмет з приводу якого здійснюється діяльність людини.

Цей погляд є цікавим з позиції усвідомлення процесу формування основних та додаткових мотивів вчинення злочинів у кіберпросторі, які у попередньому розділі роботи покладаються в основу криміналістичної класифікації таких злочинів. Сам поділ мотивів вчинення таких злочинів на корисливі, соціально-економічні, антидержавно-політичні та ідейні мотиви має під собою речовинну щодо корисливих та ідеальну щодо інших мотивів складову предмета злочинного посягання. Зазначимо, що додаткові мотиви злочинної діяльності у кіберпросторі, будучи зумовленими обраним злочинцем специфічним набором операцій у кіберпросторі, спрямовані на створення умов, що забезпечують доведення злочинної діяльності до кінця, задоволення основної (кінцевої) потреби злочинця. Для користувача кіберпростору першою сходинкою на шляху задоволення основної (кінцевої) за своїм значенням потреби є задоволення інформаційної потреби, що проявляється у вигляді інформаційного продукту.

Вплив на інформаційний продукт/ресурс фактично призводить до змін, що характеризуються ознаками матеріального світу, зокрема, мають наслідком покращення матеріального стану злочинця, утворення специфічних електронних та матеріальних слідів, носіями яких виступають відповідно комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи. Такі предмети, по суті, виконують роль похідних предметів посягання у механізмі злочинної діяльності у кіберпросторі. Зважаючи на закономірну зумовленість предметів посягання технологіями злочинної діяльності, що, у свою чергу, пов'язані із кібертехнологіями (інформаційними технологіями), можна висновувати про існування первинних та вторинних (або похідних) за послідовністю злочинного впливу предметів посягання.

Про існування системи предметів посягання при вчиненні злочину із використання кіберпростору дає можливість висновувати й полімотивованість такої злочинної діяльності. Адже застосування технологій злочинної діяльності є особливо характерним при вчиненні корисливих злочинів, що пов'язані з фінансовою або соціально-економічною сферами відносин осіб у кіберпросторі. Такі відносини

завжди відбуваються з приводу майна, адже вони спрямовані на задоволення відповідних матеріальних чи соціально-економічних потреб злочинця. Тому в систему вторинних предметів посягання у кіберпросторі будуть входити також речі матеріального світу, які можна окреслити категорією «майно».

Отже, *при вчиненні злочину у кіберпросторі інформаційний продукт виступає первинним предметом посягання, а майно, комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи – вторинними.* Зважаючи на первинність функції по відношенню до системи в основу будови такої системи покладено функціональне призначення кожного з предметів посягання у механізмі такої злочинної діяльності, який визначається, перш за все, специфікою цього простору – його інформаційною природою.

Інформаційний продукт(и) як первинний предмет посягання. Дискусії про те, що розуміти під інформаційним продуктом, ведуться з позицій багатьох наук, зокрема інформатики, економіки, маркетингу, бібліотечної справи. При цьому кожна з галузей знань визначає інформаційний продукт, виходячи зі своєї предметної сфери. Так, в економіці інформаційний продукт розглядається як один зі складових інформаційного ринку, що з позиції виробника інформаційних послуг є сукупністю даних, що сформована для поширення в речовинній або нематеріальній формі. У інформаційно-аналітичній діяльності, науковій інформатиці та бібліотечній справі інформаційний продукт ототожнюється з інформаційною продукцією, що являє собою документи, інформаційні масиви, бази даних і інформаційні послуги, які є результатом функціонування інформаційних систем[1].

Згідно ст. 1 Закону України «Про національну програму інформатизації» інформаційний продукт (або продукція) є документованою інформацією, яка підготовлена і призначена для задоволення потреб користувачів[2]. Відзначимо, що слово «продукт» у тлумачних словниках традиційно позначається як наслідок, витвір, результат будь-чого; речовий або інтелектуальний результат людської

[1] Захарова І. В., Філіпова Л. Я. Основи інформаційно-аналітичної діяльності : навч. посіб. Київ : Центр учб. літ., 2013. С. 130–140.

[2] Про національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: http://zakon2.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80?nreg=74%2F98-%E2%F0&find=1&text=%EF%F0%EE%E4%F3%EA%F2&x=10&y=10#w16.

праці[1]. Слово «інформаційний» виступає прикметником, що використовується для вказівки на зв'язок основного слова з інформацією. Згідно однієї з позицій у тлумачному словнику «термін «інформаційний» стосується інформації як сукупності відомостей або сигналів, що містяться де-небудь або що передаються від одного об'єкта іншому»[2]. В цьому сенсі інформаційний продукт це інформація/відомості, що зафіксовані у електронній формі, як результат задоволення потреб користувача/ів кіберпростору.

М. В. Карчевський справедливо робить акцент на цінності інформації[3], яка буває різною: може бути цінною по суті, оскільки є результатом тривалої роботи великої кількості осіб, або цінною за призначенням, оскільки її наявність є необхідною умовою для вирішення певного завдання, наприклад, отримання доступу до банківських рахунків, персональні або особисті дані. Втім, в своїх роботах автор цінність інформації все ж таки дорівнює категорії «ціна». В результаті виділення фізичної, економічної та юридичні ознаки комп'ютерної інформації визнає останню предметом злочину та розуміє під нею відомості про об'єктивний світ і процеси, що відбуваються в ньому, цілісність, конфіденційність і доступність яких забезпечується за допомогою комп'ютерної техніки та які мають власника і ціну[4]. Економічну ознаку інформації виражає через цілісність, доступність, конфіденційність та ціну останньої. Юридичну ознаку – через специфічність інституту права власності на інформацію[5]. Тож інформаційний продукт як предмет посягання повинен бути чужим для злочинця та мати законного користувача/ів, що закономірно пов'язано з характером зафіксованих у ньому відомостей (наприклад, твір як об'єкт авторського права, персональні дані, банківська таємниця тощо).

---

[1] Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. С. 1159.

[2] Там само.

[3] Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. С. 60.

[4] Карчевський М. В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину : дис. ... канд. юрид. наук : 12.00.08. Луганськ, 2003. С. 61.

[5] Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. С. 50.

Наведене дає можливість стверджувати, що *цінність інформаційного продукту, пов'язана з характером зафіксованих у ньому відомостей, зумовлює обрання злочинцем останнього для здійснення на нього впливу, що скерований загальним мотивом злочинної діяльності.* Доступ сторонніх осіб до таких продуктів обмежений на підставі закону, зокрема, ними виступає «інформація з обмеженим доступом» та результат чужої інтелектуальної праці.

Відповідно ч. 1 ст. 20 ЗУ «Про інформацію» інформація за порядком доступу до неї поділяється на відкриту інформацію та інформацію з обмеженим доступом. На думку В. Баскакова, з якою погоджуються з незначними зауваженнями провідні науковці, інформацію з обмеженим доступом складають відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді, доступ до яких обмежено відповідно до законодавства України її власником або добросовісним користувачем (суб'єктом владних повноважень, фізичною або юридичною особою) у зв'язку з її особливою цінністю для них на законних підставах[1]. На законодавчому рівні визначені три групи такої інформації, зокрема службова, таємна та конфіденційна (в тому числі інформація про особу). У Законі України «Про доступ до публічної інформації» конкретизовані загальні вимоги при обмеженні доступу до інформації та правовий статус кожного з видів інформації[2]. Втім, з практичних міркувань доцільно розглядати інформацію з обмеженим доступом в контексті змісту та суб'єкта, що нею володіє. Тому традиційно у теорії інформаційного права вона поділяється на:

1) державну таємницю (секретну інформацію);

2) конфіденційну інформацію, що охоплює інформацію про фізичну особу, а також інформацію, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційна інформація поділяється на:

– інформацію про особу (персональні дані);

[1] Баскаков В. Інформація з обмеженим доступом: поняття та ознаки. *Актуальні проблеми державотворення :* матеріали наук.-практ. конф. (Київ, 28 черв. 2011 р.). Київ : Ліпкан О. С., 2011. С. 47–49; Ліпкан В. А., Капінус Л. І. Доступ до інформації з обмеженим доступом: проблеми вироблення уніфікованих дефініцій. *Публічне право.* 2013. № 4. С. 45–43.

[2] Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/laws/show/2939-17.

– інформацію, що є власністю держави (службова таємниця або інформація для службового користування);

– комерційну таємницю;

– професійну таємницю (серед якої розрізняють лікарську, адвокатську, нотаріальну, страхову, банківську та деякі інші види таємниці);

– банківську таємницю[1].

Аналіз матеріалів судово-слідчої практики дозволяє визнати, що злочинець, який використовує обстановку кіберпростору при вчиненні злочину, типово посягає на персональні дані (20% проваджень), банківську (50%), державну (20%) та комерційну (10%) таємницю.

Персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована (ст. 1 Закону України «Про захист персональних даних»)[2]. Не дивлячись на те, що ст. 11 Закону України «Про інформацію» чітко визначає їх перелік, зокрема, дані про її національність, освіту, сімейний стан, релігійні переконання, стан здоров'я, а також адреса, дата і місце народження, Конституційний Суд України вважає, що перелік даних про особу, які визнаються як конфіденційна інформація, не є вичерпним[3]. В цьому є сенс, адже як свідчать наукові розробки та аналіз судово-слідчої практики до персональних даних відносять дані про інтимні сторони життя людини, неблаговидні вчинки, злочинну діяльність, дані, що скомпрометують або принизять честь і гідність особи чи близьких йому осіб[4]. Вивчення матеріалів кримінальних проваджень дозволяє

[1] Кормич Б. А. Інформаційне право : підручник. Харків, 2011. 334 с.; Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. Київ, 2007. 531 с.

[2] Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: http://zakon2.rada.gov.ua/laws/show/2297-17.

[3] Рішення Конституційного суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : рішення Конституційного суду України від 20 січ. 2012 р. № 2-рп/2012. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-12.

[4] Чуприна О. Співвідношення понять «персональні дані», «інформація про особу», «конфіденційна інформація про особу». *Підприємство, господарство і право.* 2013. № 1. С. 104–108; Марущак А. І. Правові основи захисту інформації з обмеженим доступом. Київ, 2007. С. 90.

стверджувати, що персональні дані типово стають первинний предметом посягання у механізмі вчинення злочинів, пов'язаних із анархістськими діями у кіберпросторі, що поєднані з наступними підгрупами злочинів, вчинених з корисливих та соціально-економічних мотивів: 1) злочинів, що спрямовані на заволодіння чужим майном (крадіжки; вимагання; шахрайства, привласнення, розтрати майна або заволодіння ним шляхом зловживання службовим становищем, незаконних дій з платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима), 2) злочинів, пов'язаних із насильницько-егоїстичними та комунікаційними діями (доведення до самогубства; вербування людини, вчинене з метою її експлуатації; ввезення, виготовлення, збут і розповсюдження порнографічних предметів; порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер). Злочинець, незаконно отримавши доступ до персональних даних особи (самостійно або за допомоги третьої особи), виходячи зі змісту отриманих відомостей, вирішує подальший шлях їх використання у своїй злочинній діяльності.

Банківська таємниця – це інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку в процесі обслуговування клієнта та взаємовідносин з ним чи третім особам при наданні послуг банку[1]. У ст. 60 Закону України «Про банки і банківську діяльність» чітко визначено перелік відомостей, що становлять банківську таємницю. Враховуючи той факт, що кредитно-банківська система як сукупність кредитно-фінансових інститутів акумулювала основні грошові капітали, доходи і заощадження різних прошарків населення[2], окремі відомості, що становлять банківську таємницю, викликають у злочинців особливу зацікавленість, зокрема: 1) відомості про банківські рахунки клієнтів, кореспондентські рахунки банків у НБУ; 2) операції, які були проведені на користь чи за дорученням клієнта, здійснені ним угоди; 3) системи охорони банку та клієнтів; 5) відомості стосовно комерційної діяльності клієнтів чи комерційної таємниці, будь-якого проекту, винаходів, зразків продукції

[1] Про банки і банківську діяльність : Закон України від 7 груд. 2000 р. № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14.

[2] Небава М. І. Теорія корпоративного управління: вузлові питання : навч. посіб. Київ : Центр інновацій та розвитку, 2004. С. 270.

та інша комерційна інформація; 7) коди, що використовуються банками для захисту інформації; 8) інформація про фізичну особу; 9) документи для службового користування з питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю. Така інформація вдало використовується у механізмах вчинення злочинів з корисливих мотивів, що пов'язані з фінансово-економічною сферою відносин у кіберпросторі, зокрема: спрямованих на заволодіння чужим майном, у сфері функціонування електронних розрахунків або тих, що порушують механізми захисту від монополізму та недобросовісної конкуренції.

Державну таємницю складають відомості у сфері оборони, економіки, науки і техніки, зовнішніх відносин, державної безпеки та охорони правопорядку, розголошення яких може завдати шкоди національній безпеці України та які визнані у порядку, встановленому Законом України «Про державну таємницю», державною таємницею і підлягають охороні державою[1]. Як пише М. О. Шилін динаміка сучасної оперативної обстановки по лінії контррозвідувального забезпечення державної безпеки України свідчить про подальшу активізацію діяльності спецслужб іноземних держав, зокрема, з проведення ними легальної розвідки, а також залучення громадян України до збору інформації, що становить державну таємницю в політичній, економічній, військовій, науково-технічній і оборонній сферах[2]. Сьогодні державна таємниця типово виступає предметом посягання при вчиненні злочинів у обстановці кіберпростору з антидержавно-політичних мотивів, зокрема всіх класифікаційних підгруп злочинів, що пов'язані з антидержавницькими діями.

Результат чужої інтелектуальної праці в кримінально-правовій сфері має форму об'єктів авторського права або суміжних прав. Останні виступають предметом посягання у механізмі вчинення інтелектуального піратства, як різновиду злочинів, вчинених з соціально-економічних мотивів.

---

[1] Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.

[2] Шилін М. Національна безпека: проблеми правового забезпечення діяльності суб'єктів сектору безпеки та можливі шляхи вирішення. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку :* матеріали Міжнар. наук.-практ. конф. (Острог, 1 груд. 2017 р.) / за заг. ред. М. С. Романова. Острог : Нац. ун-т «Острозька академія», 2017. С. 22.

Кримінальна відповідальність за такий злочин передбачена у статті 176 КК України «Порушення авторського права і суміжних прав». В ній міститься перелік предметів такого злочину, зокрема: твори науки, літератури, мистецтва, комп'ютерні програми і баз даних, фонограми, програми мовлення та інші об'єкти суміжних прав (виконання літературних, драматичних, музичних, музично-драматичних, хореографічних, фольклорних та інших творів; фонограми, відеограми; передачі (програми) організацій мовлення, відповідно ст. 35 Закону України «Про авторські та суміжна права»[1]). Вдаватися до їх тлумачення немає сенсу через законодавчу їх визначеність та величезну кількість наукових праць подібної тематики[2].

У результаті аналізу судово-слідчої практики розслідування вказаної категорії злочинів можна визначити, що серед об'єктів авторського права та суміжних прав предметами незаконного відтворення, розповсюдження та тиражування (щодо об'єктів суміжних прав) у кіберпросторі найчастіше виступають:

[1] Про авторські та суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII. URL: https://zakon.rada.gov.ua/laws/show/3792-12.

[2] 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.; Трунцевский Ю. В. Интеллектуальное пиратство: гражданско-правовые и уголовно-правовые меры противодействия. М. : Юрист, 2002. 148 с.; Таран О. В. Криміналістичне забезпечення розслідування злочинної діяльності у сфері порушення авторських прав : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.; 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.; Ніколаюк С. І., Никифорчук Д. Й., Томма Р. П., Барко В. І. Протидія злочинам у сфері інтелектуальної власності (ст. 176, 177, 227, 229 КК України) : наук.-практ. посіб. Київ : КНТ, 2006. 192 с.; Поджаренко К. Є. Криміналістичне забезпечення розкриття і розслідування злочинних порушень прав інтелектуальної власності : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 18 с.; Моторина Е. В. Первоначальный этап расследования нарушений авторских и смежных прав в аудиовизуальной сфере : дис. … канд. юрид. наук : 12.00.09. Ростов н/Д, 2005. 193 с.; Ларичев В. Д., Трунцевский Ю. В. Защита авторского и смежных прав в аудиовизуальной сфере: уголовно-правовой и криминологический аспекты. М. : Дело, 2004. 351 с.; Жаров В. О. Інтелектуальна власність в Україні: правові аспекти набуття, здійснення та захисту прав : монографія. Київ : Ін Юре, 2000. 188 с.

аудіовізуальні твори (традиційно фільми, що вийшли у прокатний показ) (50 %), бази даних (компіляції даних) (10 %), комп'ютерні програми (10 %) фонограми та передачі організацій мовлення (30 %).

В контексті нашого предмета дослідження потрібно зупинитись лише на такому достатньо новому правовому режимі об'єктів авторського права як «веб-сайт». Так, 23 березня 2017 року було прийнято Закон України «Про державну підтримку кінематографії в Україні», яким вносились доповнення у Закон України «Про авторське право та суміжні права» щодо порядку захисту права інтелектуальної власності у мережі Інтернет[1]. Якщо раніше у наукових колах тривали дискусії з приводу того, чим є веб-сайт[2]: базою даних (компіляцією даних)[3], складеним твором типу мультимедійного твору, засобом масової інформації, або взагалі він не є об'єктом права інтелектуальної власності, – то сьогодні законодавець визначився з його природою. Через закріплення прав та обов'язків власників веб-сайту та веб-сторінки сам веб-сайт, по суті, визнається технічною умовою існування об'єктів авторського права і суміжних прав у кіберпросторі.

Під «веб-сайтом» законодавець визнає сукупність даних, електронної (цифрової) інформації, інших об'єктів авторського права і (або) суміжних прав тощо, пов'язаних між собою і структурованих у межах адреси веб-сайту і (або) облікового запису власника цього веб-сайту, доступ до яких здійснюється через адресу мережі Інтернет, що може складатися з доменного імені, записів про каталоги або виклики і (або) числової адреси за Інтернет-протоколом (ст. 1 Закон України «Про авторське право і суміжні права»). Мінімальний набір елементів веб-сайту передбачає наявність п'яти їх видів: 1) дизайн; 2) структурне рішення; 3) програмне забезпечення; 4) контент (змістовне наповнення – будь-які твори (часто аудіовізуальні твори, бази даних, фонограми, програми)); 5) домінне ім'я як ідентифікатор

[1] Про державну підтримку кінематографії в Україні : Закон України від 23 берез. 2017 р. № 1977-VIII. URL: https://zakon.rada.gov.ua/laws/show/1977-19.

[2] Майданик Н. Web-сайт в мережі Інтернет як особливий об'єкт авторського права. *Юридична Україна.* 2008. № 12. С. 73–80.

[3] Пастухов О. М. Авторське право в Інтернеті. Київ : Школа, 2004. С. 45.

Інтернет-ресурсу, зареєстрований адміністратором мережі[1]. Якщо перші чотири закономірно відносити до об'єктів інтелектуальної власності, то щодо останнього тривають наукові дебати. Виваженим вважаємо підхід, у якому доменні ім'я визначають засобом ідентифікації певного інформаційного ресурсу в мережі Інтернет, який за певних умов є похідним засобом індивідуалізації фізичних та юридичних осіб в мереж Інтернет[2]. Отже, доменне ім'я буде предметом посягання у значенні персональної інформації про особу або нематеріального активу юридичної особи, що дорівнюється комерційній тайні.

Заволодіння ж доменним іменем призводить до отримання злочинцем повноважень адміністратора веб-сайту, що дає можливість використовувати останній як знаряддя задля досягнення кінцевої мети злочинної діяльності. В цьому сенсі Д. С. Азаров зазначав, що не важко помітити, що існують такі злочини, при вчиненні яких комп'ютерна інформація в одних випадках може бути лише предметом злочину, в інших – знаряддям злочину[3].

Знаряддя є різновидом засобів вчинення злочину у широкому розумінні, під якими розуміють речі, предмети, документи, механізми, пристосування та інші предмети матеріального світу, використовуючи які винний вчиняє злочин[4]. По-суті знаряддя вчинення злочину виконують функцію інструмента, який активно діє на предмет посягання. У кіберпросторі функцію інструмента виконують інформаційні (у вітчизняній інтерпретації комп'ютерні або інформаційно-комунікаційні технології) чи кібертехнології (термін використовується з метою скорочення громіздких словосполучень). Інформаційні технології (information technologies – IT; information communication technologies – ICT) – це методи та способи накопичення, обробки, зберігання, відображення, пошуку і

[1] Майданик Н. Web-сайт в мережі Інтернет як особливий об'єкт авторського права. *Юридична Україна.* 2008. № 12. С. 74.

[2] Кулініч О. О. Доменне ім'я як похідний засіб індивідуалізації інформаційних ресурсів фізичних та юридичних осіб у мережі Інтернет. *Актуальні проблеми держави та права.* 2009. № 51. С. 200.

[3] Азаров Д. С. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації. *Юридична Україна.* 2004. № 7 (19). С. 66.

[4] Панов Н. Н. Средства совершения преступления: понятие и виды. *Проблеми законності :* респ. міжвідом. наук. зб. / відп. ред. В. Я. Тацій. Харків, 2003. С. 130.

забезпечення цілісності інформації[1]. Отже, в криміналістичному сенсі сам інформаційний продукт навряд чи можна назвати знаряддям злочину, для цього він повинен бути поєднаний з інформаційною технологією.

Сукупність інформаційних продуктів, організована за допомогою певної інформаційної технології, у загальному розумінні виступає електронним інформаційним ресурсом (далі ресурс). В галузі телекомунікацій ресурси (information sourses) – це систематизовані масиви інформації, створювані та накопичувані у мережі з використанням інформаційних технологій і призначені для багаторазового запитування користувачами[2]. До традиційних сьогодні форм організації ресурсу відносяться: файли, бази та банки даних, електронні системи, сайти[3]. Всі вони як ресурси та відповідно й інформаційні продукти характеризуються певними ознаками як соціальне явище, зокрема: виступає системоутворюючим чинником діяльності; позитивно впливає на соціально-економічний розвиток суспільства і держави; забезпечує національну безпеку; здатний завдавати шкоди суспільству в разі низької якості або негативної інформаційної експансії з боку інших країн [4].

Наведене дає можливість стверджувати, що при вчиненні злочину у кіберпросторі, злочинець, скерований загальним мотивом злочинної діяльності, впливаючи тим чи іншим способом на інформаційний ресурс (як сукупність інформаційних продуктів), може перетворювати останній у знаряддя з метою доведення, по суті, злочину до кінця або вчинення подальших дій злочинної сукупності. Тож, *можливість використовувати інформаційний ресурс як знаряддя задля досягнення*

---

[1] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. С. 32.

[2] Там само. С. 34.

[3] Інформаційне право та правова інформатика : курс лекцій / [В. Г. Хахановський, І. В. Мартиненко, В. М. Смаглюк та ін.] ; за заг. ред. Є. М. Моісеєва. Київ : Київ. нац. ун-т внутр. справ, 2007. 253 с.; Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.

[4] Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.

кінцевої мети злочинної діяльності зумовлює обрання злочинцем певного інформаційного продукту/ресурсу для злочинного впливу на нього.

Таким ресурсом типово виступають:

– попередньостворений злочинцем файл, наприклад, шкідливий за призначенням з метою подальшого завантаження у систему та сбору інформації з обмеженим доступом, або що містить зображення порнографічного характеру;

– веб-сайт, що використовується для розміщення інформації антидержавницького характеру, розповсюдження порнографічних предметів, наркотичних засобів, пропаганди війни, доведення до самогубства, розповсюдження творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію тощо;

– автоматизовані (електронно-інформаційні) системи різного призначення (платіжні системи при протидії законній господарській діяльності, фінансуванні тероризму, економічних розкраданнях; об'єкт критичної інформаційної інфраструктури (наприклад, системи, що забезпечують диспетчерське керування повітряним або залізничним рухом, митне оформлення, поштові відправлення, постачання електроенергії та інші види робіт при вчиненні терористичного акту).

Тож, у контексті комплексного характеру злочинів, вчинених у кіберпросторі, сукупність інформаційних продуктів у значенні інформаційного ресурсу, що використовується як знаряддя вчинення злочину, не позбавляється значення предмета посягання. Відсоткові показники стосовно поширеності тих чи інших інформаційних ресурсів як предмета посягання не уявляється можливим навести. Адже аналіз матеріалів кримінальних проваджень досліджуваної категорії злочинів свідчить про типову неспроможність суб'єкта розслідування встановити всі обставини вчинення кожного зі злочинів злочинної сукупності, а тому досить часто не всі ресурси, що стали предметом посягання у механізмі злочинної діяльності у кіберпросторі, встановлюються.

Таким чином, *обрання злочинцем певного інформаційного продукту/ресурсу для скерованого загальним мотивом злочинної діяльності впливу зумовлює два не виключаючих один одного чинника:*

1) *цінність за характером зафіксованих у інформаційному продукті /ресурсі відомостей;*

2) *можливість використовувати інформаційний ресурс як знаряддя задля досягнення кінцевої мети злочинної діяльності*.

Майно як вторинний (похідний) предмет посягання. В цивілістиці до поняття «майно» традиційно відносять все, що має грошову, мінову або споживчу вартість, всі так звані «майнові блага», з приводу яких виникають цивільні правовідносини (матеріальні цінності, фінансові ресурси, результати роботи, послуги тощо)[1]. В кримінальному праві майно ототожнюється з категорією «матеріальні цінності», які поділяються на дві групи: ті, що мають позитивні властивості, та ті, що мають негативні (небезпечні) властивості. Якщо першу групу матеріальних цінностей законодавець ставить під кримінально-правову охорону, то другу він забороняє[2]. Втім, матеріальні цінності другої групи не втрачають значення предмета посягання в криміналістичному сенсі, адже вони піддаються впливу в результаті застосування тієї або іншої технології вчинення злочину.

На наше переконання, поділ майна на негативні та позитивні за своїми властивостями матеріальні цінності є вдалим з позиції застосування аналогічного підходу при характеристиці майна у системі предметів посягання щодо злочинів, вчинених у кіберпросторі.

Матеріальні цінності, що мають позитивні властивості, у виді грошових готівкових або безготівкових коштів, коштовних товарів виступають типовим предметом посягання при вчиненні корисливих злочинів у кіберпросторі, зокрема таких їх класифікаційних підгруп як: 1) злочини, що спрямовані на заволодіння чужим майном, та пов'язаних із ними злочини у сфері функціонування електронних розрахунків; 2) злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції. Типовим похідним предметом посягання при вчиненні терористичного акту із використанням обстановки кіберпростору виступає цілісний майновий комплекс критично важливого об'єкта інфраструктури. Враховуючи положення ст. 190 Цивільного кодексу України та Закону України «Про основні засади забезпечення кібербезпеки України» цілісний майновий комплекс являє собою матеріальний об'єкт на земельній ділянці із інженерними комунікаціями, системою енергопостачання та

[1] Цивільне право України. Загальна частина / за ред. І. А. Бірюкова, Ю. О. Заіки. Київ : Алеута, 2014. 510 с.

[2] Лащук Є. В. Предмет злочину в кримінальному праві : дис. … канд. юрид. наук : 12.00.08. Київ, 2005. С. 56.

завершеним циклом виробництва продукції (робіт, послуг), що належить об'єкту критичної інфраструктури або має стратегічне значення для економіки і безпеки держави. Їх перелік визначено Постановою 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»[1]. Виведення з ладу або порушення функціонування таких майнових комплексів може справити негативний вплив на стан національної безпеки і оборони України, навколишнього природного середовища, заподіяти майнову шкоду та/або становити загрозу для життя і здоров'я людей (п. 6 ст.1 Закону України «Про основні засади забезпечення кібербезпеки України»)[2]. Так, наприклад, наприкінці 2016 року більше 30 підстанцій енергокомпанії «Укренерго», «Чернівціобленерго» та «Київобленерго» одночасно зазнали кібератаки в результаті використання невстановленими злочинцями шкідливого програмного засобу «Industroyer», що був замаскований під ddos-атаку. За інформацією одного з обленерго, підключення зловмисників до його інформаційних мереж відбувалося з підмереж глобальної мережі Internet, що належать провайдерам в Російській Федерації[3].

Комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи як вторинні (похідні) предмети посягання (матеріальні цінності, що мають позитивні властивості). Аналіз матеріалів кримінальних проваджень приводить до думки, що комп'ютери, комп'ютерні мережі, мережі електрозв'язку та документи стають предметом посягання при вчиненні досліджуваної категорії злочинів

[1] Про затвердження переліку об'єктів державної власності, що мають стратегічне значення для економіки і безпеки держави : постанова Кабінету Міністрів України від 4 берез. 2015 р. № 83. URL: http://zakon5.rada.gov.ua/laws/show/83-2015-%D0%BF.

[2] Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

[3] Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. *Міністерство енергетики та вугільної промисловості України :* [сайт]. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109.

як речі матеріального світу у вигляді певних технічних або комбінованих (банківська платіжна картка) засобів автоматизованої обробки інформації, які одночасно виконують функцію захисту інформації від несанкціонованого втручання в роботу з останньою. Традиційно вони виступають предметами посягання при вчиненні злочинів, пов'язаних із анархістськими діями у кіберпросторі, тобто злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (розділ XVI КК України), які, як ми вже наголошували, найчастіше входять до комплексу злочинів інших класифікаційних груп. З цієї причини, а також тому, що інформаційний продукт як первинний предмет посягання не може існувати без матеріального носія, апаратним засобам, комп'ютерам, комп'ютерним мережам, мережам електрозв'язку основну увагу варто приділяти в контексті типових слідів вчинення досліджуваної категорії злочинів.

Матеріальні цінності, *що мають негативні властивості*, як-от наркотичні засоби, психотропні речовини, прекурсори, технічні засоби отримання інформації, зброя, бойові припаси та вибухові речовини виступають безпосереднім предметом посягання при вчиненні через обстановку в кіберпросторі злочинів, що порушують встановлений порядок обігу певних речей.

Про специфічні типові ознаки кожного з наведених видів майна як предмета посягання можна вести мову лише в контексті типових способів та технологій вчинення злочину в кіберпросторі. Адже предмет посягання, спосіб або технологія вчинення злочину взаємообумовлені у механізмі злочинної діяльності у кіберпросторі. Тому закономірною є поширеність одних видів майна як предметів посягання порівняно з іншими. Так, наприклад, безготівкові грошові кошти (60% проваджень) можна сьогодні назвати найпоширенішим серед майна предметом посягання у злочинах, що вчинені у кіберпросторі. Це пояснюється паралельними процесами: постійним збільшенням кількість безготівкових операцій, що проводяться через мережу Інтернет (за даними НБУ станом на 1 жовтня 2017 року складає 39,0 % всіх операцій)[1], стрімким розвитком технологій електронної

[1] Безготівкові розрахунки в Україні зростають: найчастіше українці розраховуються безготівково у торговельних мережах. *Національний банк України :* [сайт]. URL: https://bank.gov.ua/control/uk/publish/article?art_id=58370337.

комерції та банкінгу, а також їх активним пристосуванням у технологіях корисливої злочинної діяльності у кіберпросторі.

Отже, предмети злочинного посягання у кіберпросторі розподіляються на дві групи, які знаходяться у взаємозв'язку та не існують відокремлено як такі. В основі їх зв'язку знаходиться полімовтивованість злочинної діяльності у кіберпросторі.

2.3. Характеристика та взаємозв'язок типової особи злочинця й типових слідів злочинів, вчинених у кіберпросторі

Одним з обєктів дослідження криміналістики виступає злочинна діяльність, в якій «соціальний суб'єкт» займає провідне місце.[1] Саме він постає джерелом злочинної діяльності, і саме тому особа злочинця розглядається як центральний елемент у механізмі вчинення злочину, що відображається в криміналістичній характеристиці.[2]

У процесі філософського осмислення сенс поняття «особа» розкривається співвідношенням індивідуального та соціального, загального та одиничного – у напрямі від загальноабстрактного (індивіда) через особливе (індивідуальність) до конкретного (особи)[3]. Для характеристики особи І. Кант свого часу запропонував систему трьох груп ознак, зокрема: 1) задатки тваринності людини як живої субстанції, що можна підвести під загальну рубрику фізичного й суто механічного самолюбства – тобто такого, для якого не потрібно мати розум; 2) задатки людяності, які можна підвести під загальну рубрику фізичного, але порівняльного самолюбства (для чого необхідний розум), а саме схильність висновувати про себе як про щасливого або нещасного лише порівняно з іншими; 3) задатки особи як сутності істоти розумної та здатної відповідати за свої вчинки[4]. Цю систему

[1] Карпов Н. С. Злочинна діяльність : монографія. Київ : Семенко Сергій, 2004. С. 20

[2] Волобуєв А.Ф. Механізм злочину та його зв'язок з концептуальними положеннями криміналістики: монографія. Кривий Ріг: Вид. Р. А. Козлов, 2019, с. 22.

[3] Петрушенко В. Л. Філософія. Курс лекцій : навч. посіб. 2-ге вид., випр. і доповн. Київ : Каравела ; Львів : Новий світ-2000, 2002. С. 347; Валуйська М. Ю. Кримінологічна характеристика особистості злочинців, що вчинили умисні вбивства при обтяжуючих обставинах : дис. ... канд. юрид. наук : 12.00.08. Харків : ХНУВС, 2002. С. 15.

[4] Кант И. Трактаты и письма / пер. с нем. М. : Наука, 1980. С. 96.

було покладено в основу виокремлення в багатьох науках трьох груп ознак особи: біологічних, психологічних та соціальних – які залежно від предмета конкретної науки обирають її об'єктом для аналізу.

Криміналісти повністю запозичили кантівську систему ознак особи для характеристики особи злочинця. Традиційним у криміналістиці став опис особи злочинця в системі трьох груп ознак: 1) біологічних, що містять статеві, вікові, анатомічні, фізіологічні й інші ознаки; 2) психічних, що свідчать про інтелект, емоційну та вольову сфери індивіда; 3) соціальних, що характеризують його суспільний статус, професійну належність, родинний стан, місце проживання, рід занять, взаємини з іншими людьми тощо[1]. Утім такий підхід має надто описовий характер, тому втрачає сенс з позицій прагматичного значення криміналістичної характеристики та її окремих елементів. До того ж, якщо в криміналістичному дослідженні йдеться про систему ознак особи злочинця, то системно їх може бути визначено лише в характеристиці конкретної особи з метою профілактичного впливу на неї, а не індивіда (загального абстрактного чи типового злочинця). У цьому контексті науковці зауважували про потребу визначення дослідником спрямованості (мети) надання характеристики особи злочинця [2]. Більшість криміналістів вважає, що опис особи злочинця як елемента криміналістичної характеристики полягає у виявленні тих її якостей, якими зумовлено вибір саме цього виду злочину, способу його скоєння, предмета злочинного посягання, обстановки, а також мети і мотивів, обраних ним у певному випадку[3].

Будь-яка злочинна діяльність має відповідні закономірності, зумовлені об'єктивними та суб'єктивними чинниками, що відбиваються

[1] Леонтьев А. Н. Деятельность. Сознание. Личность. М. : Политиздат, 1975. С. 231; Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2003. С. 105.

[2] Ахмедшин Р. Л. Криминалистическая характеристика личности преступника. Томск : Томск. ун-т, 2005. С. 102.

[3] Бондаренко Д. А. Злочини, пов'язані з використанням владних та інших повноважень: особа злочинця як елемент криміналістичної характеристики. *Вісник Запорізького юридичного інституту.* 2000. № 2. С. 217; Біленчук П. Д. Криміналістичне дослідження обвинуваченого. Київ : УАВС, 1995. С. 8–12; Сатуев Р. С., Шраер Д. А., Яськова Н. Ю. Экономическая преступность в финансово-кредитной системе. М. : Центр экономики и маркетинга, 2000. С. 51.

в слідах[1]. Тому, з одного боку, ознаки та якості особи злочинця, що прямо впливають на регуляцію злочинної діяльності, зумовлюють природу слідів злочину, з іншого, – сам злочинець перебуває під впливом об'єктивних умов навколишнього середовища, яке може позначатися на злочинцеві вже в момент початку злочинної діяльності, що трансформує типові сліди злочину. Тому ми пристаємо до думки А. М. Кустова, що зі всієї безлічі властивостей і якостей особи злочинця для криміналістики становлять інтерес лише ті з них, що задіяні в процесі детермінації механізму злочину, зумовлюють особливості його відображальних можливостей і процесу слідоутворення й водночас зазнають на собі та відображають дію інших осіб, предметів і процесів, з якими їм доводиться взаємодіяти[2].

Для досліджуваної нами категорії злочинів навколишнім середовищем злочинця стає кіберпростір. Деякі криміналісти розглядають кіберпростір у контексті місця вчинення злочину як місця, де не діють географічні та юридичні категорії[3]. Проте це не так.

Технологічна складова кіберпростору уможливила утворення під час вчинення злочинів у кіберпросторі, крім традиційних у криміналістичному сенсі слідів (слідів-відображень, слідів-предметів та слідів-речовин[4]), також «інформаційних»[5], «віртуальних»[6] або «цифрових»[7] слідів – так званих нетрадиційних слідів, що містяться в

[1] Лук'янчиков Є. Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти) : дис. … д-ра юрид. наук : 12.00.09. Київ, 2005. С. 51.

[2] Кустов А. М. Криминалистика и механизм преступления : цикл лекций. М. : Моск. психол.-соц. ин-т ; Воронеж : МОДЭК, 2002. С. 112.

[3] Протасевич А. А., Зверянская Л. П. Особенности осмотра места происшествия по делам о киберпреступлениях. *Известия Иркутской государственной экономической академии (Байкальский госуниверситет экономики и права).* 2013. № 2. С. 23.

[4] Криминалистика : учебник / [Т. В. Аверьянова, Р. С. Белкин и др.]. М. : НОРМА-ИНФРА, 1999. 971 с.; Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 2 : Частные криминалистические теории. 464 с.

[5] Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. С. 146.

[6] Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Воронеж. гос. ун-т, 2002. С. 74–76.

[7] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

електронному середовищі[1]. Фактично ж останні у вигляді будь-яких змін інформації містяться в предметах матеріального світу – конкретних технічних або комбінованих засобах автоматизованої обробки інформації. З огляду на віддаленість доступу до предмета посягання як особливість кіберпростору, завдяки якій він набув активного використання під час вчинення злочину, аксіомою варто визнати той факт, що сліди злочину в електронному середовищі відбиваються одночасно в багатьох апаратних засобах комп'ютерної техніки, комп'ютерної мережі або телекомунікаційної мережі, мережі електрозв'язку. Останні ж фізично перебувають на чітко визначеній географічній території під юрисдикцією певної держави та у власності конкретної особи.

У цьому контексті В. В. Крилов свого часу визначав три групи слідів: сліди на машинних носіях, за допомогою яких діяв злочинець на своєму робочому місці; сліди на «транзитних» машинних носіях, за допомогою яких злочинець здійснював зв'язок з інформаційними ресурсами, що піддалися втручанню; сліди на машинних носіях інформаційної системи, до якої здійснено неправомірний доступ[2].

А. А. Протасович та Л. П. Зверянська з урахуванням сучасних умов функціонування кіберпростору наводять чотири місця вчинення кіберзлочину, відповідно до місцезнаходження слідів: 1) робоче місце, робоча станція (місце обробки інформації, що стала предметом посягання); 2) місце постійного зберігання або резервування інформації – сервер або стример; 3) місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, що має іншу локацію (може збігатися з робочим місцем, але перебувати поза межами організації, наприклад, у разі стороннього зламу шляхом віддаленого мережевого доступу); 4) місце підготовки злочину (розробки вірусу, програм зламу, добору паролів) або місце безпосереднього використання інформації (копіювання, поширення,

[1] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. С. 89.

[2] Крылов В. В. Расследование преступлений в сфере информации. М. : Городец, 1998. С. 180.

модифікації), отриманої в результаті неправомірного доступу до даних, які зберігалися[1].

Аналіз матеріалів кримінальних проваджень, відкритих за ознаками злочинів досліджуваної категорії, дає можливість свідчить про те, що при вчиненні 20 % злочинів у кіберпросторі знаходилось за межами України місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації, 40% таких злочинів – місце підготовки злочину (розробки вірусу, програм зламу, добору паролів; 10 % злочинів – місце (комп'ютер, сервер або стример) обробки інформаційного продукту як предмета посягання.

У цьому контексті варто зауважити, що для суб'єкта кіберпростору як споживача телекомунікаційних послуг обладнання є лише кінцевим елементом мережі. Такі послуги надає оператор або провайдер телекомунікацій, яких для здійснення їхньої діяльності в Україні має бути внесено до відповідного реєстру, що веде Національна комісія зі здійснення державного регулювання у сфері зв'язку та інформатизації (НКДРЗІ)[2]. Відповідно до ч. 2 ст. 27 Закону України «Про телекомунікації», право власності на телекомунікаційну мережу, а також право на її технічне обслуговування й експлуатацію належить будь-якій фізичній особі-суб'єкту підприємницької діяльності або юридичній особі, які є резидентами України, незалежно від форм власності[3]. Національні оператори та провайдери, на відміну від закордонних, зобов'язані здійснювати діяльність у сфері телекомунікацій на підставі законодавства України, серед іншого з метою сприяння проведенню оперативно-розшукових заходів, досудового та судового розгляду. Тому в процесі збирання інформації про особу злочинця для слідчого на першому плані опиняються такі питання: національні та/або закордонні оператори/провайдери забезпечували доступ злочинця до інформаційного продукту/ресурсу, який є предметом або знаряддям злочинної діяльності; електронний

[1] Протасевич А. А., Зверянская Л. П. Особенности осмотра места происшествия по делам о киберпреступлениях. *Известия Иркутской государственной экономической академии (Байкальский госуниверситет экономики и права).* 2013. № 2. С. 23–26.

[2] Реєстр операторів, провайдерів телекомунікацій. URL: http://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk.

[3] Про телекомунікації : Закон України від 18 листоп. 2003 р. № 1280-IV. URL: http://zakon0.rada.gov.ua/laws/show/1280-15/page2?text=%F0%E5%E7%E8%E4%E5%ED%F2#w15.

сервіс національної чи закордонної компанії було застосовано для вчинення злочину. Ці питання прямо пов'язані з рівнем професіональності злочинця, котрий діє в обстановці кіберпростору, на чому вважаємо за необхідне закцентувати.

В. Д. Берназ відмічає істотні зміни в характері сучасної злочинності – набирає обертів саме професіональна злочинність[1]. На це звертали увагу багато науковців, які досліджували особу так званого «комп'ютерного злочинця», однак «професіональність» зводилась до професії, іноді до мотиваційної складової злочинця. В. В. Крилов виокремлював такі самостійні типи злочинців, як «хакер», «шпигун», «терорист», «корисливий злочинець», «вандал» та «психічно хворий»[2]. Майже традиційним став розподіл комп'ютерних злочинців, які здійснювали несанкціоноване втручання в систему, за метою та сферою їх діяльності на: «хакерів» (які отримують задоволення від вторгнення в систему та її вивчення), «кракерів» (втручаються з метою завдавання шкоди системі), «фріків» (мають на меті отримання кодів доступу до послуг, паролів тощо), «колекціонерів» (колекціонують та використовують програмні продукти), «кіберкруків» (здійснюють мережеві шахрайства), «комп'ютерних піратів» (злам продуктів та їх розповсюдження за плату) й багато інших видів[3]. С. В. Кригін зазначав, що сферу діяльності злочинця не слід плутати зі спеціальністю. Дослідник наводить види злочинців за сферою діяльності («програміст», «електронник», «користувач», «обслуговуючий персонал» та «керівництво»)[4]. В. Б. Вехов як кваліфікуючу ознаку комп'ютерного злочинця використовував категорію доступу до засобів комп'ютерної техніки[5]. На думку науковця, такий вид злочинця представлений

[1] Берназ В. П. Правовое и криминалистические проблемы двойственных полномочий детективов НАБУ. *Криминалист первопечатный.* 2015. № 11. С. 56.

[2] Крылов В. В. Расследование преступлений в сфере информации. М. : Городец, 1998. С. 231–232.

[3] Комп'ютерна злочинність : навч. посіб. / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. Київ : Атіка, 2002. С. 133–134.

[4] Крыгин С. В. Расследование преступлений, совершаемых в сфере компьютерной информации : дис. … канд. юрид. наук : 12.00.09. Н. Новгород, 2002. С. 73–74.

[5] Вехов В. Б. Компьютерные преступления. Способы совершения методики расследования. М., 1996. 182 с.

двома основними групами: 1) внутрішні користувачі; 2) зовнішні користувачі як суб'єкти, що звертаються до інформаційної системи як посередника, аби отримати необхідний доступ для користування інформацією. Такий підхід загалом набув підтримки багатьох криміналістів, до кола інтересів яких належить дослідження особи комп'ютерного злочинця[1]. У цьому контексті деякі автори зазначають про злочинців як зареєстрованих (санкціонованих, законних) і незареєстрованих (несанкціонованих, незаконних) користувачів [2].

Ці позиції, безумовно, варті уваги, але сфера діяльності злочинця не завжди відображає зв'язок особи злочинця, що у кіберпросторі вчиняє злочин, з типовими слідами його вчинення. Фактично рівень професіональності конкретної особи як користувача комп'ютера зумовлює можливість змінення нею сфери діяльності.

Маркетологи з ринку праці визначають такі фахові рівні користувачів комп'ютерів: користувач, упевнений користувач, досвідчений користувач, користувач професійного рівня[3]. Критеріями такої диференціації слугують кількість програм, які опанував користувач; ступінь опанування ним кожної з програм; рівень професійної самооцінки. З урахуванням того кримінологи наводять три типи комп'ютерних злочинців: «початківці», «злочинці, що закріпились» та «професіонали»[4].

Вважаємо, що формальне застосування такого роду підходів для типізації особи злочинця, що діє у кіберпросторі, не матиме практичного сенсу з позицій формулювання типових версій про особу злочинця. Адже професійний рівень користувача не відображає всього

[1] Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.; Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків : ХНУВС, 2010. 112 с.

[2] Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. С. 152.

[3] Владения ПК и список программ для резюме Александра Грак, карьерный консультант. URL: https://www.im-konsalting.ru/blog/uroven-vladeniya-kompyuterom-dlya-rezyume.

[4] Ковалев Д. И. Криминологическая характеристика личности преступника, совершившего преступление в сфере компьютерной информации. *Вестник Академии.* 2011. № 3. С. 90–94.

спектру ознак злочинця, активно задіяних у процесі детермінації механізму злочину.

На нашу думку, слідчий на підставі аналізу слідів вчинення досліджуваної нами категорії злочину може висновувати про професіональний рівень користувача як злочинця, що зумовлений певною сукупністю ознак, як-от:

1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів);

2) мобільність злочинця (індивідуальна професійна, соціальна або географічна)[1];

3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети;

4) роль у складі організованої злочинної групи.

Розглянемо докладніше кожен з критеріїв професіональності користувача як злочинця.

1. Вільний доступ користувачів до технологій анонімізації під час роботи в мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж (VPN-технологій) та інших засобів-анонімайзерів) не означає, що кожний такий користувач використовує технологію правильно. Так, на форумах фахівці зазначають, що не можна закривати вкладку браузера з анонімайзером, а всі переходи здійснювати лише через неї (оскільки IP-адреса «фіксується» протягом усієї сесії в Інтернеті); жодним чином не можна використовувати легальні логін, пароль, поштову скриньку, реальні фотографії (відомості EXIF про фотографування), характерну для особи орфографію; необхідно враховувати специфіку дії анонімайзера (наприклад, Tor надає анонімність, а VPN приватність. Для банкінгу потрібна приватність, тому питання з приховуванням паролів відкрите, й вирішують його лише фахівці високої кваліфікації). І це лише окремі помилки, що мають наслідком викриття користувачів. Відчуття ж «невразливості» злочинця низького або середнього професіонального рівня може призвести й до більш вагомих помилок, які свідчать про ознаки злочинця.

[1] Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 37–70.

2. Мобільність означає здатність швидко орієнтуватися в ситуації, обирати найбільш доцільні форми діяльності[1]. В інформаційному суспільстві комп'ютерні мережі та інші засоби інформаційно-комунікаційних технологій сприяють глобалізації, розвитку міжнародного ринку праці, вдосконаленню різних видів індивідуальної мобільності особи[2]. Як види мобільності традиційно наводять географічну, соціальну та професійну. Географічну мобільність розглядають у контексті ринку праці: особа, діяльність якої забезпечує сфера телекомунікацій, може постійно змінювати своє географічне місцезнаходження, працювати «дистанційно». Соціальну мобільність у соціології визначено як здатність людей у суспільстві переміщуватися між різними соціальними рівнями й економічними групами (економічна мобільність)[3]. У кіберпросторі злочинець-користувач може бути суб'єктом багатьох соціальних спільнот (груп) у соціальних мережах, мати багато активних акаунтів (з англ. *account*) чи профілів, облікових записів, або ж узагалі не мати потреби в цьому. Варто додати, що географічна мобільність не завжди пов'язана з професійною, адже людина може мати високий ступінь географічної мобільності без можливості змінити особистий вибір і компетентність (роз'їзна робота з низьким рівнем професійної, соціальної та економічної мобільності)[4].

3. На важливості психологічних ознак злочинця, що впливають на формування та реалізацію злочинних цілей, у контексті окремих видів злочинів справедливо наголошував Г. А. Матусовський[5]. В. К. Гавло активно використовував термін «психолого-криміналістична характеристика злочину», маючи на увазі динамічну систему відносно стійких кількісних та якісних ознак діяльності суб'єкта злочину, що відбиває його психічні властивості, стани та процеси з підготовки,

[1] Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. С. 682.

[2] Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 40.

[3] Аніщенко В. М. Соціальна мобільність. *Енциклопедія освіти* / за ред. В. Г. Кременя. Київ : Юрінком Інтер, 2008. С. 840.

[4] Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 44.

[5] Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. С. 56.

приховування й протидії розкриттю та розслідуванню злочину[1]. Власне, автор спирається на визначені в психології три основні форми прояву психіки людини: психічні процеси, стани та властивості. Психічні властивості – це сталі психічні утворення людини, що формуються в процесі життєдіяльності, виховання та самовиховання, зокрема темперамент, характер, здібності (навички)[2]. Психічні процеси (пізнавальні, як-от відчуття, сприймання, пам'ять, мислення, уява; емоційно-вольові, як-от емоції, почуття, воля) характеризують психіку людини в ситуації «статична подія», психологічні стани (як-от бадьорість, втома, апатія, депресія, ейфорія, відчуження, нудьга, страх, відчай, сум тощо) – у ситуації «постфактум». Утім, усі ці психологічні характеристики/ознаки особи стосуються загальної роботи людської психіки[3].

Об'єктом вивчення криміналістики є діяльність злочинців, структуру якої в криміналістиці визначають через механізм вчинення злочинів. Тому в криміналістичній науці більшої підтримки набула ідея щодо визначення типових для певної сукупності (групи) осіб-злочинців психологічних характеристик, що впливають на формування і здійснення злочинних цілей, маючи високий ступінь відображення в слідах злочину. Тож, не всі психологічні ознаки злочинця є рівнозначними в контексті методики розслідування окремого виду злочинів.

Злочинцям, що діють у кіберпросторі, притаманний вольовий компонент людської психіки. Воля – це свідоме управління людиною своєю діяльністю та поведінкою, що виявляється у прийнятті рішення, подоланні труднощів і перешкод на шляху досягнення мети, виконання поставлених завдань[4]. У психології вольова поведінка закономірно передбачає вольові дії, ключовою характеристикою яких є мета і мотив. Вольові дії можуть бути простими і складними[5]. Головні ознаки вольових дій полягають у свідомому подоланні

[1] Гавло В. К. К вопросу о разработке психолого-криминалистической характеристики преступления. *Актуальные проблемы правоведения в современный период.* Томск : ТГУ, 1996. С. 185–186.

[2] Сергєєнкова О. П., Столярчук О. А., Коханова О. П., Пасєка О. В. Загальна психологія : навч. посіб. Київ : Центр учб. літ., 2012. С. 10.

[3] Там само. С. 6.

[4] Варий М. Й. Психологія : навч. посіб. 2-ге вид. Київ : Центр учб. літ., 2009. С. 151.

[5] Сергєєнкова О. П., Столярчук О. А., Коханова О. П., Пасєка О. В. Загальна психологія : навч. посіб. Київ : Центр учб. літ., 2012. С. 132.

перешкод на шляху досягнення мети; конкуруючих мотивах; наявності вольового зусилля[1]. 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 злочинної 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 тощо). Розв'язання проблеми конкуренції мотивів вчинення злочину нерозривно пов'язане з психологічними властивостями злочинця (психотипом). Тому досить 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 такого роду тестувань можуть бути досить цінними для працівників кіберполіції під час первинної перевірки інформації та слідчого з позицій визначення кола підозрюваних в установі-жертві.

4. У вітчизняній кримінально-правовій доктрині виокремлюють чотири види злочинних спільнот: 1) група без попередньої змови; 2) група з попередньою змовою; 3) організована злочинна група (ОЗГ); 4) злочинна організація. Організовані групи для вчинення таких злочинів можна додатково розподілити на суто національнальні (українські) й транснаціональні, члени яких діють на території України. Такий поділ підтверджує й практика ведення ЄРДР: відповідно до п. 4.4.3 Положення про порядок ведення ЄРДР 2012 року, окрема категорія злочинів підлягає реєстрації з додатковою

[1] Варий М. Й. Психологія : навч. посіб. 2-ге вид. Київ : Центр учб. літ., 2009. С. 153–156.

позначкою «вчинені організованими групами та злочинними організаціями з транснаціональними зв'язками» [1].

Так, згідно щорічним офіційним звітам про результати роботи підрозділів НП України, співробітниками кіберполіції в 2016 році було виявлено 2 організовані групи і злочинні організації, що діяли на території України, загалом щодо них зареєстровано 65 епізодів тяжких та особливо тяжких злочинів; у 2017 році – 7 організованих груп і злочинних організацій, з них 4 групи з межрегіональними зв'язками, відповідно 166 епізодів тяжких та особливо тяжких злочинів; станом на 1 листопада 2018 року – 9 груп, з них 1 група з межрегіональними зв'язками, 1 група з транснаціональними, зареєстровано 116 тяжких та особливо тяжких злочинів. Ці показники утворюються на підставі матеріалів кримінальних проваджень, які мають перспективу судового розгляду (коли окремим членам груп оголошено підозру). Реальна ж кількість таких груп залишається поза офіційної статистики, адже лише аналіз обраних злочинцем ресурсів як предметів посягання та способів (методів) дії дозволить висновувати про недоступність останніх для одинака або малої групи осіб, а тому про вчинення злочину організованою групою осіб.

Стосовно комп'ютерних злочинів Н. Н. Шилан, Ю. М. Кривоніс і Г. М. Бірюков констатували багаторівневість та ієрархічність організованих злочинних груп[2]. Місце або роль кожного з членів групи визначаються за його професіональними та особистими психологічними якостями. Аналіз судово-слідчої практики підтверджує, що найкраще така закономірність виявляється у транснаціональних організованих групах, ведення відповідного обліку сприяє всебічному дослідженню цього питання. Таким чином, явище «транснаціональності злочинної діяльності у кіберпросторі» потребує окремої уваги.

У науковій літературі криміналістичного спрямування «комп'ютерні злочини», або «кіберзлочини» досить часто наділяють

[1] Про Єдиний реєстр досудових розслідувань : наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69. URL: https://zakon.rada.gov.ua/rada/card/v0069900-12.

[2] Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации. Луганск : РИО ЛИВД, 1999. С. 22.

ознаками «транснаціональних злочинів»[1] чи «транскордонних злочинів»[2]. Утім, ці поняття є різними. Термін «транскордонність» у наукових публікаціях характеризує ситуацію, коли особа здійснює протиправне діяння, перебуваючи фізично в одній державі, тоді як предмет злочинного посягання наявний у іншій[3]. У цьому сенсі ми включили до характеристики злочинця такий критерій його професіональності, як мобільність.

У контексті ж транснаціональної організованої групи осіб видається доречним звернутися до ст. 3 Конвенції ООН проти транснаціональної організованої злочинності 2000 року, де чітко визначено ознаки злочинної діяльності організованої злочинної групи, що має транснаціональний характер, зокрема: а) злочин вчинено в більш, ніж одній державі; б) злочин вчинено в одній державі, але переважна більшість заходів з його підготовки, планування, керівництва або контролю відбувалася в іншій державі; в) злочин вчинено в одній державі, але за участю організованої злочинної групи, що здійснює злочинну діяльність у більш, ніж одній державі; г) злочин вчинено в одній державі, але істотні наслідки цього вчинення наявні в іншій державі[4]. У ст. 2 Конвенції організовану злочинну групу трактовано як структурнооформлену групу в складі трьох чи більше осіб, що існує впродовж визначеного періоду часу та діє узгоджено з метою вчинення

---

[1] Зелінська Н. А. Міжнародно-правова концепція міжнародного злочину : автореф. дис. … д-ра юрид. наук : 12.00.11. Київ, 2007. С. 8.

[2] Биленчук П. Д., Еркенов С. Е., Кофанов А. В. Транснациональная преступность: состояние и трансформация : учеб. пособие / под ред. П. Д. Биленчука. Киев : Атика, 1999. С. 91.

[3] Осипенко А. Л., Кушниренко С. И. Правовые и организационные основы международного сотрудничества в противодействии трансграничным преступлениям, совершаемым с использованием Интернета. *Современное право.* 2008. № 8. С. 38.

[4] Конвенція ООН проти транснаціональної організованої злочинності 2000 року : Резолюція 55/25 ГА ООН від 15 листоп. 2000 р. *Збірник міжнародних договорів України про правову допомогу у кримінальних справах. Багатосторонні договори.* Київ, 2006. С. 554–606; Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів суходолом, морем і повітрям) : Закон України від 4 лют. 2004 р. № 1433-IV. *Відомості Верховної Ради України.* 2004. № 19. Ст. 263.

одного або декількох серйозних злочинів чи злочинів, визнаних такими Конвенцією, щоб одержати (прямо чи опосередковано) фінансову або іншу матеріальну вигоду. Як «серйозний злочин» у ратифікації Конвенції в Україні варто розуміти «тяжкий» і «особливо тяжкий злочин»[1]. У самій Конвенції транснаціональними визначено дії, що пов'язані з перешкоджанням здійсненню правосуддя, відмиванням доходів від злочинів та корупцією.

Тож, злочини у кіберпросторі ми вважаємо вчиненими транснаціональними організованими групами за таких умов: 1) доведено участь у злочинній діяльності трьох і більше осіб; 2) кваліфікація за національним кримінальним законодавством як тяжкого та особливо тяжкого злочину; 3) доведено наявність умислу щодо отримання матеріальної та фінансової вигоди; 4) відповідність визначеним у Конвенції ООН проти транснаціональної організованої злочинності 2000 року ознакам трансаціональності[2]. Водночас усі кіберзлочини або дії, передбачені XVI КК України, не можна безапеляційно вважати транснаціональними, адже такі злочини в переважній своїй кількості не є тяжкими, виняток становлять лише дві форми дій (вчинені повторно чи за попередньою змовою групою осіб, або якщо ними заподіяно значну шкоду): 1) створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ч. 2 ст. 361-1); 2) несанкціонований збут або розповсюдження інформації з обмеженим доступом (ч. 2 ст. 361-2).

У результаті аналізу матеріалів судово-слідчої практики можна визначити, що в Україні були зареєстровані випадки вчинення транснаціональними ОЗГ таких класифікаційних підгруп злочинів у кіберпросторі: злочини, спрямовані на заволодіння чужим майном, та пов'язані з ними злочини у сфері функціонування електронних

[1] Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів суходолом, морем і повітрям) : Закон України від 4 лют. 2004 р. № 1433-IV. *Відомості Верховної Ради України.* 2004. № 19. Ст. 263.

[2] Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* 2015. № 4. С. 411.

розрахунків (ст. 185, 191, 200 КК України); злочини, пов'язані з насильницько-егоїстичними діями (ст. 149, 301) та злочини, пов'язані із анархістськими діями у кіберпросторі: злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ч. 2 ст. 361-1).

Криміналістичні аспекти щодо ролей учасників таких організованих груп перетинаються з кримінологічним дослідженням мережевої або корпоративної моделі як видів організованої групи, що протиставляються між собою[1]. Корпоративній моделі притаманна централізована система, що має авторитарний характер; її схема є вертикаллю влади, елементи моделі можуть існувати паралельно з реальними структурами суспільства (державними або приватними). Для злочинних мереж, на відміну від корпоративних утворень, характерні непостійне членство й висока адаптивність до політичних, економічних і соціальних змін, що відбуваються в суспільному житті, без централізованої системи контролю[2]. А. Л. Осипенко наводить визначальні чинники діяльності таких груп: 1) гнучке керування; 2) відносна рівноправність учасників групи, можливість змінення статусу (ролі) залежно від ситуації; 3) здатність до швидкого змінення складу групи та перерозподілу ролей; 4) швидкість відновлення втрачених злочинних зв'язків; 5) здатність виконувати те саме злочинне завдання застосуванням різного комплексу дій[3]. Злочинець виконує певну роль у корпоративній або мережевій злочинній групі залежно від свого професіонального рівня.

З огляду на вищенаведені теоретичні позиції, спираючись на узагальнення матеріалів національної судово-слідчої практики й на підставі охарактеризованих нами критеріїв визначення

[1] Транснациональная организованная преступность: дефиниции и реальность : монография / отв. ред. В. А. Номоконов. Владивосток : Дальневост. ун-т, 2001. С. 81; Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности : монография. Харьков : Нац. ун-т внутр. дел, 2002. 412 с.

[2] Транснациональная организованная преступность: дефиниции и реальность : монография / отв. ред. В. А. Номоконов. Владивосток : Дальневост. ун-т, 2001. С. 92–93.

[3] Осипенко А. Л. Организованная преступность в сети Интернет. *Вестник Воронежского Института МВД России.* 2012. № 3. С. 14.

професіональності (кваліфікації) злочинця, можна певним чином типізувати особу, що вчиняє злочин у обстановці кіберпростору.

Злочинець – користувач початкового рівня з урахуванням своїх професійних навичок роботи з комп'ютером не використовує технології анонімізації доступу до ресурсів Інтернет; характеризується високою соціальною мобільністю з різних причин (нереалізованість комунікаційних потреб (людина з обмеженими фізичними можливостями, наявність психічних хвороб), наявність географічної мобільності, за відсутності професійної та економічної мобільності (сезонний працівник; робота за кордоном вахтовим методом; кур'єр; водій; сортувальник тощо, причому злочинець виконує роботи низької кваліфікації)). Проблеми конкуренції мотивів вчинення злочину він не має, його злочинна діяльність зазвичай становить собою елементарну вольову дію, як-от розміщення в мережі Інтернет інформації певного місту.

Злочинець такого типу вчиняє в кіберпросторі злочини, пов'язані з насильницько-егоїстичними чи насильницько-дискримінаційними діями; окремі види злочинів з антидержавно-політичних мотивів (злочини проти основ національної безпеки України; злочини, пов'язані з тероризмом; пропаганда війни й поширення комуністичної, нацистської символіки та пропаганда комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів). Звернемося до прикладу[1]. Мешканець Херсонської області гр. К., зареєстрований як користувач соціальної мережі «ВКонтакте» «Інтернет ресурс» - «http://vk.com» під своїм «нік-неймом», у період з 25 березня 2011 року до 03 жовтня 2014 року на особистій сторінці в розділі «Новини», переглядаючи відеофайли, розміщені невстановленою особою в розділі «Новини» зазначеної соціальної мережі, яку технічними та іншими засобами встановити неможливо, що за висновком експерта містять ознаки порнографії та належать до продукції порнографічного характеру, за допомогою функції «додати в мої відеозаписи», надав загальний доступ для перегляду до цих десяти відеозаписів користувачам соціальної мережі.

[1] Вирок Старокостянтинівського районного суду Хмельницької області від 21 берез. 2017 р. Справа № 683/444/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/65809534.

К. було засуджено за вчинення злочинів, передбачених ч. 2 ст. 300, ч. 2 ст. 301 КК України.

Вчиняючи злочини з антидержавно-політичних мотивів, вони можуть діяти як самостійно, так і в складі корпоративної злочинної групи, виконуючи роль організатора, виконавця чи посібника. Так, наприклад, упродовж травня-липня 2014 року гр. О., діючи за попередньою змовою з іншими невстановленими особами, через соціально спрямовані Інтернет-ресурси «ВКонтакте», «Одноклассники», «Facebook», програми «Skype», «Viber», з використанням мобільного зв'язку організовував акції протесту проти дій органів державної влади України в містах Києві, Львові, Тернополі, Кіровограді, Запоріжжі, Дніпропетровську, Одесі, Миколаєві, Херсоні, Полтаві, Миргороді, залучаючи до цього мешканців різних регіонів України[1]. Також він організовував їх фінансування, детально інструктував щодо порядку проведення акцій, бажаного результату, обов'язкового використання засобів масової інформації, як місцевих, так і загальнодержавних, вимагав складання й направлення йому фото- та відеозвітів про виконану роботу, а також ставив завдання щодо залучення учасників акцій.

Таких злочинців працівники правоохоронних органів найчастіше виявляють під час оперативно-розшукової діяльності. Унаслідок вчинення злочинцем-користувачем початкового рівня злочину зазвичай залишаються такі сліди:

– нетрадиційні (цифрові) - в комп'ютері злочинця у вигляді змін у файловій системі, спеціального програмного забезпечення, інформації на зйомних носіях;

– нетрадиційні (цифрові) – на сервері національного оператора або провайдера у вигляді спеціальних файлів реєстрації, так званих Log-файлах, де відбувається протоколювання технічної інформації, що містить відомості про технічний обмін, бази даних;

– традиційні (матеріальні) сліди у вигляді документів (офіційних та неофіційних).

Злочинець – звичайний користувач. Якщо злочинець і використовує технології анонімізації доступу до ресурсів мережі

[1] Вирок Тернопільського міськрайонного суду Тернопільської області від 19 лют. 2016 р. Справа № 607/16616/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/55977478.

Інтернет (часто Tor), то припускається вагомих помилок, що зводять нанівець його намагання бути анонімним у мережі. Фахівець з комп'ютерного обладнання та мереж під час побіжного аналізу комп'ютера жертви й мережі досить легко визначить фактичні відомості про особу, котра здійснювала певну операцію. Усі види мобільності (географічна, соціальна, професійна та економічна) мають усереднені схожі показники. Втім, розглядаючи географічну мобільність у контексті ринку праці, слід визнати нетиповість «дистанційної роботи» такої особи. Конкуренція мотивів наявна лише за умови діяльності його в складі мережевої злочинної групи: коли він приймає рішення щодо подальшого виконання ролі в групі або вчинення іншого злочину, виявляючи ознаки організатора однієї зі складових мереж мережевої групи. Злочинець такого типу часто вчиняє в кіберпросторі злочини, віднесені до таких класифікаційних підгруп: злочини, що порушують встановлений порядок обігу певних речей; інтелектуальне піратство, злочини, пов'язані з комунікаційними діями. Показовою можна вважати діяльність гр. А., який у квітні 2015 року створив Інтернет-сайти з метою отримання прибутку від розміщеної на сайті реклами. Оскільки рекламні сайти як такі не користуються попитом серед користувачів Інтернету, для привернення уваги на своїх сайтах А. надавав користувачам можливість перегляду фільмів у режимі «он-лайн». Загальна сума збитків, спричинених власникам авторських прав наданням доступу до аудіовізуальних творів компаній «Twentieth Century Fox Film Corporation» та «Universal City Studios LLLP» (Universal) на сайтах «live-films.in.ua» та «kinozal.biz.ua» («kinozal.tech»), становила 2 363 398 грн[1].

Трапляються випадки вчинення зловмисниками злочинів з антидержавно-політичних мотивів, пов'язаних з державно-політичною сферою відносин суб'єктів у кіберпросторі. До прикладу, гр. К. за місцем проживання через можливості провайдера ТОВ «ПТК» з використанням встановленого на його ноутбуці Інтернет-браузера «Opera» з активованим сервісом «VPN» авторизувався в соціальній Інтернет-мережі «ВКонтакте» та від імені створеного ним

[1] Вирок Ковпаківського районного суду м. Суми від 1 черв. 2017 р. Справа № 592/4835/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/66841350.

аккаунта розповсюдив репости записів із закликами до змінення меж території та державного кордону України, порушуючи порядок, встановлений Конституцією України[1].

Інтерес працівників правоохоронних органів до такого злочинця виникає найчастіше під час проведення оперативно-розшукової діяльності (оперативної розробки). Після вчинення злочину злочинець-звичайний користувач залишає такі типові сліди:

– нетрадиційні - в комп'ютері на робочому місці злочинця у вигляді змін у файловій системі та наявності певного спеціального програмного забезпечення, інформації на зйомних носіях;

– нетрадиційні - в сервері, в комп'ютері-жертви у вигляді змін в оперативному запам'ятовуючому пристрої, у конфігурації, позаштатних режимів роботи;

– нетрадиційні - на серверах національного та/або закордонного оператора/провайдера у вигляді спеціальних файлів реєстрації, баз даних;

– традиційні матеріальні сліди у вигляді слідів-предметів (офіційних та неофіційних документів); речей, що мають особливий порядок обігу (спеціальні технічні пристрої, зброя тощо); слідів-відображень (відбиток пальця, мікрочастка одягу на засобах комп'ютерної техніки та поруч з ними); слідів-речовин (наркотичні засоби; прекурсори, вибухова речовина тощо).

Злочинець – упевнений користувач зазвичай пов'язаний з організацією-жертвою за трудовою угодою або має особисті стосунки з фізичною особою-жертвою (90% матеріалів), через це має доступ до інформації, необхідної для вчинення злочину (ідеться про паролі, адреси, коди доступу, назву файлу, шлях до нього тощо). Втім цей факт не заважає йому досить вдало використовувати технології анонімізації доступу до ресурсів мережі Інтернет з метою приховування злочинної діяльності, створення ілюзії віддаленого доступу до предмета посягання. Серед видів мобільності переважають соціальна та професійна, інші з них мають середні показники. Злочинець означеного типу традиційно вчиняє в кіберпросторі злочини, спрямовані на заволодіння чужим майном та пов'язані з

[1] Вирок Київського районного суду м. Одеси від 24 січ. 2018 р. Справа № 520/316/18. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/71757839.

ними злочини у сфері функціонування електронних розрахунків; злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції; інтелектуальне піратство та злочини, пов'язані з комунікаційними діями; злочини пов'язані з анархістськими діями в кіберпросторі. До речі, 80 % матеріалів кримінальних проваджень стосовно наведеної категорії злочинів кваліфікуються за сукупністю статей, де обов'язковим елементом постають злочини, пов'язані з анархістськими діями в кіберпросторі, що передбачені розділом XVI КК України. Такий злочинець приблизно в половині випадків діє в складі корпоративної організованої групи як виконавець злочину.

Розглянемо приклад[1]. Гр. А., перебуваючи на посаді старшого оперуповноваженого з особливо важливих справ інформаційно-моніторингового відділу Управління координації та моніторингу ризиків Головного управління внутрішньої безпеки Міністерства доходів і зборів України, діючи умисно, з корисливих мотивів з вересня 2013 року до лютого 2014 року на початку кожного місяця, перебуваючи в м. Києві, неодноразово здійснював несанкціонований збут інформації з обмеженим доступом щодо експортно-імпортних операцій на митній території України, що зберігається в Єдиній автоматизованій інформаційній системі (ЄАІС) Міндоходів, громадянину України Б. за щомісячну грошову винагороду в розмірі від 1000 до 2000 гривень. Несанкціоноване копіювання інформації здійснювалося з робочого місця іншої особи без відома та за відсутності останньої. Для входу в ЄАІС А. використовував свій особистий логін та пароль. Збут інформації відбувався шляхом завантаження файлів з інформацією за допомогою комп'ютерної техніки, розташованої в різних місцях через ресурси «http://rusfolder.ru», «http://www/sendspace.com» («файлообмінники»). Надалі пароль для їх завантаження покупець отримував через електронну поштову скриньку під час електронного листування. Окремо надавався пароль для розархівування файлів. З метою приховування своєї протиправної діяльності, досягнення максимальної конспірації та уникнення відповідальності за скоєні дії А. за реалізовані

[1] Вирок Шевченківського районного суду м. Києва від 23 квіт. 2014 р. Справа № 761/10994/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/38502750.

ним інформаційні масиви з обмеженим доступом отримував грошові кошти через «електронні гаманці» системи «WebMoney Transfer», зокрема, за реквізитами, зареєстрованими ним на вигаданих осіб. Кінцевим рахунком для отримання грошових коштів у готівковій формі був «електронний гаманець» за реквізитами А.

Типовим первинним джерелом інформації про такого злочинця стає заява або повідомлення про вчинення кримінального правопорушення. Унаслідок вчинення злочину «злочинцем-упевненим користувачем» зазвичай залишаються такі сліди:

– нетрадиційні – в комп'ютері, який застосовував злочинець, у вигляді змін у файловій системі, спеціальне «хакерське» програмне забезпечення;

– нетрадиційні – в комп'ютері-жертві у вигляді змін в оперативному запам'ятовуючому пристрої, у конфігурації, позаштатних режимів роботи;

– нетрадиційні – на серверах, частіше національного оператора/провайдера у вигляді спеціальних файлів реєстрації, баз даних;

– традиційні – матеріальні сліди у вигляді слідів-предметів (офіційних та неофіційних документів); додаткових технічних пристроїв; спеціалізованої конфігурації обладнання, нестандартного периферійного обладнання); слідів-відображень та слідів-речовин (фарба для принтера, порошки та змазки для техніки; клеї, чистий пластик і фарби для виготовлення підроблених банківських пластикових карток тощо).

Злочинець – досвідчений користувач. Між досвідченим та впевненим злочинцем-користувачем відмінності є незначними. Це пов'язано з тим, що впевнений злочинець має високий рівень професійної мобільності й у разі невикриття правоохоронними органами першого вчиненого ним злочину він підвищує свій професійний рівень, часто відмовляється від участі в організованій злочинній групі та розпочинає індивідуальну злочинну діяльність. Як фахівець високої кваліфікації він використовує технології анонімізації доступу до ресурсів мережі Інтернет, через що має високий ступінь географічної мобільності. Злочинну діяльність вчиняє шляхом складної вольової дії, тому завжди наявна конкуренція мотивів. Встановлення під час досудового розслідування факту наявності конкуренції мотивів злочинця та шляхів розв'язання цієї проблеми

дозволить надалі зазначити необхідність залучення слідчим психолога з метою визначення психотипу, складання психологічного портрету злочинця. Для злочинця означеного типу характерним є вчинення злочинів, спрямованих на заволодіння чужим майном та пов'язаних з ними злочинів у сфері функціонування електронних розрахунків; злочинів, що порушують механізми захисту від монополізму та недобросовісної конкуренції: інтелектуального піратства та злочинів, пов'язаних із комунікаційними діями. Аналогічно до попереднього типу, понад половина таких злочинів підлягають кваліфікації за сукупністю зі статтями розділу XVI КК України (класифікаційна підгрупа злочинів, пов'язаних з анархістськими діями в кіберпросторі). Комплекс слідів злочину, які залишає досвідчений користувач, майже аналогічний до слідів, залишених упевненим користувачем, на відміну до того, що нетрадиційні сліди найчастіше залишаються на серверах закордонного оператора/провайдера.

Так, у м. Біла Церква Київської області гр. Н. з метою здійснення DDoS-атак на будь-які сервери за винагороду завантажив та скопіював на жорсткий диск свого компютера з Інтернету програмне забезпечення, необхідне для організації та проведення DDoS-атак за назвою «Bleck Energy», що надавало йому можливість здійснювати DDoS-атаки на обрані ним сервери, IP-адреси та ресурси[1]. Виконавши тестування зазначеного програмного продукту, Н., спілкуючись на сторінках форуму «xakerok.org», від невстановленої слідством особи отримав додатковий спеціальний «файл динамічної бібліотеки» «*.dll», після чого програмний продукт «Bleck Energy» став повністю придатним для здійснення DDos-атак. Також від невстановленої слідством особи на ім'я «Botnetman» зловмисник отримав так званий «Botnet» (файл управління комп'ютерами, зараженими вірусами), що надавав можливість одночасно з 1000 комп'ютерів здійснити звернення на той чи інший сервер,

IP-адресу чи ресурс у мережі Інтернет, таким чином паралізувавши його роботу. 21.02.2008 р. Н. за допомогою ICQ (програма для відправлення повідомлень у мережі Інтернет) з № 475917365

[1] Вирок Білоцерківського міськрайонного суду Київської області від 5 жовт. 2010 р. Справа № 1-7/2010. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/63156830.

(псевдонім «Botanik») та № 400349 (без псевідоніму) на форумах сайту «www.xakery.ru» розмістив оголошення в розділі «DDoS service» з приводу проведення DDoS-атак на будь-які сервери за винагороду. 04.07.2008 р. на ці оголошення на ICQ №475917365 до Н. від невстановленої слідством особи, представленої під псевдонімом «Wolf», надійшло замовлення на проведення DDoS-атаки на сервери за різними IP-адресами, належними ТОВ «ОСМП», ТОВ «Кіберплат Україна». Виконуючи заказ, Н. увійшов у глобальну мережу Інтернет на ресурс «www.cxim.inattack.ru/www2/www» та за допомогою програми «Bleck Energy» протягом доби здійснював DDoS-атаки на сервери зазначених компаній, за що від «Wolf» на зареєстрований у мережі Інтернет гаманець в електронній платіжній системі отримав винагороду в розмірі 100000 рублів, які згодом перевів у гривні на власну платіжну картку.

Злочинець – користувач-професіонал. Здатність такого злочинця до використання технологій анонімізації доступу до ресурсів Інтернет, індивідуальна професійна, соціальна та географічна мобільності злочинця, складність його злочинної діяльності (що визначає психотип злочинця) наділені найбільш високим рівнем кваліфікації. Це вимагає максимальної концентрації зусиль працівників поліції, залучення до розслідування значної кількості спеціалістів різного фаху, здійснення діяльності в межах міжнародного співробітництва. Для слідчого або кіберполіцейського в процесі розслідування відповідної злочинної діяльності ключовою обставиною слугуватиме участь злочинця такого типу в складі організованої групи або злочинної організації з транснаціональними зв'язками. Як приклад можна навести групу так званих «балаківських хакерів», діяльність яких було докладно описано в російських джерелах інформації[1]. Організована група осіб у 2003 році здійснювала кібератаки на інтернет-сайти дев'яти букмекерських британських компаній. Їх web-сторінки було заблоковано й робота припинилася. Для розблокування роботи сторінки злочинці вимагали передати гроші.

За матеріалами анкетування практичних працівників поліції та аналізу матеріалів оперативної і слідчої практики можна визначити

[1] Черкасов В. Н. Дело «балаковских» хакеров. Факты и размышления. *Информационная безопасность регионов.* 2009. № 2 (5); 2010. № 1 (6); 2010. № 2 (7); 2011. № 1 (8). С. 158–163.

три закономірності злочинної діяльності осіб відповідного типу: 1) «професіонал» зазвичай є одним з організаторів у структурі мережевої організованої групи, створеної для вчинення злочинів з корисливих мотивів, пов'язаних з фінансово-економічною сферою відносин у кіберпросторі (70% респондентів), та з соціально-економічних мотивів, пов'язаних з соціальною сферою відносин суб'єктів (50% респондентів); 2) «професіонал» типово вчиняє на замовлення третьої особи будь-який зі злочинів з антидержавно-політичних мотивів або ідейних мотивів, пов'язаних зі світоглядною сферою; 3) злочини, пов'язані з анархістськими діями в кіберпросторі, «професіонал» може вчиняти одноособово (за відсутності сукупності зі злочином іншої класифікаційної підгрупи досліджуваної категорії злочинів). Втім через брак матеріалів практики щодо фактичного притягнення до кримінальної відповідальності на території України «професіоналів» визначені статистичні показники у наведених закономірностях чітко визначити на цей час неможливо.

Як приклад маємо такий випадок[1]. У Херсонській області за вчинення кримінального правопорушення, передбаченого ч. 2 ст. 361-1 КК України, до відповідальності було притягнуто двох осіб. Гр. А., маючи спеціальні технічні знання у сфері програмування, за допомогою невстановленого досудовим розслідуванням комп'ютера з метою використання та розповсюдження на базі операційної системи «Android» створив програмне забезпечення за назвою «grafon.apk» та файл «restricted» для мобільних комп'ютерів, після чого передав гр. Б. логін і пароль доступу до панелі управління зазначеного програмного забезпечення. У невстановлений слідством день і час у травні 2016 року через панелі управління бот-мережею ШПЗ «SexDrugWokrug.apk», використовуючи невстановлений досудовим розслідуванням комп'ютер, А. використав і розповсюдив через низку власних сайтів зазначене програмне забезпечення з метою отримання віддаленого доступу та проведення несанкціонованих операцій з платіжними засобами українських і зарубіжних користувачів та подальшого виведення грошових коштів із вказаних платіжних засобів

[1] Вирок Луцького міськрайонного суду Волинської області від 1 берез. 2018 р. Справа № 161/1345/18. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/72886703.

через систему миттєвих інтернет-розрахунків «WebMoney Transfer» на власні банківські рахунки.

Інформацію про вчинення кримінального правопорушення злочинцем такого типу вдається отримати в результаті проведення оперативно-розшукової діяльності працівниками правоохоронних органів, а також під час діяльності в порядку надання міжнародної правової допомоги. При цьому нетрадиційні й традиційні сліди злочину зазвичай містяться на місці підготовки до злочину (розробки вірусу, програм зламу, добору паролів) та місці (комп'ютері, сервері або стримері) обробки інформаційного продукту як предмета посягання.

Видається, що наведена типізація особи злочинця дозволить визначити закономірні зв'язки в системах «злочинець-організована група», «типові сліди-злочинець» та «злочинець-специфіка злочинної діяльності», що значно сприятиме роботі слідчих та працівників кіберполіції в контексті встановлення комплексу взаємопов'язаних злочинів, вчинених у кіберпросторі.

2.4. Характеристика типових способів/технологій вчинення злочинів у кіберпросторі

Вчення про спосіб вчинення злочину ілюструє розвиток криміналістики як науки. Первісне формування окремих методик розслідування відбувалося на підставі дослідження даних про спосіб злочину, за загальним принципом Б. М. Шавера «від способу вчинення злочину – до методу його розкриття»[1]. Способом вчинення злочину в криміналістиці традиційно вважають об'єктивно і суб'єктивно зумовлену систему поведінки суб'єкта до, під час та після скоєння злочину[2].

Аналіз публікацій щодо методик розслідування свідчить про те, що типізація способів вчинення будь-якого виду злочинів базується на емпіричних даних з подальшим переходом до їх аналітичного опрацювання, що дає можливість визначити типові й специфічні

[1] Шавер Б. М. Об основных принципах частной методики расследования преступлений. *Социалистическая законность.* 1938. № 1. С. 47; Барцицька А. А. Криміналістичні технології: сутність та місце в системі криміналістичної науки : дис. … канд. юрид. наук : 12.00.09. Одеса, 2011. С. 147.

[2] Криминалистика / под ред. Н. П. Яблокова, В. Я. Колдина. М. : МГУ, 1990. С. 327.

прийоми підготовки, вчинення та приховування такого злочину. Тим самим створюється інформаційне підґрунтя для подальшого пізнання механізму вчинення злочину конкретного виду.

Способи вчинення злочинів у обстановці кіберпростору як самостійна категорія є малодослідженими в криміналістичній науці. Водночас необхідно визнати, що абсолютна більшість криміналістів здійснювала висвітлення способів вчинення суто комп'ютерних злочинів шляхом їх різноманітних класифікацій, як-от: вид комп'ютерного злочину[1], тип комп'ютерного захисту[2], метод виконання злочинцем тих чи інших дій, спрямованих на отримання доступу до засобів комп'ютерної техніки[3]. Причому в більшості авторських класифікацій способів вчинення таких злочинів ужито термінологію, запропоновану ще в 1991 році Генеральним Секретаріатом Інтерполу в так званому кодифікаторі комп'ютерних злочинів, де кожний спосіб злочину позначено власним ідентифікатором у вигляді комплексу літер, першою з яких є літера «Q»[4]. Для опису злочину використовують п'ять груп кодів, зокрема:

1) QA – несанкціонований доступ і перехоплення (QAH – комп'ютерний абордаж, QAI – перехоплення, QAT – крадіжка часу, QAZ – інші види несанкціонованого доступу і перехоплення);

---

[1] Крылов В. В. Расследование преступлений в сфере информации. М. : Городец, 1998. С. 228; Снігерьов О. П., Голубєв В. О. Проблеми класифікації злочинів у сфері комп'ютерної інформації. *Вісник Університету внутрішніх справ МВС України.* 1999. № 5. С. 25–28; Настільна книга слідчого / редкол.: В. Я Тацій, М. Г. Панов, В. Ю. Шепітько. Київ : Ін Юре, 2003. С. 563–565.

[2] Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М. : Мир, 1999. С. 51–82.

[3] Батурин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991. С. 85–99; Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посіб. Київ : Укр. акад. внутр. справ, 1994. С. 24–25; Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М. : Право и Закон, 1996. С. 55–104.

[4] Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2001. 496 с.; Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М., 1998. 256 с.

2) QD – змінення комп'ютерних даних (QDL – логічна бомба, QDT –троянський кінь, QDV – комп'ютерний вірус, QDW – комп'ютерний черв'як, QDZ – інші види змінення даних);

3) QF – комп'ютерне шахрайство (QFC – шахрайство з банкоматами, QFF – комп'ютерна підробка, QFG – шахрайство з ігровими автоматами, QFM – маніпуляції з програмами введення-виведення, QFP –шахрайство з платіжними засобами, QFT – телефонне шахрайство, QFZ – інші комп'ютерні шахрайства);

4) QR – незаконне копіювання (QRG – комп'ютерні ігри, QRS – інше програмне забезпечення, QRT – топографія напівпровідникових виробів, QRZ – інше незаконне копіювання);

5) QS – комп'ютерний саботаж (QSH – з апаратним забезпеченням, QSS – із програмним забезпеченням, QSZ – інші види саботажу);

6) QZ – інші комп'ютерні злочини (QZB – з використанням комп'ютерних дошок оголошень, QZE – розкрадання інформації, що становить комерційну таємницю, QZS – передача інформації конфіденційного характеру, QZZ – інші комп'ютерні злочини).

Вітчизняні науковці, використовуючи в своїх дослідженнях наведені лексичні конструкції як найбільш уживані в міжнародній практиці обліку злочинів, вдаються до деталізації окремих з них за допомогою спеціальної технічної термінології. Так, спираючись на позиції комп'ютерної вірусології, криміналісти намагалися додатково класифікувати способи змінення комп'ютерних даних шляхом застосування комп'ютерного вірусу залежно від його виду («вірус-супутник», «файл-спутник», «вірус-черв'як», «вірус-паразит», «студентський вірус», «вірус-невидимка», «вірус-привид-мутант», «комбіновані віруси»)[1]. Кожен з цих вірусів має свою специфіку, втім згодом розробляють нові віруси з іншим принципом дії, наприклад, на цей час набуло поширення використання так званого «вірусу-криптомайнера», що таємно від користувача, наприклад, у момент відкриття будь-якого файлу, встановлює «програму-клієнта», що під'єднується до одного з майнинг-пулів і починає здобувати будь-яку з криптовалют. Майнинг-пули часто самі добирають відповідний

[1] Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч посіб. / за ред. Р. А. Калюжного. Запоріжжя : ГУ ЗІДМУ, 2002. С. 118–120.

варіант валюти для конкретної конфігурації обладнання користувача. Так, у Луганській області у 2018 році працівниками кіберполіції було викрито діяльність 20-річного мешканця міста Рубіжне, який, маючи навички у сфері програмування і роботи з комп'ютерним програмним забезпеченням, створив такий шкідливий програмний засіб та впродовж 2017 року поширював його через Інтернет з метою видобування криптовалюти Monero (XMR), яка має власну номінальну вартість у разі її обміну на національну валюту України або національну валюту іншої держави[1].

Деталізації підлягають також способи несанкціонованого доступу, зокрема, зазначається про різноманітні види атак через Інтернет із застосуванням методів соціальної інженерії (як-от отримання доступу до інформації про комп'ютерну систему шляхом попередньої диверсії, рекламування користувачеві способів усунення несправностей, надання допомоги з боку злочинця)[2].

У публікаціях колективу працівників Міжвідомчого науково-дослідного центру з проблем боротьби з організованою злочинністю при РНБО України під час огляду видів протиправних дій у сфері використання платіжних карток детально розкрито способи збирання інформації про справжні платіжні картки, виготовлення та розповсюдження підроблених платіжних карток, способи шахрайських дій у сфері використання платіжних засобів та банкоматів (використання загублених або викрадених карток; використання не одержаних держателем карток; використання одержаних за підробленими документами; умисні перевитрати за рахунками; використання інформації про справжні платіжні картки для оплати поштових, телефонних або інтернет-замовлень; використання справжніх карток у діяльності фіктивних підприємств з обслуговування рахунків; зловживання працівниками банківських

[1] В Луганской области полиция разоблачили хакера, который создал и распространил вредоносный вирус-майнер. URL: https://www.ukrinform.ru/rubric-regions/2498815-policia-razoblacila-hakera-kotoryj-sozdal-vredonosnyj-virus-dla-majninga.html.

[2] Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч посіб. / за ред. Р. А. Калюжного. Запоріжжя : ГУ ЗІДМУ, 2002. С. 146–158.

структур; шахрайства з використанням повністю підроблених карток за методом «чистий пластик»)[1].

Науковці часто уникають опису способів вчинення традиційних злочинів у кіберпросторі[2] або розглядадають способи, наведені В. Б. Вєховим[3]. Адже монографія «Компьютерные преступления: способы совершения и раскрытия», видана науковцем у 1996 році, донині залишається однією з тих, що містить найбільш повну класифікацію способів дій, спрямованих на отримання доступу до засобів комп'ютерної техніки[4]. У наступних своїх роботах автор детально розглядає метод, за допомогою якого злочинець здійснює цілеспрямований вплив на засоби комп'ютерної техніки та інформацію[5]. Дослідник наводить шість груп способів у комплексі з відповідними слідами їх застосування: 1) безпосередній доступ; 2) дистанційний доступ; 3) фальсифікація вхідних (вихідних) даних і керівних команд; 4) несанкціоноване внесення змін до наявних програм для ЕОМ і створення шкідливих програмних засобів; 5) незаконне розповсюдження машинних носіїв, що містять комп'ютерну інформацію; 6) комплексні способи. Як на нас, кінцева мета таких дій залишилася поза межами уваги автора, що дає нам можливість вважати їх лише однією зі складових злочинної діяльності у обстановці кіберпростору.

---

[1] Бутузов В. М., Гавловський В. Д., Тітуні К. В., Шеломенцев В. П. Правові та організаційні засади протидії злочинам у сфері використання платіжних карток : наук.-практ. посіб. / за ред. І. В. Бондаренко. Київ, 2009. С. 60–102; Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. С. 193–213.

[2] Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.

[3] Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків : ХНУВС, 2010. 112 с.; Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / за ред. Я. Ю. Кондратьєва. Київ : Паливода А. В., 2004. 144 с.

[4] Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. Изд. 2-е, доп. и испр. М. : ЛексЭст, 2004. 160 с.

[5] Там само.

Під час вивчення злочинної діяльності, процесів вчинення злочинів науковці вважають за найдоцільніше звертатися до технологічного підходу[1]. А, отже, способи, за допомогою яких злочинець здійснює незаконний вплив на засоби комп'ютерної техніки та інформацію, як такі, що представлені лише в одній з кваліфікаційних підгруп злочинів досліджуваної категорії (є пов'язаними з анархістськими діями в кіберпросторі (розд. XVI КК України)), заслуговують на увагу в перебігу дослідження технологій вчинення злочину. До того ж, сам В. Б. Вехов наголошує, що більшої поширеності набули комплексні способи впливу на інформацію, засновані на використанні злочинцем двох і більше способів різних груп. Під час анкетування практичних працівників правоохоронних органів майже 90 % респондентів зауважили, що для вчинення злочинів у обстановці кіберпростору застосовується комплекс прийомів та методів дії в кіберпросторі, водночас не всі з них спрямовані на отримання доступу до засобів комп'ютерної техніки.

С. В. Кригін, розглядаючи модель вчинення злочину в сфері комп'ютерної інформації в контексті способів вчинення злочину, пропонує наводити типову систему ознак стосовно кожного способу, зокрема описувати: принцип дії (суб'єктний, що застосовується за постійної участі особи; програмний, що виконується через програмні засоби комп'ютерної техніки; апаратний); наслідки способу (знищення, блокування, модифікація, копіювання інформації); інтелектуальність (висока, середня, низька); предмет злочину (відомості, програма, апаратура, канали зв'язку)[2]. Загалом досить ускладнюючи опис способів вчинення такого злочину, автор справедливо акцентує на тому, що суб'єкт виявлення та розслідування злочину повинен мати знання про технології обробки інформації, які використовує злочинець. Саме в цьому є сенс з позицій вчинення злочинів в обстановці кіберпростору.

[1] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. С. 38.; Когутич І. І. Про перспективи «комп'ютерізації» та сутність технології в криміналістиці. Часопис Київського університет права. 2015. № 4. С. 255-259.

[2] Крыгин С. В. Расследование преступлений, совершаемых в сфере компьютерной информации : дис. … канд. юрид. наук : 12.00.09. Н. Новгород, 2002. С. 96.

Вважаємо, що в класифікації способів досліджуваного виду злочинів необхідно враховувати не лише фактичний спосіб дії злочинця, а й інформаційно-комунікаційні технології (кібертехнології), що були покладені в основу досягнення кінцевої злочинної мети. На нашу думку, вони виконують функцію елемента, що забезпечує інтерактивну взаємодію способів підготовки, вчинення та приховування злочину.

Д. М. Цехан зазначає, що якісне вдосконалення способів вчинення традиційних злочинів мало наслідком появу своєрідних технологій злочинної діяльності, що дає підстави висновувати про існування кореляційних зв'язків між високими інформаційними технологіями та інноваційними формами злочинної діяльності[1]. Аналіз судово-слідчої практики дозволяє стверджувати, що в описовій частині постанов, ухвал та вироків у справах досліджуваної категорії (в частині опису фабули події злочину) завжди міститься вказівка на кібертехнології, які дозволили досягти злочинного результату.

Про інформаційно-комунікаційні технології (information communication technologies – ICT) ми вже зазначали як про методи й способи накопичення, обробки, зберігання, відображення, пошуку та забезпечення цілісності інформації [2]. У ст. 1 Закону України «Про Національну програму інформатизації» інформаційну технологію визначено як цілеспрямовану організовану сукупність інформаційних процесів з використанням засобів обчислювальної техніки, що забезпечують високу швидкість обробки даних, швидкий пошук інформації, розосередження даних, доступ до джерел інформації незалежно від місця їх розташування[3]. Оскільки всі ці процеси нині відбуваються за допомогою засобів комп'ютерної техніки, доречним видається застосування й інших термінів – «комп'ютерно-інформаційні технології» або «кібертехнології». Комп'ютерні інформаційні технології класифікують за різними критеріями.

[1] Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / за ред. О. О. Подобного. Одеса : Юрид. літ., 2011. С. 43.

[2] Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. С. 32.

[3] Про Національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: http://zakon5.rada.gov.ua/laws/show/74/98-%D0%B2%D1%80.

Традиційною є класифікація за «видом дій з використанням технологій», зокрема, на: 1) технології зберігання і обробки інформації – на якому машинному носії та де зберігати, як зберігати (один або декілька файлів, архівом чи потрібна резервна копія тощо), як обробляти – які дії слід виконати з інформацією в процесі її обробки); 2) телекомунікаційні технології – як передавати дані комп'ютерними мережами; 3) технології мультимедіа та віртуальна реальність – як обробляти звукові й відеодані, як організувати віртуальну реальність для дистанційних ігор, аукціонів тощо; 4) технології програмування – як створювати програми для розв'язання реальних задач; 5) технології обробки зображень – як обробляти різні графічні дані; 6) технології розпізнавання (наприклад мови, відбитка пальця руки); 7) технології криптографії – як кодувати інформацію за допомогою шифрування[1].

Особливу наукову цінність для дослідження способів та технологій вчинення злочинів у кіберпросторі має розподіл комп'ютерно-інформаційних технологій залежно від сфер застосування технологій на дві великі групи[2]: а) базові (універсальні) технології – їх використовують практично у всіх сферах діяльності; б) технології предметних галузей (спеціальні) – їх застосовують у певних сферах діяльності суб'єкта.

У свою чергу, фахівці з інформатики розподіляють базові технології на групи за видами оброблюваної інформації: 1) для обробки різних даних – система управління базами даних і табличні процесори; 2) для обробки тексту – текстові процесори, технології гіпертекстового зв'язку документів; 3) для обробки графіки – графічні процесори; 4) для обробки об'єктів реального світу – засоби мультимедіа. Фірми-виробники програмного забезпечення часто об'єднують потрібні користувачу програми в пакети прикладних програм. Ці технології є широкодоступними.

Назва «технології предметних галузей», або «спеціальні технології» свідчить сама за себе. Такі технології поділяють на

[1] Слепухина А. С. Компьютерные информационные технологии : курс лекций. Витебск : МИТСО, 2009. 201 с. URL: http://life-prog.ru/1_21247_kurs-lektsiy.html.

[2] Слепухина А. С. Компьютерные информационные технологии : курс лекций. Витебск : МИТСО, 2009. 201 с. URL: http://life-prog.ru/1_21247_kurs-lektsiy.html.

підгрупи залежно від сфер їх застосування, наприклад, існують технології електронної комерції, технології електронного документообігу, банківські технології, експертні системи, шкідливе програмне забезпечення, блокчейн-технологія (з англ. «blockchain», для обігу криптовалюти Bitcoin), технології робототехніки, технології розумного дому тощо. Злочинець-упевнений користувач, злочинець-досвідчений користувач та злочинець-користувач професіонал досить легко поєднують такі технології в комплекс для злочинної діяльності – наприклад, декілька злочинів, об'єднаних єдиним злочинним замислом, або однотипні злочинні дії (про зв'язок останніх «за розвитком» зазначено в попередніх підрозділах роботи).

Вважаємо, що обрання зловмисником певної з комп'ютерних технологій за основу своєї злочинної діяльності може послугувати підставою для класифікації способів злочинних дій у кіберпросторі.

Унаслідок аналізу матеріалів слідчо-судової практики ***типові на цей час в Україні способи вчинення злочинів у кіберпросторі*** можна класифікувати наступним чином.

1. Способи злочинних дій, пов'язані з функціонуванням соціально-орієнтованих мереж (від англ. social networks), діяльність яких заснована на так званій вікі(viki)-технології. Остання є технологією побудови Web-системи, призначеної для колективної розробки, зберігання, структурування тексту, гіпертексту, файлів, мультимедіа. Користувач отримує можливість зареєструватися й розміщувати на своїй інтернет-сторінці (аккаунті) будь-яку інформацію про себе, свої інтереси, події з особистого та суспільного життя, обговорювати (в онлайн або офлайн режимах) з іншими користувачами мережі будь-які теми[1]. Інформація, яку публікує користувач, є структурованою в часі, може піддаватися редагуванню й зберігатися (або не зберігатися) в соціальній мережі залежно від його бажання без використання спеціальних програмних засобів. Доступ до матеріалів веб-сторінки може бути наданий будь-кому з користувачів мережі або певній категорії осіб, окремим особам – таким чином між суб'єктами кіберпростору виникають багаторівневі соціальні зв'язки.

Зазвичай злочинець початкового рівня та рівня користувача з метою доведення до відома необмеженої кількості користувачів

[1] Информатика для гуманитариев : учебник / [Г. Е. Кедрова и др.]. М. : Юрайт, 2018. С. 159–162.

соціальної мережі, а також сповіщення всіх користувачів мережі, яких додано до розділу «Друзі» цього аккаунту, розміщує (з власного комп'ютера або здійснює так званий «репост» – поширення з іншого електронного джерела) на сторінці фото-, відеофайли, інші форми публікації протизаконного характеру, що містять:

– порнографію (часто дитячу);

– заклики до насильницької зміни конституційного ладу, захоплення державної влади, змінення меж території та державного кордону України, до вчинення терористичного акту;

– пропаганду культу насильства та жорстокості, расової, національної та релігійної нетерпимості, війни, комуністичного й націонал-соціалістичного (нацистського) тоталітарних режимів;

– інформацію спрямовуючого (мотивуючого) характеру на вчинення терористичних актів (тим самим здійснюється вербування людей), на працевлаштування молодих жінок за кордон (вербування особи з метою її сексуальної експлуатації, експлуатації її праці), самогубства (з метою доведення до самогубства);

– розпусні дії інтелектуального характеру щодо малолітньої або неповнолітньої особи.

Способи підготовки, пов'язані з завантаженням, пошуком, створенням, зберіганням, редагуванням відповідних текстових, фото-, відеофайлів або інших форм публікації. Способи приховування найчастіше не застосовують. В окремих випадках для забезпечення анонімності злочинець може використовувати віртуальні приватні мережі (VPN-технології). Наведена група способів вчинення злочину може набувати реалізації у формі одиничного злочину або містити багато епізодів злочинної діяльності. Розглянемо приклад. Влітку 2014 року мешканець Полтави гр. К., діючи за попередньою змовою в складі групи з іншими невстановленими слідством особами, з метою виготовлення, зберігання, розповсюдження відеопродукції, що пропагує культ насильства та жорстокості, а також примушування інших осіб до участі у створенні такої продукції, в соціальній мережі «ВКонтакте» створив сторінку (групу) за назвою «Модный Приговор Полтава» та іншу сторінку за назвою «ХХХ», під час користування якими здійснював адміністративні права. Після того на початку вересня 2014 року на території залізничного вокзалу станції Полтава-Південна за попередньою змовою з групою невстановлених слідством осіб за допомогою невстановленого слідством мобільного телефону

зняли відеозапис із застосуванням фізичного насильства щодо гр. О., примушуючи його таким чином до участі у створенні відеозапису, який за висновком мистецтвознавчої експертизи від 25 червня 2015 року за № 160 є таким, що пропагує культ насильства та жорстокості. Надалі К. виготовив та зберігав цей відеозапис за місцем свого проживання й за допомогою власного ноутбука опублікував його на вищезгаданих сторінках сайту «ВКонтакте»[1].

Багатоепізодна злочинна діяльність може мати довготривалий характер, що сьогодні доволі характерно. Так, з 2012 до 2016 року мешканець Кіровограда гр. П. розміщував у створеному ним акаунті заклики не вважати Донбас частиною України, що було кваліфіковано як посягання на її територіальну цілісність[2].

Трапляються окремі випадки використання наведених вище способів особами, що мають психічні розлади. Так, у квітні 2013 року гр. М. у вечірній час за місцем свого проживання зайшов у соціальну мережу «ВКонтакті» та відправив іншій (малолітній) особі заявку щодо віднесення його до категорії «Друзі». Після підтвердження останньою заявки у М. виник умисел на вчинення розпусних дій щодо неї. Реалізуючи свій злочинний намір, він почав їй неодноразово писати повідомлення з сексуальним змістом, у яких пропонував малолітній вступити з ним у статевий зв'язок. Згідно з актом амбулаторної комісійної судово-психіатричної експертизи, М. страждає на раннє органічне ураження головного мозку з помірною інтелектуально-амнестичною недостатністю та змінами особистості, що не дозволяє йому повною мірою усвідомлювати свої дії та керувати ними, але не позбавляє його здатності діяти повністю. До М. було примусово застосовано заходи медичного характеру[3].

Найчастіше розглянутим вище чином у обстановці кіберпростору вчиняють злочини таких класифікаційних підгруп: а) злочини, пов'язані з насильницько-егоїстичними діями; б) злочини,

[1] Вирок Ленінського районного суду м. Полтави від 30 серп. 2016 р. Справа № 553/2825/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/60132327.

[2] Вирок Кіровського районного суду м. Кіровограда від 15 лип. 2016 р. Справа № 404/3962/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/59029350.

[3] Вирок Переяслав-Хмельницького міськрайонного суду Київської області від 30 серп. 2013 р. Справа № 373/2151/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/33209010.

пов'язані з антидержавницькими діями; в) злочини політико-ідеологічного спрямування; г) злочини, пов'язані з насильницько-дискримінаційними діями. Варто додати, що в окремих випадках для вчинення такого роду злочинів використовують технології відеохостінгу (веб-сервіс, що дозволяє завантажувати й переглядати відео в браузері за принципом «користувач генерує контент» (англ. *user-generated content*). Найбільшого поширення в Україні набув сервіс відеохостінгової компанії «Youtube». Однак через якісний контроль представниками компанії (модераторами) змісту викладеної інформації з метою недопущення вчинення злочинів через відповідний сервіс практику його застосування зі злочинною метою не можна назвати поширеною.

2. Способи злочинних дій, пов'язані з функціонуванням технології BitTorrent, створеної для передавання великих за обсягом файлів одним користувачем іншому або громадськості. Це працює таким чином: 1) після ініціалізації запуску додатку (торрент-клієнт) на власному комп'ютері додаток формує опис для файлу, в якому зазначено найменування, розмір, розподіл на фрагменти й інформацію щодо розподілу даних, які зберігаються з новим розширенням «*.torrent*»; 2) здійснюється завантаження файлів на окремий виділений сервер (торрент-треккер), який не бере самостійної участі в закачуванні, а лише керує ним; клієнт зберігає координати сервера і вкладає адресу для завантаження файлу; 3) кожний користувач, що бажає його завантажити, повинен також завантажити торрент-клієнт, який обробляє всі файли з відповідним розширенням, у результаті пошуку з виділеного сервера надходить інформація про місце розташування інформації; 4) кожний користувач має власну частину завантажених фрагментів файлів, а додаток налагоджує з'єднання з користувачами і надає запит на окремі фрагменти інформації для скачування. Більша кількість задіяних у мережі користувачів забезпечує швидкість завантаження файлу. Сервер може надавати привілеї для скачування за певних умов (залежно від кількості завантажених та виданих файлів)[1]. Злочинці-користувачі вдало застосовують цю технологію для розповсюдження через Інтернет комп'ютерних програм, аудіовізуальних творів, баз даних (компіляції даних), фонограм та організації мовлення з порушенням авторського

[1] Как работает технология Torrent? URL: https://itproger.com/news/63.

або суміжних прав шляхом їх розміщення для копіювання в мережі, а також творів, що мають порнографічний характер, шляхом надання доступу до них користувачам. Так, мешканець міста Запоріжжя в період з 30 серпня до 21 вересня 2012 року, маючи намір щодо поширення відеофайлів порнографічного змісту, з використанням Інтернет-ресурсу «tracker.zp.ua» поширював відеофайли порнографічного змісту, внаслідок чого інші особи отримували ці файли в користування[1].

3. Способи злочинних дій, пов'язані з функціонуванням сервісів електронної дошки оголошень (від англ. абревіатури *«BBC»*). З розвитком Інтернету започаткувала свою роботу на платних чи безоплатних засадах безліч сайтів з оголошеннями комерційного та/або некомерційного характеру. Ефективність таких сайтів є набагато вищою за звичайну паперову рекламну продукцію (газети, каталоги, буклети тощо). Окремі суб'єкти ведення бізнесу створюють власні електронні дошки в межах технологій електронної торгівлі, про що буде зазначено далі. Найбільш поширеними дошками оголошень є сервіси, що діють у режимі онлайн зв'язку, – наразі українці часто використовують «olx.ua», «bigl.ua» (раніше «aykro»), «ria.com», а також відповідні закордонні сервіси.

Нині шахрайські дії масово вчиняються шляхом розміщення оголошення щодо продажу користувачам інтернет-сайту будь-якого матеріального предмета, причому злочинець не має наміру поставляти його покупцеві. Зловмисник запевняє потерпілого, що відправить замовлений товар кур'єрською/поштовою службою після отримання ним як передоплати грошових коштів, для чого використовуються можливості різноманітних платіжних систем та сервісів Інтернет-банкінгу. Так, мешканець м. Нікополь, користуючись сайтом «olx.ua», багаторазово вчиняв аналогічні шахрайські дії, пропонуючи потерпілим придбати двоколісний скутер. Жертви шахрая з використанням Інтернет-банкінгу «Приват24» здійснювали

[1] Вирок Шевченківського районного суду м. Запоріжжя від 26 лют. 2013 р. Справа № 1-кп/336/67/2013. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/29608881.

передплату товару різного грошового розміру на розрахунковий рахунок, відкритий на ім'я підставних осіб в ПАТ КБ «Приватбанк»[1].

Також злочинець, розмістивши оголошення, сам може бути продавцем зброї, бойових припасів або вибухових речовин, наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів, спеціальних технічних засобів отримання інформації. Так, у першій декаді листопада 2016 року мешканець м. Рівне за допомогою сайту електронної торгівлі «AliExpress» придбав з Китайської народної республіки спеціальні технічні засоби негласного отримання інформації (а саме GSM- мікрофони марки «Mini A8»). Пересвідчившись, що вони в робочому стані й придатні для використання за призначенням, зловмисник незаконно збув їх різним громадянам з використанням мережі Інтернет за допомогою сайтів «Olx», «Ukgro», «Evende» та «Weebly» через відділення «Нової пошти» за умови «післяплати»[2].

Розглянуті способи є характерними для вчинення шахрайства з використанням комп'ютерної техніки (ст. 190 ч. 3 КК України) та злочинів, що порушують встановлений порядок обігу певних речей, як самостійної класифікаційної підгрупи злочинів.

4. Способи злочинних дій, пов'язані з функціонуванням технологій електронної комерції, створені для здійснення торгівлі через Інтернет. Терміном «технології електронної комерції» позначають різноманітні принципи, яким має відповідати програмне забезпечення та сервіси для електронної комерції. Саме для них підтримуються так звані відкриті інтернет-стандарти. Власне, здійснюється стандартизація всіх форм взаємодії між організаціями, залученими в повний цикл «постачання – продаж – купівля (англ. Supply – Selling – Buying)». Сюди відносять технології електронного обміну інформацією (англ. Electronic Data Interchange, EDI), електронного руху капіталу (англ. Electronic Funds Transfer, EDF), електронної торгівлі (англ. E-trade), обігу електронних грошей (англ. E-cash), електронний маркетинг (англ. E-marketing), електронний

[1] Вирок Нікопольського міськрайонного суду Дніпропетровської області від 2 груд. 2015 р. Справа № 182/3014/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/54012641.

[2] Вирок Рівненського міського суду Рівненської області від 27 лип. 2017 р. Справа № 569/10782/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/67942562.

банкінг (англ. E-banking), електронні страхові послуги (англ. E-Insurance) тощо[1].

На підставі аналізу матеріалів кримінальних проваджень можна назвати такі поширені групи способів злочинних дій з використанням технологій електронної комерції.

4.1. Замовлення на сайті, що здійснює електронну торгівлю (діє аналогічно до електронної дошки оголошень), товарів, що мають особливий порядок обігу, та їх отримання у формі внутрішнього або міжнародного поштового відправлення.

Варто відзначити, що в разі замовлення такого товару за кордоном з паралельним вчиненням дій, що унеможливлюють ідентифікацію замовленого товару митним органом України, зокрема надавання як підстави для переміщення товарів через митний кордон України документів, що містять неправдиві дані стосовно найменування та характеристик товару, діяльність злочинця утворюватиме комплекс дій, що кваліфікуються за ст. 201 (контрабанда) та статтею КК України, яка передбачає відповідальність за незаконне придбання певних предметів (зброї, бойових припасів або вибухових речовин, наркотичних засобів, психотропних речовин або їх аналогів та прекурсорів, спеціальних технічних засобів отримання інформації). Як приклад можна навести вже описану злочинну діяльність мешканця м. Рівне, який для придбання за допомогою сайту електронної торгівлі «AliExpress» з Китайської народної республіки спеціальних технічних засобів негласного отримання інформації вдавався до зазначення в митних документах неправдивих даних стосовно характеристик товару[2]. Однак таку сукупність дій не можна вважати типовою технологією, адже закордонний відправник, маючи зацікавленість у подальшій співпраці із замовником, сам намагається приховати відомості про справжнє призначення товару.

[1] Шалева О. І. Електронна комерція : навч. посіб. Київ : Центр учб. літ., 2011. С. 10.

[2] Вирок Рівненського міського суду Рівненської області від 27 лип. 2017 р. Справа № 569/10782/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/67942562.

Звернемося до показового прикладу[1]. На початку січня 2015 року в м. Бердянську гр. М. з метою незаконного виготовлення для подальшого збуту особливо небезпечної психотропної речовини через сайт «Legal skupe smoke.brd» у мережі Інтернет вступив у злочинну змову з невстановленою особою, за якою через термінал «ПриватБанк» перерахував цій особі гроші, після чого, одержавши від неї відомості про номер посилки з реагентами для виготовлення психотропної речовини, отримав цю посилку у відділенні «Нової пошти». Опанувавши технологію виготовлення особливо небезпечної психотропної речовини, за попередньою змовою з групою осіб за допомогою реагенту масою 10 г виготовив особливо небезпечну психотропну речовину AB-PINACA та 4-метил-а-пірролідиногексанофенон (MPHP), обіг якої заборонений. 12 січня 2015 року М., продовжуючи свою злочинну діяльність, переніс у пакеті цю речовину в громадське місце, де сховав під підвіконня, повідомивши через сайт «Legal skupe smoke.brd» невстановлену особу про місцеперебування пакунка. У цей час інші дві особи через сайт «Legal skupe smoke.brd» вступили в злочинну змову з невстановленою особою, яка, отримавши оплату через термінал «ПриватБанк», повідомила їх про місце схову наркотичного засобу. Останні також розфасували по пакунках цю речовину та продовжили свою злочинну діяльність з її збуту. Така злочинна діяльність мала багатоепізодний характер. Організатор поставок наркотичного засобу залишився невстановленим.

4.2. Розповсюдження через сайти, які спеціалізуються на трансляції відеозображень еротичного та порнографічного характеру відеопродукції, зображень порнографічного характеру, створення та організація функціонування «студій» з виготовлення та розповсюдження такої відеопродукції, забезпечення її трансляції та зображень у режимі онлайн (з використанням режиму «Privat chat»), а також можливе одночасне створення та адміністрування відповідних сайтів.

Так, упродовж чотирьох років (з 2009 до 2013 р.) на території Одеської області діяла організована група у складі семи осіб із внутрішньо та зовнішньо стійкими ієрархічними зв'язками, що з

[1] Вирок Бердянського міськрайонного суду Запорізької області від 5 квіт. 2016 р. Справа № 310/7032/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56953260.

корисливих мотивів, маючи на меті безпосереднє скоєння тяжких злочинів, займалася виготовленням з метою збуту та розповсюдженням через Інтернет за допомогою комп'ютерних програм відеопродукції, зображень порнографічного характеру[1]. Визначивши спрямованість своєї злочинної діяльності, дві особи, діючи як лідери злочинної групи, за допомогою глобальної мережі Інтернет познайомилися з невстановленими в ході слідства власниками таких сайтів компютерної мережі «Інтернет», як «777LiveCams», «CamContacts», «ImLive», «LiveJasmin», «Streamate», що спеціалізуються на трансляції відеозображень еротичного та порнографічного характеру, досягли з ними домовленості про збут на цих «сайтах» відеопродукції та зображень порнографічного характеру, таким чином вступивши з ними в попередню змову. За досягнутою з невстановленими досудовим слідством власниками «сайтів» домовленістю для рекламних цілей та залучення якомога більшої кількості дівчат-моделей було створено та зареєстровано студію «Debirs», отримано доступ до зазначених «сайтів», у режимі on line – тобто реального часу, розпочалася пряма трансляція відеопродукції та зображень порнографічного характеру. Особи (клієнти), зацікавлені в перегляді відеозображень дівчат-моделей, «увійшовши» на вказані сайти, за допомогою своїх електронних платіжних карток повинні були оплачувати час спілкування в приват-чатах з моделями з розрахунку від 0,50 ЄВРО до 1,99 долара США за хвилину залежно від категорії сайту.

4.3. Надання можливості відвідувачам створеного веб-сайту переглядати або копіювати аудіовізуальні твори, комп'ютерні програми, фонограми, права на які належать іншій особі.

Так, мешканець м. Вижниця Чернівецької області у вересні 2012 року створив веб-сайт «ost.cv.ua», здійснюючи його адміністрування з використанням власного персонального комп'ютера з метою ведення електронної комерції[2]. Надалі з використанням створеного веб-сайту «ost.cv.ua» злочинець умисно, протиправно, без

[1] Вирок Колегії суддів Приморського районного суду м. Одеси від 6 черв. 2016 р. Справа № 522/6835/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/58207973.

[2] Вирок Вижницького районного суду Чернівецької області від 12 груд. 2013 р. Справа № 713/2307/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/36016798.

відповідного дозволу правовласників, з порушенням вимог Закону України «Про авторське право і суміжні права» з вересня 2012 року до 13 липня 2013 року надав доступ користувачам Інтернету для перегляду та копіювання у значній кількості аудіовізуальних творів, права на які належать компаніям «Twentieth Century Fox Film Corporation», «Universal City Studios LLLP», «Columbia Pictures Industries, Inc. (Sony Pictures)», «Disney Enterprises Inc.» та «Warner Bros. Entertainment Inc.». Тим самим зловмисник завдав цим компаніям матеріальної шкоди на загальну суму 180 254 1,35 грн.

4.4. Створення умов для азартних ігор у формі інтерактивного електронного (віртуального) казино. Так, у 2013 році в м. Ніжин Чернігівської області гр. Н. як суб'єкт господарської діяльності орендував приміщення, в якому встановив дев'ять ігрових автоматів і п'ять комп'ютерів з програмним забезпеченням ігрових систем «Win&Win Casino» та «Champion», призначених для віртуальних азартних ігор у мережі Інтернет, об'єднав їх у локальну мережу з постійним доступом до Інтернету й таким чином обладнав електронне (віртуальне) казино. З метою отримання прибутку зазначений громадянин організував діяльність, пов'язану з наданням фізичним особам можливості доступу до азартних ігор через мережу Інтернет в електронному (віртуальному) казино, віддаленому від місця розташування сервера, обов'язковою умовою участі в яких є сплата гравцем грошей, зокрема через систему електронних платежів, що дає змогу учаснику отримати чи не отримати виграш залежно від випадку[1].

На цей час триває слідство у справі стосовно 12 колишніх громадян РФ, які найняли близько 80 працівників для організації та проведення азартних ігор у мережі. За офіційним повідомленням Департаменту кіберполіції, його працівники під процесуальним керівництвом Київської місцевої прокуратури № 2 задокументували діяльність зазначеної групи осіб, які організували в Україні проведення азартних ігор у віртуальному (електронному) казино на восьми Інтернет-майданчиках, зокрема: «eldoradoclub[.]com», «vulkanclub[.]com», «24vulkan[.]com», «slotvulkanclub[.]com», «estcasino[.]com», «greencasino[.]com», «anonymcasino[.]com»,

[1] Вирок Ніжинського міськрайонного суду Чернігівської області від 6 трав. 2016 р. Справа № 740/432/15. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/57559283.

«pharaonclub[.]com». Характерною ознакою веб-ресурсів зловмисників було те, що вони були орієнтовані на споживачів з країн СНД. У разі спроби зайти на веб-ресурс з IP, розташованого в Україні, користувачеві пропонували звернутися до служби підтримки сайту. Своєю чергою, служба підтримки пропонувала використати спеціальні програми із замінення IP-адреси, щоб забезпечити анонімний вхід та вільне відвідування своїх ресурсів. Водночас схему введення-виведення грошей під час гри було побудовано з використанням лише російських банківських установ та платіжних систем[1].

5. Способи злочинних дій, пов'язані з функціонуванням технології електронної розсилки **(***e-mail, від англ. electronic mail); IP-телефонії (найчастіше через комп'ютерну програму Viber;* програмне забезпечення із закритим кодом *Skype*), призначені для відправлення/отримання електронних повідомлень між користувачами комп'ютерної/телекомунікаційної мережі.

Наразі ці масові за характером способи використання технології дозволяють як розпочинати, так і доводити до завершення злочини різної кваліфікації та ступеня тяжкості: від завідомо неправдивого повідомлення про підготовку вибуху (ст. 259 КК України) до державної зради (ст. 111 КК України). Проте їх зазвичай використовують злочинці типу «користувач низького рівня» або «злочинець-звичайний користувач». Безпосередній спосіб дій злочинця полягає у відправленні/отриманні електронних повідомлень. Дії злочинця часто є такими:

5.1. Злочинець надсилає державним та комерційним установам неправдиву інформацію про замінування будівель (безпосередній спосіб вчинення злочину). Наприклад, 8 червня 2016 року гр. М. за місцем свого мешкання, скориставшись власним ноутбуком, за допомогою мережі Інтернет створив повідомлення з погрозою скоєння вибухів у супермаркетах торговельної мережі «Варус» міст Кам'янського та Дніпра. За допомогою комп'ютерної програми «Говорилка», призначеної для замінення набраного тексту на аудіо-файл з людським голосом, виготовив аудіо-файл, який містив інструкцію про оплату йому винагороди за відміну підриву будівель.

[1] Поліція оголосила підозру організаторам кількох онлайн-казино. URL: https://cyberpolice.gov.ua/news/policziya-ogolosyla-pidozru-organizatoram-kilkox-onlajn-kazyno-5427.

З використанням електронної поштової скриньки іншої особи, пароль до якої він отримав випадково, зазначені письмові повідомлення та аудіо-файл було відправлено на електронну поштову скриньку CALL-центру Служби Безпеки України[1].

5.2. Злочинець надсилає представникам іноземних розвідок відомості військового характеру або конфіденційну інформацію, що має різні ступені таємності (безпосередній спосіб вчинення злочину), чим завдає шкоди національній безпеці та інтересам України у сфері забезпечення порядку, знижує обороноздатність, створює умови для підривної діяльності.

5.3. Злочинець надсилає потерпілому неправдиву інформацію у формі масової розсилки для введення останнього в оману з метою отримання від нього інформації, потрібної для подальшого здійснення ним трансакції (спосіб підготовки шахрайства). Показовим є приклад щодо шахраїв, яких було викрито влітку 2017 року поліцейськими Департаменту кіберполіції. Злочинці за допомогою смс-розсилки на території Київської області завдали громадянам збитків близько 150 000 грн. Зловмисники розсилали смс-повідомлення через організовану злочинною групою мережу «фішингових сайтів», посилання на які надходили громадянам. Злочинці використовували у своїй «діяльності» дві схеми незаконного збагачення: 1) повідомляли громадян про виграш автомобіля та шахрайським шляхом виманювали у них гроші; 2) рекомендувалися працівниками банку та повідомляли про несанкціоновані дії з картою, для припинення яких пропонували повідомити *cvv*-код картки, після отримання якого знімали з банківського рахунку всі кошти[2].

5.4. Злочинець обманним шляхом отримує від жертви подальшого вимагання відомості (серед іншого фото- та відеофайли), що ганьблять гідність, честь чи ділову репутацію фізичної особи (спосіб підготовки вимагання). Так, 8 вересня 2013 року Х., використовуючи обліковий запис мережі «Skype», за допомогою

[1] Вирок Дніпровського районного суду м. Дніпродзержинська Дніпропетровської області від 4 жовт. 2017 р. Справа № 209/3720/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/69294676.

[2] Кіберполіція викрила шахраїв, що за допомогою СМС-розсилки ошукували громадян. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-shaxrayiv-shho-za-dopomogoyu-sms-rozsylky-oshukuvaly-gromadyan-foto-2963.

відеоконференції зв'язався з обліковим записом потерпілої особи і, маючи на меті подальше вимагання від неї грошових коштів, запропонував останній для оцінки параметрів тіла зняти з себе одяг з метою можливої пропозиції щодо її участі в телевізійному кліпі. Погодившись на пропозицію, та повністю зняла з себе одяг і стала позувати перед веб-камерою[1]. За нерозголошення зробленого ним таким чином відеозапису в оголеному вигляді потерпілої Х. став вимагати від неї 1000 доларів США.

5.5. Злочинець незаконно здійснює ознайомлення з чужою електронною кореспонденцією або змістом телефонних розмов, іншою кореспонденцією. Так, у червні 2011 року мешканець м. Києва, маючи умисел на порушення таємниці кореспонденції, що передається через комп'ютер, додав до налаштувань електронної пошти потерпілої особи спеціально створену ним невстановлену електронну скриньку, на яку здійснювалося пересилення всієї вхідної кореспонденції, що надходила на електронні скриньки потерпілої особи, таким чином зловмисник отримав можливість ознайомлюватися з її вхідною кореспонденцією[2]. У цьому разі йдеться про злочин, передбачений ст. 163 КК України.

6. Способи злочинних дій, пов'язані з функціонуванням технологій електронних платіжних систем (англ. *electronic payment systems*), призначені для здійснення платіжних операцій через мережу Інтернет. За допомогою платіжної системи здійснюються оплати різного призначення, тому досить часто цю технологію використовують одночасно з технологією електронної комерції. Типовий спосіб дій злочинця полягає у створенні фіктивних сайтів, через які від потерпілих за різні послуги або товари приймаються електронні платежі. Так, працівники Причорноморського управління Департаменту кіберполіції спільно зі слідчими поліції Одещини викрили двох місцевих мешканців, які, створивши фіктивний Інтернет-ресурс «kadastor.in.ua», приймали оплату послуг кадастрового бюро за оформлення та отримання безоплатної

[1] Вирок Солом'янського районного суду м. Києва від 28 листоп. 2014 р. Справа № 1-кп/760/715/14. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/41620960.

[2] Ухвала Шевченківського районного суду м. Києва від 7 квіт. 2014 р. Справа № 761/10495/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/38305124.

земельної ділянки на території Одеської області. Для реалізації своїх злочинних намірів шахраї власноруч виготовляли фіктивні договори з використанням реквізитів підприємства «Земельне кадастрове бюро» та скріплювали їх підробленою мокрою печаткою. Сайт відрізнявся від реального оформленням та доменним ім'ям[1].

Усе частіше в Україні трапляються випадки використання електронних платіжних систем для фінансування тероризму. Зокрема, в перебігу тривалої злочинної діяльності група осіб створила злочинну схему з видачі готівки клієнтам так званого «Першого фінансового центру», створеного як банківська установа на території непідконтрольного державній владі м. Луганська. Звертаючись у центр, клієнти отримували готівку, а кошти з їх рахунків перераховувалися на рахунки працівників центру. Наприкінці кожного робочого дня ці кошти концентрувалися на банківських рахунках члена злочинного угруповання, звідки спрямовувалися співучасникам злочинної діяльності за межі території проведення антитерористичної операції та мешканцю міста Києва Х. У наведеному механізмі вчинено дії щодо переказів грошових коштів з використанням платіжних систем Ipay, EasyPay, Portmone, LiqPay[2].

7. Способи злочинних дій, пов'язані з функціонуванням технології зберігання та обробки інформації. Це система запису інформації на електронний пристрій, де фігурують два знаки (0; 1). На магнітному носії уздовж доріжок розташовуються ділянки з записаним магнітним полем двох напрямків, одне з яких відповідає цифрі « 0», а інше – «1». У байті налічується 256 різних комбінацій нулів та одиниць. Власне, ця технологія й стала першоосновою існування кіберпростору, тому її покладено в основу будь-якої дії з його використанням. Утім, якщо розглядати використання для злочинної дії лише цієї технології, варто враховувати особу, яка має право доступу до комп'ютерної інформації та вчиняє злочин, передбачений ст. 362 КК України, у формі активних дій з несанкціонованого змінення, знищення, блокування, перехоплення

[1] На Одещині кіберполіція виявила фіктивний сайт земельного кадастрового бюро. URL: https://cyberpolice.gov.ua/news/na-odeshhyni-kiberpolicziya-vyyavyla-fiktyvnyj-sajt-zemelnogo-kadastrovogo-byuro-7030.

[2] Вирок Дарницького районного суду м. Києва від 28 груд. 2015 р. Справа № 753/23764/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/54799070.

або копіювання інформації. Так, гр. К., обіймаючи посаду начальника загону геолого-екологічного центру Львівської геологорозвідувальної експедиції дочірнього підприємства НАК «Надра України» «Західукргеологія» та маючи доступ до службової інформації означеного підприємства, що є власністю держави, одночасно був засновником, директором ПП «Ноосфера-Захід». В інтересах названого приватного підприємства в 2010–2011 роках зловмисник здійснив несанкціоновані дії з інформацією, обробка якої відбувається в електронно-обчислювальних машинах (комп'ютерах) ДП НАК «Надра України» «Західукргеологія», що призвело до її витоку[1]. Він несанкціоновано скопіював зі службового комп'ютера на власний флеш-накопичувач фрагменти електронних звітів «Геологічна будова і корисні копалини території аркуш М-35-XXV (м. Івано-Франківськ)» та «Державна геологічна карта України. Аркуш М-35-XXXII» (Чернівці) й незаконно використав її як виконавець робіт від імені ПП «Ноосфера-Захід» на замовлення інших компаній. Особа, котра не має права доступу до інформації, обирає за основу своєї злочинної діяльності інші спеціальні технології.

На цей час набув поширення злочин, передбачений ст. 330 КК України, що полягає в збиранні відомостей, що становлять конфіденційну інформацію, яка є власністю держави. Способом його вчинення є копіювання електронної інформації. Так, у період з грудня 2015 року до січня 2016 року гр. О., перебуваючи на посаді заступника начальника відділу технічного супроводження управління планування технічного забезпечення озброєння Збройних Сил України, маючи доступ до документів, що становлять службову інформацію у сфері оборони країни, на виконання завдання представника іноземної організації виготовив електронну копію документа з інформацією, котрій надано гриф «Для службового користування» та яка містить відомості відносно закупівлі безпілотних авіаційних комплексів іноземного виробництва, що можуть задовольнити потребу Збройних Сил. Зазначені дії було вчинено з метою подальшого передавання

[1] Вирок Івано-Франківського міського суду від 11 берез. 2013 р. Справа № 0907/17660/2012. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/29872888.

відомостей, що становлять службову інформацію у сфері оборони країни, представнику іноземної організації[1].

8. Способи злочинних дій, пов'язані з функціонуванням шкідливого програмного забезпечення. (з англ. «crimeware», де «*crime* – злочинність, soft*ware* – програмне забезпечення; часто як синонім застосовують «вірус»). Це програмне забезпечення злочинці (за типами «впевнений користувач», «досвідчений користувач» та «професіонал») за власною ініціативою або на замовлення трьої особи розробляють та/або поширюють для отримання несанкціонованого доступу до комп'ютера з метою несанкціонованого доступу до інформації та спричинення шкоди. Так, у наведеному вище прикладі мешканець м. Біла Церква на замовлення невстановленої особи здійснював DDoS-атаки за допомогою заздалегідь скопійованого з мережі програмного засобу за назвою «Bleck Energy», невстановлена слідством особа на ім'я «Botnetman» надала йому можливість одночасно з 1000 комп'ютерів здійснити звернення на той чи інший сервер, IP-адресу чи ресурс у мережі Інтернет, таким чином паралізувавши його роботу[2]. Такого роду злочини традиційно кваліфікують за відповідними частинами ст. 361 КК України. Однак це є типовим лише за умови невстановлення кінцевої мети дій злочинця (підготовка до вчинення злочину з корисливих мотивів).

Наведені нами групи способів не є вичерпними, але на цей час вони найоб'єктивніше відбивають інтерактивний характер злочинної діяльності у кіберпросторі. Інтерактивність – це принцип організації системи, за якого кінцевої мети вдається досягти шляхом інформаційного обміну елементів цієї системи[3]. У Тлумачному словнику української мови лексему «інтерактивний» подано в

---

[1] Вирок Шевченківського районного суду м. Києва від 24 трав. 2017 р. Справа № 761/12994/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/66711667.

[2] Вирок Білоцерківського міськрайонного суду Київської області від 5 жовт. 2010 р. Справа № 1-7/2010. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/63156830.

[3] Liu Yuping and Shrum L. J. What is Interactivity and is it Always Such a Good Thing? Implications of Definition, Person, and Situation for the Influence of Interactivity on Advertising Effectiveness. *Journal of Advertising.* 2002. No. 31 (4). P. 53–64. URL: https://www.yupingliu.com/files/papers/liu_shrum_interactivity.pdf.

контексті процесу, що переривається іншим процесом у динаміці[1]. Поєднання таких способів здійснюється в процесі реалізації злочинцем/ями конкретного виду злочинів, вчинених у кібепросторі.

Терміном «технологія» позначають типову, алгоритмічну систему методів та прийомів, що забезпечує вирішення однотипних завдань з метою підвищення ефективності відповідних процесів та рентабельності кінцевої продукції[2]. Така «однотипність завдань» під час вчинення в обстановці кіберпростору злочинів різної кримінально-правової класифікації набуває форм додаткового та основного мотивів аналізованої злочинної діяльності. Оскільки саме мотиви було покладено в основу криміналістичної класифікації злочинів досліджуваної категорії, то про характерні технології вчинення злочинів у обстановці кіберпростору можна висновувати у разі вчинення сукупності злочинів у межах однієї або декількох класифікаційних підгруп злочинів, визначених у попередньому розділі. Як свідчить аналіз матеріалів слідчо-судової практики, типовість технологій вчинення досліджуваної категорії злочинів найяскравіше виявляється стосовно злочинів, вчинених із корисливих та соціально-економічних мотивів.

Будь-яка технологія дійсно передбачає наявність відповідного алгоритму дій. Алгоритм традиційно становить собою певну послідовність дій, виконання яких дає можливість досягти запланованого (бажаного суб'єктом) результату. Тому пізнання сутності технології вчинення злочинів у кіберпросторі має відбуватися на системному рівні. На наше переконання, технологію вчинення злочину найдоцільніше досліджувати з позицій процесу досягнення кінцевого злочинного результату, коли прослідковується зв'язок між основними та підпорядкованими злочинами, що входять до злочинної сукупності. А. Ф. Волобуєв описував в цьому сенсі технологію вчинення заволодіння чужим майном чи одержання іншої незаконної вигоди[3].

---

[1] Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. С. 508.

[2] Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / за ред. О. О. Подобного. Одеса : Юрид. літ., 2011. С. 24.

[3] Волобуєв А. Ф. Технології злочинної діяльності як об'єкт криміналістичного дослідження. *Теорія та практика судової експертизи і*

На підставі аналізу матеріалів слідчо-судової практики можна визначити типові для України ***технології вчинення злочинів у обстановці кіберпростору***, розподіливши їх за такими групами:

1. Технології незаконного збагачення, засновані на попередньому заволодінні персональними даними/комерційною таємницею фізичної/юридичної особи шляхом несанкціонованого втручання в роботу комп'ютерної техніки.

Такі технології найчастіше застосовують злочинець-досвідчений користувач та/або злочинець-користувач професіонал. Останній часто діє в складі організованої групи з розподілом ролей, де є організатором. Така злочинна діяльність утворюється сукупністю злочинів з двох умовних груп: 1) злочини, передбачені ст. 189 (вимагання) та/або ст. 190 (шахрайство); 2) злочини, передбачені окремими статтями розділу XVI КК України (зокрема, ст. 361 (несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та/або ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут).

Можна визначити загальні закономірності застосування цієї групи технологій: 1) початкові дії злочинця спрямовані на отримання доступу до комп'ютера жертви шляхом здійснення незаконного впливу на засоби комп'ютерної техніки та інформацію; 2) залежно від змісту отриманих персональних даних жертви злочинець може корегувати свої подальші дії з незаконного збагачення, вчиняючи вимагання або шахрайство; 3) в основу функціонування технологій полягає застосування сукупності кібертехнологій, часто технологій функціонування соціально орієнтованих мереж, технологій електронної комерції, сервісів електронної дошки оголошень, шкідливого програмного забезпечення.

Розглянемо доволі показовий приклад вчинення вимагання[1]. Мешканець Львівської області, маючи необхідні навички у сфері

криміналістики : зб. наук.-практ. матеріалів. Харків : Право, 2003. Вип. 3. С. 148–152.

[1] Викрито хакера, який зламував облікові записи користувачів соціальних мереж. *Департамент кіберполіції :* [сайт]. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-oblikovyx-zapysiv-korystuvachiv-soczialnyx-merezh-6339.

програмування, створив Інтернет-сайт «xakercki-poslygu[.]hol.es», на якому пропонував свої послуги щодо зламу облікових записів, електронних скриньок. Листування між ним та клієнтами відбувалося за допомогою закритої спільноти, яку він адміністрував у соціальній мережі. Під час спілкування з клієнтами він також надавав їм посилання на нібито форму зворотнього зв'язку, звертаючись до якої, користувачі потрапляли на фішинговий сайт (фіктивний, спеціально створений злочинцем з метою отримання від жертви інформації, зокрема їх логінів та паролів). Отримавши таким чином доступ до облікових записів жертв, злочинець блокував доступ законних користувачів до аккаунтів шляхом змінення паролю. За повернення доступу він висував вимоги майнового характеру. Суми, які він вимагав, коливалися залежно від платоспроможності жертви. Також слідством було встановлено, що під виглядом додатку для злому соціальних мереж зловмисник розмістив для вільного завантаження шкідливе програмне забезпечення, призначене для несанкціонованого втручання в роботу мобільних телефонів з операційною системою «Android», у результаті чого хакер мав змогу переглядати телефонну книжку, фотографії та записи вхідних і вихідних викликів жертви. Цю інформацію надалі могло бути використано для вчинення вимагання або шахрайства.

2. Технології заволодіння безготівковими коштами шляхом застосування електронних платіжних систем, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки.

Застосовують такі технології зазвичай злочинець-досвідчений користувач та/або злочинець-користувач професіонал. Така злочинна 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). Характерною особливістю цієї групи технологій є їх застосування організованою злочинною групою.

Кожен учасник злочинної діяльності за відсутності транснаціонального компонента в такій групі виконує покладену на нього функцію, зокрема зі: 1) створення фіктивного підприємства для маскування злочинної діяльності; 2) здійснення несанкціонованого

втручання в роботу комп'ютерної техніки та дій, спрямованих на забезпечення незаконної трансакції; 3) реалізації механізмів легалізації отриманих безготівкових коштів та переведення їх у готівкову форму. Показовою є діяльність групи осіб у м. Луцьку[1]. Так, 29 листопада 2012 року група осіб, серед яких не встановлені слідством особи, діючи за попередньою змовою з метою заволодіння чужим майном, маючи спеціальні знання, вміючи користуватися спеціалізованим програмним забезпеченням, призначеним для проникнення в комп'ютер через 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 рахунку 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 було кваліфіковано за ч. 1 ст. 205; ч. 2 ст. 361; ч. 3 ст. 190; ч. 2 ст. 200; ч. 2 ст. 209. У перебігу досудового слідства також було встановлено вчинення цією особою іншого злочину у 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 статтей розділу XVI КК України. Наприклад, у травні 2016 року група осіб вступила у злочинну змову з метою проведення

[1] Вирок Луцького міськрайонного суду Волинської області від 21 жовт. 2013 р. Справа № 161/10410/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/34405754.

несанкціонованих платіжних операцій з рахунків українських та зарубіжних користувачів через систему миттєвих інтернет-розрахунків «WebMoney Transfer»[1]. 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» та 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 та розповсюдив у мережі Інтернет через низку власних сайтів вищезгаданий програмний засіб. Останній, за висновками комп'ютерно-технічної експертизи, є шкідливим програмним забезпеченням («троян»), що встановлюється як звичайна програма та надалі отримує права суперкористувача, працює таємно у фоновому режимі, перехоплює платіжні операції, а також збирає особисті дані користувача. Управління ним здійснюється з віддалених Інтернет-серверів, а саме розміщується на веб-сайтах вільного доступу. Останні мають ідентичній зміст про нібито додаток до АС «Android» за назвою «SexDrugWokrug.apk», який за описом призначений для пошуку друзів та 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» та переходить у фоновий режим, намагаючись з'єднатися з 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, та в разі позитивного результату намагається заволодіти грошовими коштами потерпілого шляхом здійснення

[1] Вирок Луцького міськрайонного суду Волинської області від 21 берез. 2018 р. Справа № 161/1345/18. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/72886703.

несанкціонованих платежів через систему миттєвих інтернет-розрахунків «WebMoney Transfer».

3. Технології «шпигунства», засновані на попередньому отриманні доступу до державної/комерційної таємниці шляхом несанкціонованого втручання в роботу комп'ютерної техніки. В Україні такі технології типово застосовують злочинець-упевнений користувач та злочинець-досвідчений користувач, які діють одноосібно з власних мотивів або на замовлення. Діяльність злочинця кваліфікується за сукупністю статей, що передбачають відповідальність за вчинення злочинів з двох умовних груп:

1) злочини, пов'язані зі збиранням або передаванням відповідного виду інформації з обмеженим доступом (ст. 231 (незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю) та/або ст. 232 (розголошення комерційної або банківської таємниці); ст. 111 (державна зрада) та/або ст. 114 (шпигунство);

2) злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, про які йдеться в розділі XVI КК України (ст. 361 (несанкціоноване втручання особи, що не має права доступу до інформації) та/або ст. 362 (несанкціоновані дії з інформацією особи, що має право доступу). Технології зберігання та обробки інформації, шкідливого програмного забезпечення, електронної розсилки та вікі(viki)-технології є найчастіше використовуваними злочинцем.

Видається доречним такий приклад[1]. 12 червня 2013 року о 01 год 34 хв гр. М., діючи умисно, віддалено з метою незаконного втручання в роботу комп'ютера шляхом подолання системного захисту, встановленого на сервері ТОВ «Укрнет2», видаючи себе за користувача системи, без згоди останнього змінив пароль доступу до електронної поштової скриньки та в такий незаконний спосіб створивши умови для вчинення подальших протиправних дій, отримав можливість змінювати на свою користь режим роботи поштового сервера, ознайомлюватись із відомостями, що становлять комерційну таємницю фізичної особи-підприємця О. Після цього з

[1] Вирок Луцького міськрайонного суду Волинської області від 12 трав. 2014 р. Справа № 161/20739/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/38642120.

метою комерційного шпигунства шахрай змінив режим роботи вузлового комп'ютера ТОВ «Укрнет». Для цього в обліковому записі без дозволу О. активував додаткову функцію «Пересилання» та в налаштуваннях зазначив параметри, за яких усі вхідні листи, отримані на електронну адресу О., автоматично пересилалися до спеціально створеної ним поштової скриньки. У результаті зловмисник отримав можливість ознайомлюватися з листуванням потерпілого. Таким шляхом М. скопіював клієнтську базу О., яку використовував у своїй комерційній діяльності, та отримав можливість повністю видаляти проекти робіт і замовлення, адресовані потерпілому. У цивільному позові матеріальну шкоду, завдану О., було оцінено в розмірі 200 000 грн. Гр. М. було притягнуто до кримінальної відповідальності за вчинення сукупності злочинів, передбачених ст. 231 та ч. 2 ст. 361 КК України.

Варто додати, що в разі вчинення такої злочинної діяльності «на замовлення» замовник часто залишається невстановленим, через що в суді вину підтверджують лише за статтями розділу XVI КК України. Показовою в цьому сенсі є раніше згадувана діяльність старшого оперуповноваженого з особливо важливих справ інформаційно-моніторингового відділу Головного управління внутрішньої безпеки Міністерства доходів і зборів України А., який неодноразово здійснював несанкціонований збут інформації з обмеженим доступом іншій особі за щомісячну грошову винагороду. Його діяльність було кваліфіковано за ст.ст. 361-2, 362 КК України [1].

4. Технології службових розкрадань шляхом застосування електронних платіжних систем, засновані на несанкціонованих діях з інформацією, вчинені особою, котра має право доступу до неї. В Україні такі технології типово застосовує злочинець-упевнений користувач, що діє одноосібно з власних мотивів або в групі осіб з чітким розподілом ролей. Діяльність злочинця кваліфікується за сукупністю ст. 191 КК України зі статтями розділу XVI КК України (найчастіше ст. 361-2, 362, 363; іноді ст. 361, 361-1, 363-1 відносно дій, що характеризують способи приховування злочину). Злочинні технології базуються на використанні банківських технологій,

[1] Вирок Шевченківського районного суду м. Києва від 23 квіт. 2014 р. Справа № 761/10994/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/38502750.

електронної комерції, електронних платіжних систем. Особливо складним для слідчого є встановлення корисливої мети діяльності злочинця. Так, мешканка м. Києва, перебуваючи на посаді адміністратора торговельного залу супермаркету «Варус», мала право доступу та безпосередній доступ до електронної програми касових операцій «Утиліта» зазначеного супермаркета. Маючи умисел щодо внесення неправдивих відомостей до розділу названої програми, а саме змінення суми фактичного залишку грошових коштів, зловмисниця неодноразово вносила зміни до розділу фактичного залишку грошових коштів, зменшуючи суму. Попри наявність фактичного матеріального збитку, спричиненого такими діями, розслідуванням не було доведено корисливу мету злочинця[1]. Вчиняючи такі злочини, шахраї зазвичай посилаються на помилкові дії або намагання приховати нестачу, яка фактично існувала до моменту їх злочинної дії.

5. Технології приховування незаконного походження безготівкових коштів, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки. Такі технології вдало застосовує група осіб, що дозволяє організатору злочинної схеми уникати кримінальної відповідальності, причому поза увагою слідчого залишається багато обставин вчинення злочину. Через це злочинна діяльність часто кваліфікується за ст. 361 та ст. 361-2 КК України або за ст. 205, 209 КК України. Така ситуація не дає можливості чітко впорядкувати сукупність злочинів, поєднаних цією технологією у єдиний ланцюг поведінки.

Розглянемо приклад. Невстановлені особи, перебуваючи у невстановленому місці, на початку листопада 2014 року, діючи умисно, з корисливих мотивів прийняли рішення зареєструвати в системі розрахунків «WebMoney Transfer» облікові записи на анкетні дані сторонніх осіб з метою їх подальшого незаконного використання для проведення незаконних трансакцій з титульними одиницями обліку майнових прав, також вони розробили відповідний план та

[1] Вирок Дарницького районного суду м. Києва від 25 жовт. 2016 р. Справа № 753/15944/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/62224792.

розподілили між собою злочинні ролі[1]. На початку листопада 2014 року на сайті Webmoney невстановлені особи запропонували гр. К. створити декілька акаунтів за винагороду, на що той погодився. Користуючись довірою до себе з боку працівників Дружківського МВ ГУМВС України в Донецькій області, К. незаконно отримав доступ до персональних даних фізичних осіб та паспортів осіб, які проходили як свідки, потерпілі, підозрювані за кримінальними провадженнями. Ці дані зловмисник використав для створення акаунтів (облікових записів окремих осіб у системі Webmoney Transfer). Пізніше невстановлені особи, незаконно використовуючи реквізити доступу до записів у системі, шляхом здійснення електронних трансакцій перевели з платіжної системи Epayments грошові кошти в сумі 20 265 та 9000 доларів США, легальне походження яких документально не підтверджено. З метою подальшої конвертації коштів у безготівкові кошти в банківській системі України особи здійснили трансакції з переведення титульних одиниць обліку майнових прав на облікові записи інших користувачів системи.

6. Технології незаконного збагачення, засновані на попередньому несанкціонованому втручанні в роботу комп'ютера, комп'ютерної системи, мережі з метою нейтралізації засобів інтелектуального захисту. Нині цю технологію не застосовує лише злочинець-користувач низького рівня. Кваліфікується така діяльність за сукупністю ст. 176 (порушення авторського та суміжних прав) та ст. 361 КК України. Так, у 2017 році мешканець м. Львова з корисливих мотивів з метою отримання прибутку, не маючи відповідного дозволу від правовласника програмного продукту «1С» – ДП «Єврософтпром», маючи дистрибутив програмного продукту«1С:Підприємство 8 (8.3.6.236)», єдиної автоматизованої системи, до складу якої віднесено безпосередньо програмне забезпечення та систему захисту від несанкціонованого використання із застосуванням апаратних ключів HASP, шляхом використання програмних засобів (патчів) для змінення функціональності програмних продуктів «1С» втрутився в роботу автоматизованої системи, що призвело до незаконного запуску та використання програмного продукту на платформі

[1] Вирок Дружківського міського суду Донецької області від 11 жовт. 2016 р. ЄУН 229/2951/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/62206468.

«1С:Підприємство8 (8.3.6.236)». Зазначені дії ОСОБА_1, призвели до порушення, встановленого порядку маршрутизації інформації, внаслідок чого програмний продукт«1С:Підприємство 8 (8.3.6.236)» став спроможним завантажуватися та працювати без електронного (апаратного) ключа захисту[1].

7. Технології незаконного збагачення шляхом незаконних дій з платіжними картками. Така злочинна діяльність в Україні найчастіше кваліфікується за сукупністю ст.ст. 200, 190 КК України. Можна навести такі сучасні закономірності названої злочинної діяльності: 1) складність технологій і тип злочинця нерозривно пов'язані; чим вище професіональний рівень зловмисника, тим складнішою є технологія; 2) початкові дії традиційного злочинця не спрямовані на незаконний вплив на засоби комп'ютерної техніки та інформацію; 3) така злочинна діяльність пов'язана із застосуванням комплексу спеціальних комп'ютерних технологій, що дозволяють виготовити дублікат справжньої банківської картки.

Найбільшого поширення на сьогодні набула технологія з визначеними етапами злочинної діяльності: 1) через електронні дошки оголошень або соціальні спільноти злочинець замовляє та отримує пристрій, що має функції зчитування, стирання, запису інформації на магнітній смузі пластикової платіжної карти; 2) використовуючи ті самі ресурси, злочинець підшукує персональні банківські відомості – так звані «дампи» про чужі банківські карти, їх власників/утримувачів та за допомогою кріпто-валюти «btc» (біткоін) через власний особистий рахунок набуває собі «дампи», емітовані іноземними банками, інформацію яких зберіг на власній Інтернет-сторінці; 3) підбір платіжних карт у вигляді емітованих в установленому законодавством порядку пластикових карток, що використовуються для переказу грошей з рахунку платника або відповідного рахунку банку, оплати товарів і послуг через банківські термінали; 4) за допомогою придбаного раніше обладнання здійснюється запис інформації на магнітні смуги підібраних для цього платіжних карток.

Так, гр. К., реалізовуючи свій злочинний намір з використанням Інтернет-ресурсу «Google Disk», отримував від невстановленої особи

[1] Вирок Франківського районного суду м. Львова від 23 черв. 2017 р. Справа № 465/2887/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/67455018.

на свій обліковий запис «Google» електронні файли, що містили інформацію про дані магнітних смуг платіжних карток клієнтів АТ «Ощадбанк» (що дають можливість ідентифікувати платіжну систему та емітента), які були необхідні для незаконного виготовлення «дублікатів» платіжних банківських пластикових карток та їх ПІН-кодів[1]. Для підробки платіжних карт К. за погодженням з невстановленою особою використовував спеціальні платіжні засоби у вигляді емітованих в установленому законодавством порядку пластикових карток (банківські платіжні картки, зокрема, строк дії яких завершився, картки надання дисконтних знижок у різноманітних закладах харчування, АЗС тощо з наявною відповідною магнітною смугою), а також білі пластикові картки з магнітними смугами. З квітня 2016 року, діючи за попередньою змовою з невстановленою особою, шахрай з'єднував зазначене обладнання в єдиний програмно-технічний комплекс, під'єднував до мережі Інтернет та за допомогою пристроїв «MSR606» (с/н 20130821 та с/н 20132176) записував на магнітні смуги підшуканих платіжних карток реквізити (отримані від невстановлених розслідуванням осіб текстові та цифрові дані) банківських карт клієнтів АТ «Ощадбанк», отримуючи таким чином їх копії. Частина з них була не персоніфікованою, але функціональною за призначенням. Після виготовлення таких копій банківських карток клієнтів АТ «Ощадбанк» зловмисник провів низку несанкціонованих трансакцій через банкомати.

Знання типових способів/технологій вчинення злочинів у кіберпросторі, закономірних зв'язків між мотивом вчинення злочину та предметом посягання, особою злочинця та слідами вчинення злочину дозволить слідчому в перебігу розслідування конкретного кримінального правопорушення якісно та методично обґрунтовано поставитися до висування версій, організації та планування досудового розслідування.

[1] Вирок Шевченківського районного суду м. Києва від 30 листоп. 2016 р. Справа № 761/39282/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/63392350.

РОЗДІЛ 3
ВІДКРИТТЯ КРИМІНАЛЬНОГО ПРОВАДЖЕННЯ ТА ВЗАЄМОДІЯ СЛІДЧОГО ПІДЧАС РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

3.1. Організаційні форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі

Специфічність механізму вчинення злочинів у кіберпросторі, зокрема, особливості їх слідів, які можуть бути легко фальсифіковані або взагалі знищені, обумовлює й особливості початку кримінального провадження щодо цих злочинів. Тут йдеться про ті особливості, які вимагають їх врахування з точки зору забезпечення судової перспективи таких справ.

Взагалі реформування кримінально-процесуального законодавства надало питанню початку кримінального провадження важливого значення у розробці методик розслідування певних видів (груп) злочинів. Ця проблема спричинена відмовою законодавця від такої стадії кримінального процесу, як порушення кримінальної справи, що до прийняття 2012 року КПК України передбачала механізм перевірки заяв і повідомлень про кримінальне правопорушення. Саме з ним була пов'язана наявність в окремих криміналістичних методиках такого структурного елементу, як «попередні дії слідчого до порушення кримінальної справи»[1], «дослідчі ситуації»[2] або «оцінка первинної інформації»[3].

В чинному КПК України (ч. 1 ст. 214) визначено процедуру початку досудового розслідування, яка передбачає обов'язок слідчого (прокурора) невідкладно (не пізніше 24 год) після подання заяви, повідомлення про вчинене кримінальне правопорушення або після

[1] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. С. 157.

[2] Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности : монография. Харьков : Нац. ун-т внутр. дел, 2002. 412 с.

[3] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 426 с.

самостійного виявлення ним з будь-якого джерела обставин, що можуть свідчити про вчинення кримінального правопорушення, внести відповідні відомості до Єдиного реєстру досудових розслідувань (ЄРДР) і розпочати розслідування. Також обов'язком слідчого є надання заявнику через 24 години з моменту внесення таких відомостей витягу з Єдиного реєстру досудових розслідувань. Згідно з ч. 4 ст. 214 КПК України, відмова слідчого або прокурора в прийнятті та реєстрації заяви чи повідомлення про кримінальне правопорушення не допускається[1].

Таким чином, кримінально-процесуальний закон на цій стадії не передбачає оцінки заяви або повідомлення про вчинене кримінальне правопорушення на предмет наявності чи відсутності ознак складу злочину. Фактично слідчий зобов'язується констатувати виявлення злочину на момент внесення отриманої інформації до ЄРДР. Але це виглядає дещо нелогічним, адже слідчий не має у своєму розпорядженні достатнього арсеналу процесуальних засобів підтвердження або спростування отриманої інформації. Очевидно, що це повинно здійснюватися ним вже під час досудового розслідування.

Ця проблема спричинила жваві дискусії поміж вчених. Так, на думку Ю. П. Аленіна, процесуальний порядок, встановлений у ст. 214 КПК України, не враховує загальні положення процесуальної діяльності та національні правові традиції. Науковець стверджує, що будь-яка галузь процесуального права має передбачати попередній[2], перевірочний, фільтраційний етап перед основним провадженням[3]. Інші дослідники початок досудового розслідування, регламентований ст. 214 КПК України, пропонують розглядати як самостійну стадію кримінального процесу, аргументуючи це тим, що будь-яка його

[1] Узагальнення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ «Про практику розгляду скарг на рішення, дії чи бездіяльність органів досудового розслідування чи прокурора під час досудового розслідування» (станом на 12.01.2017). URL: http://protokol.com.ua/ua/vssu_uzagalnennya_pro_praktiku_rozglyadu_skarg_na_rishennya_dii_chi_bezdiyalnist_organiv_dosudovogo_rozsliduvannya/.

[2] Галаган В. І. Проблеми вдосконалення кримінальнопроцесуальної діяльності органів внутрішніх справ України : монографія. К. : Нац. академія внутр. справ України, 2002. 300 с.

[3] Аленін Ю. П. Початок досудового розслідування за КПК України 2012 р. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 201.

стадія визначається чотирма ознаками: 1) безпосередніми завданнями; 2) підсумковими рішеннями; 3) особливою процесуальною формою; 4) певним колом учасників[1].

У зв'язку з цим важливим є врахування таких міркувань:

– завданням початку досудового розслідування є своєчасна реакція з боку вповноважених державних органів на інформацію про кримінальне правопорушення (полягає в невідкладній реєстрації в ЄРДР і початку кримінального провадження) поєднана з аналізом отриманих відомостей, які можуть не утримувати ознак саме кримінального правопорушення або взагалі бути помилковими чи неправдивими;

– на цій стадії не лише приймаються заяви, повідомлення про вчинене кримінальне правопорушення та здійснюється їх перевірка, але й приймається обґрунтоване рішення щодо проведення досудового розслідування за іншими джерелами інформації;

– ця стадія не залежить від інших етапів кримінального провадження, зміст її зумовлений колом вирішуваних питань.

Отже, сутність стадії початку досудового розслідування виявляється в процесуальній діяльності слідчого, прокурора з розгляду первинної інформації про кримінальне правопорушення (її прийняття, реєстрація, перевірка та прийняття рішення).

Потрібно зазначити, що у криміналістичній інтерпретації не сформувався єдиний підхід щодо визначення місця стадії початку досудового розслідування в окремих методиках розслідування злочинів. Більшість науковців, що досліджують методики розслідування окремих видів злочинів, узагалі намагаються уникати цієї проблеми, не висвітлюючи завдань слідчого з виявлення кримінального правопорушення, сучасних реалій реформування правоохоронних органів і перспектив діяльності «детективів» у структурі Національної поліції України.

У цьому контексті В. А. Журавель відзначає потребу у виділенні самостійного етапу розслідування «відкриття кримінального

[1] Кримінальне процесуальне право України : навч. посіб. / [К. В. Бєляєва, А. М. Бірюкова, В. І. Бояров та ін.] ; за заг. ред. В. Г. Гончаренка, В. А. Колесника. Київ : Юстиніан, 2014. 573 с.; Нор В. Т., Бобечко Н. Р. Кримінально-процесуальне законодавство України: досягнення, загрози, очікування. Право України. 2016. № 12, С. 9-18.

провадження»[1]. На думку науковця, доцільність виокремлення його як «вихідного етапу розслідування» зумовлена специфікою процесуальних дій, з провадження яких розпочинається досудове розслідування, колом суб'єктів, які беруть участь у здійсненні цих дій (слідчий, прокурор, заявник та інші), характером вихідних завдань, що підлягають виконанню, потребою у визначенні головних напрямів діяльності слідчого. Аргументуючи своє бачення періодизації процесу розслідування, автор посилається на кримінально-процесуальну позицію, висловлену в одному з базових підручників з кримінального процесу, зокрема резюмує таке: «Зазначена діяльність відповідає критеріям самостійного провадження, оскільки є системою процесуальних дій у межах кримінальної процесуальної форми досудового провадження, які зумовлюють виникнення певної сукупності процесуальних відносин та спрямовані на виконання єдиного завдання, і цілком правомірним є розуміння й дослідження цієї діяльності саме як самостійного провадження»[2].

Утім на доктринальному рівні в кримінально-процесуальній літературі досудове розслідування залишається самостійною стадією кримінального процесу, яка відповідно до конструкції чинного КПК України починається з моменту внесення відомостей про кримінальне правопорушення до ЄРДР і закінчується закриттям кримінального провадження або направленням до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру або клопотання про звільнення особи від кримінальної відповідальності[3]. З огляду на це, є некоректним ототожнення початку провадження з перебігом досудового розслідування.

З криміналістичних позицій А. Ф. Волобуєв звертає увагу на руйнацію не лише теоретичних конструкцій криміналістичної методики, а й певного алгоритму діяльності органів досудового слідства внаслідок

[1] Журавель В. Проблеми періодизації досудового розслідування. *Вісник Національної академії правових наук України*. 2014. № 2 (77). С. 141.

[2] Вапнярчук В. В. Досудове провадження. Глава 14. *Кримінальний процес* : підручник / [Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.] ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. С. 334.

[3] Лобойко Л. М., Банчук О. А. Кримінальний процес : навч. посіб. Київ : Ваіте, 2014. С. 22.

перекладання функції перевірки заяв і повідомлень на слідчого[1]. На цьому акцентує увагу чимало криміналістів і процесуалістів[2]. Ця проблема є достатньо актуальною, оскільки кримінально-процесуальний закон створює організаційно-правові передумови для формування криміналістичної науки, якій потрібно орієнтуватися на нові реалії практики застосування положень КПК України.

З позицій слідчої практики процесуальний порядок початку кримінального провадження триває з моменту, коли суб'єкту розслідування стало відомо про джерело обставин, що можуть свідчити про кримінальне правопорушення, до моменту внесення відповідної інформації до ЄРДР. Внутрішня організація слідчим початку кримінального провадження залежатиме від чинників як правового, так і неправового (організаційного) характеру. Оскільки способи внутрішньої організації будь-якого процесу прийнято іменувати словом «форма» (лат. forma), що означає зовнішній вигляд, вияв, конфігурацію або межі об'єкта[3], то теоретичний аспект організації слідчим початку провадження ми будемо окреслювати категорією «форма початку кримінального провадження».

Правові чинники зумовлюють форми початку кримінального провадження, пов'язані з характером джерела обставин[4], що можуть свідчити про вчинення певного виду кримінального правопорушення. З огляду на зміст ст. 214 КПК України та відповідно до численних підзаконних актів (Порядок ведення єдиного обліку в органах

---

[1] Волобуєв А. Ф. Проблемні питання початку досудового розслідування. *Актуальні проблеми кримінального права, процесу та криміналістики* : матеріали V Міжнар. наук.-практ. конф. (Одеса, 1 листоп. 2013 р.). Одеса : Фенікс, 2013. С. 237–240.

[2] Татаров О. Ю. Досудове провадження в кримінальному процесі України: теоретико-правові та організаційні засади (за матеріалами МВС) : монографія. Донецьк : Промінь, 2012. 640 с.; Смоков С. М. Окремі проблемні питання, які виникають при застосуванні норм нового КПК України. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 110–115.

[3] Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. 4-е изд., доп. М. : Азбуковник, 1999. 944 с. URL: http://www.ozhegov.org/words/38325.shtml.

[4] Никифорчук Д. Й. До питання використання результатів оперативно-розшукової діяльності у кримінальному судочинстві. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. Вип. 22. С. 61-66.

(підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події[1], Положення про порядок ведення Єдиного реєстру досудових розслідувань[2], Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України[3], Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами НП України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні[4]), можна виокремити три групи джерел обставин, що можуть свідчити про вчинені кримінальні правопорушення, зокрема:

1) заяви і повідомлення осіб про вчинене кримінальне правопорушення, що надходять до правоохоронного органу (Національної поліції, органу безпеки, слідчого, іншого органу або службової особи, уповноваженої на прийняття та реєстрацію заяв і повідомлень про кримінальні правопорушення);

2) матеріали розпочатого раніше кримінального провадження;

3) ініціативні рапорти співробітників оперативного підрозділу про виявлення ними кримінального правопорушення з інших джерел інформації.

Розгляньмо ці групи детальніше.

1. Заяви і повідомлення осіб про вчинене кримінальне правопорушення, що надходять до правоохоронного органу. Внесення до ЄРДР відомостей про кримінальне правопорушення, викладених у

[1] Про завтвердження порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події : наказ МВС України від 8 лют. 2019 р. № 100. URL: https://zakon.rada.gov.ua/laws/show/z0223-19#n7.

[2] Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 6 квіт. 2016 р. № 139. URL: https://www.gp.gov.ua/ua/pd.html?_m=publications& t=rec&id=110522.

[3] Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ МВС України від 15 листоп. 2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

[4] Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

цьому джерелі інформації, є обов'язком слідчого або щодо проваджень у формі приватного обвинувачення прокурора. Це процесуальне рішення вони приймають упродовж визначених законом 24 годин з моменту реєстрації уповноваженими працівниками чергової частини таких заяв і повідомлень. Їх реєстрацію здійснюють цілодобово в журналі Єдиного обліку, працівник чергової частини доповідає відповідну інформацію начальнику органу поліції та за резолюцією останнього спрямовує заяву або повідомлення начальникові слідчого підрозділу для внесення слідчими відповідних відомостей до ЄРДР.

До початку кримінального провадження за умови наявності реальної можливості конкретизувати отриману інформацію про вчинення злочину слідчий спроможний провести лише огляд місця події.

2. Матеріали кримінального провадження. Слідчий у межах компетенції, визначеної ст. 40 КПК України, може виявити відомості про вчинення кримінального правопорушення під час досудового розслідування в іншому кримінальному провадженні.

Розслідування злочину з позиції криміналістичної науки можна відобразити у вигляді послідовного або паралельного виконання слідчим низки локальних завдань, які у своїй системі забезпечують розкриття злочину й усебічне, повне та об'єктивне дослідження обставин, що належать до предмета доказування в кримінальному провадженні[1]. Визначення змісту типової слідчої ситуації конкретного злочину, оцінка предмета доказування у справі надають можливість сформулювати відповідне тактичне завдання розслідування щодо виявлення інших епізодів злочинної діяльності й обрати криміналістичні засоби його виконання: слідчі (розшукові) дії та інші заходи.

Наділення слідчого повноваженнями проводити негласні слідчі (розшукові) дії, які мають характер пошукових заходів, що традиційно проводять оперативні підрозділи для виявлення злочину, суттєво змінює характер діяльності слідчого під час розслідування кримінального правопорушення. Адже негласні слідчі (розшукові) дії та оперативно-розшукові заходи мають схожий порядок проведення. У сучасних умовах на високому рівні такою компетентністю вже

[1] Баев О. Я. О методических основах расследования насильственных преступлений. *Актуальные вопросы уголовного права, процесса и криминалистики* : сб. науч. тр. Калининград, 1998. С. 74.

володіють працівники слідчого підрозділу, які до призначення на посаду слідчого працювали в оперативних підрозділах або пройшли фахову підготовку чи підвищення кваліфікації за профілем їхньої роботи.

Повідомлення органів поліції про вчинення нового епізоду злочину, встановленого під час розслідування дорученої справи, здійснюють шляхом складання слідчим рапорту на ім'я начальника органу поліції.

3. Ініціативні рапорти співробітників оперативного підрозділу про виявлення ними кримінального правопорушення та долучені до них матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп, відповідальність за які передбачена КК України.

Не всі заяви та повідомлення про вчинене кримінальне правопорушення спрямовують до слідчого відділу, певну їх частину, яку начальник органу (підрозділу) поліції оцінює як анонімне повідомлення або звернення громадян у значенні письмової або усної форми пропозиції (зауваження), заяви (клопотання) чи скарги[1], направляють для виконання в оперативний підрозділ. Співробітник оперативного підрозділу має законодавчо визначений проміжок часу для підтвердження викладених у них обставин шляхом здійснення оперативно-розшукових заходів в межах попередньої перевірки.

Про результати такої перевірки поліцейські доповідають безпосередньому керівникові у формі рапорту. Якщо внаслідок перевірки отримано відомості про осіб, які вчинили кримінальні правопорушення, а також про події та факти, які можуть сприяти розкриттю та досудовому розслідуванню, то за резолюцією відповідного керівника органу або підрозділу поліції приймають рішення про оформлення отриманої інформації з метою її передання на розгляд керівникові органу досудового розслідування та внесення до ЄРДР. Оформлюють повідомлення у формі ініціативного рапорту.

Про такий рапорт ідеться також за умови, коли підстави для проведення оперативно-розшукової діяльності містяться в інших джерелах інформації про злочин, зокрема:

1) повідомленнях осіб, які затримали підозрювану особу під час вчинення або замаху на вчинення кримінального правопорушення або

[1] Про звернення громадян : Закон України від 2 жовт. 1996 р. № 393/96-ВР. *Відомості Верховної Ради України.* 1996. № 47. Ст. 256.

безпосередньо після вчинення кримінального правопорушення чи під час безперервного переслідування особи, яку підозрюють у його вчиненні;

2) заявах і повідомленнях громадян, з якими встановлено негласне співробітництво;

3) повідомленнях посадових осіб, громадських організацій;

4) публікаціях засобів масової інформації;

5) письмових дорученнях і постановах слідчого;

6) матеріалах інших правоохоронних органів;

7) запитах і повідомленнях правоохоронних органів інших держав, міжнародних правоохоронних організацій;

8) інших відомостях, отриманих унаслідок оперативно-розшукової діяльності.

Якщо інформація стосується тяжких та особливо тяжких злочинів, що готуються, то оперативно-розшукову діяльність здійснюватимуть у межах плану заходів з реалізації матеріалів оперативно-розшукової справи, який згідно Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами НП України затверджують начальники оперативного підрозділу й органу досудового розслідування. Оскільки цією Інструкцією на керівників органу досудового розслідування та оперативних підрозділів (за посадовими інструкціями) покладено однакові обов'язки щодо забезпечення збору, накопичення, систематизації отриманої інформації та здійснення її перевірки з метою встановлення осіб, які вчинили кримінальні правопорушення, а також подій і фактів, які можуть сприяти їх розкриттю та досудовому розслідуванню, то спільна узгоджена діяльність слідчого й оперативного працівника для початку кримінального провадження стала правилом, а не рекомендацією.

Тому в практичній площині з метою виявлення злочину слідчий діє двома способами. По-перше, оцінює наданий йому оперативним підрозділом матеріал перевірки на предмет визначення ознак вчинення злочину певної кваліфікації. По-друге, бере активну участь у розробленні плану заходів з реалізації матеріалів оперативно-розшукової справи та з дотриманням режиму секретності здійснює методичне супроводження справи та надання практичної допомоги оперативному підрозділу. Тут ідеться згідно з вищенаведеною Інструкцією про можливість закріплення керівником органу

досудового розслідування на письмове звернення керівника оперативного підрозділу слідчого за оперативно-розшуковою справою.

Матеріали саме такої оперативно-розшукової діяльності стають для слідчого джерелом обставин, що засвідчують вчинення кримінального правопорушення, їх відображають у формі рапорту співробітника оперативного підрозділу, іноді безпосередньо слідчого. З метою реалізації цих матеріалів слідчий розпочинає досудове розслідування відповідно до положень ст. 214 КПК України. У зв'язку із зазначеним, слід констатувати важливість розуміння слідчим засад оперативно-розшукової діяльності. Особливості використання функціоналу оперативно-розшукової діяльності з метою виявлення кримінального правопорушення є *організаційними чинниками, що зумовлюють особливості форми початку кримінального провадження щодо окремого виду злочинів*.

Отже, особливості використання функціоналу оперативно-розшукової діяльності з метою виявлення кримінального правопорушення є *організаційними чинниками, що зумовлюють організаційні форми початку кримінального провадження щодо окремого виду злочинів*.

Тож, у методиках розслідування окремих видів злочинів можна визначити форми початку кримінального провадження в значенні певних способів слідчого організовувати виявлення ознак кримінального правопорушення, що зумовлені специфікою джерела обставин, які можуть свідчити про вчинення злочину певного виду, і типовим функціоналом оперативно-розшукової діяльності щодо окремого виду злочинів. Можна назвати наступні чотири форми початку кримінального провадження.

1. Кримінальне провадження розпочинають в результаті отримання заяви потерпілого/повідомлення особи про кримінальне правопорушення («безальтернативна форма»). По суті, це безальтернативний спосіб реагування на отриману інформацію – вчиненні активних дій з внесення таких відомостей до ЄРДР протягом 24 годин.

2. Кримінальне провадження розпочинають в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації («альтернативна форма»). Ця форма початку провадження пов'язана з оцінною діяльністю слідчого щодо матеріалів перевірки оперативних джерел інформації про злочин.

Слідчий під час отримання матеріалів перевірки має альтернативу внесенню відповідної інформації до ЄРДР – це повернення матеріалів до оперативного підрозділу для доопрацювання з рекомендаціями щодо подальших дій суб'єкта перевірки. Тому у криміналістичній науці питання діяльності працівників оперативних підрозділів традиційно розглядають крізь призму їхньої взаємодії зі слідчими[1].

У цьому контексті слід акцентувати увагу на значенні заяви та повідомлення, що містять оцінні (суб'єктивні) судження заявника або не містять дані про особу відправника (анонімні). Їх за оцінкою начальника органу (підрозділу) поліції вважають зверненням і перевіряють саме шляхом здійснення заходів оперативно-розшукової діяльності. Згідно з Порядком розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України[2], щодо кожного звернення суб'єкт отримання не пізніше ніж у п'ятиденний термін приймає одне з таких рішень: 1) прийняти до розгляду; 2) передати на вирішення до підпорядкованого органу (підрозділу) поліції; 3) надіслати за належністю до іншого державного органу або посадовій особі; 4) залишити без розгляду за наявності підстав, визначених у ст. 8 Закону України «Про звернення громадян». Цей механізм у правоохоронних органах можна вважати «своєрідною фільтрацією» заяв і повідомлень про вчинений злочин.

3. Кримінальне провадження розпочинають в рамках реалізації матеріалів ОРС («безініціативна форма»). Цю форму слідчий реалізує шляхом методичного супроводження оперативно-розшукової діяльності в межах ОРС. Унаслідок діяльності оперативних підрозділів за спільним зі слідчим планом реалізації матеріалів ОРС

---

[1] Бекетов М. Ю. Следователь органов внутренних дел и милиция: взаимодействие при расследовании преступлений : учеб. пособие. М. : Щит-М, 2004. 96 с.; Пивоваров В. В., Щербина Л. І. Взаємодія органів досудового слідства та дізнання при розслідуванні кримінальних справ : монографія. Харків : Право, 2006. 176 с.; Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с.

[2] Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ МВС України від 15 листоп. 2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

слідчий встановлює факт підготовки та вчинення тяжких й особливо тяжких злочинів, що призводить до «безоціночного» внесення відомостей, викладених в ініціативному рапорті про виявлення злочину, до ЄРДР. Тут не може йтися про «абсолютну ініціативу» слідчого в питаннях проведення слідчих (розшукових) дій, адже їх здійснення буде пов'язане із завершенням оперативно-розшукових заходів, а проведення подальших негласних слідчих (розшукових) дій залежатиме від результатів проведення оперативно-розшукових заходів, значення таких результатів для кримінального провадження. У цьому контексті вбачається практичний сенс у позиції В. М. Мєшкова та В. Л. Попова, які зазначали, що в розробці всіх рекомендацій, як криміналістичних, так й оперативно-розшукових, повинен діяти постулат про те, що діяльність з виявлення, розкриття, розслідування злочинів є єдиною та неподільною[1]. У своїй праці з проблем оперативно-розшукової тактики вчені стверджують, що немає і не може бути різних стадій розкриття та розслідування злочину. Тому пропонують розглядати діяльність оперативного співробітника та слідчого як єдине ціле. В Україні саме такий зміст досудового слідства нині намагаються реалізувати за задумом законодавця.

4. Кримінальне провадження розпочинають в результаті виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні («ініціативна форма»). Традиційно діяльність з розслідування злочинів є специфічним видом соціальної практики, що полягає в пізнанні подій протиправного характеру за допомогою передбачених законом засобів і прийомів, з-поміж яких і примусова реалізація їх у разі чинення протидії[2]. Основу комплексу пізнавальних засобів становлять слідчі (розшукові) дії. Деталізувати таку форму початку кримінального провадження можна через визначення ситуаційного характеру підготовки та проведення засобів

[1] Мешков В. М., Попов В. Л. Оперативно-розыскная тактика и особенности легализации полученной информации в ходе предварительного следствия : учеб.-практ. пособие. М. : Щит-М, 1999. С. 9.

[2] Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. *Теорія і практика :* навч. посіб. Київ : КНТ, 2008. С. 147.

криміналістичної техніки та криміналістичної тактики на криміналістичних етапах розслідування.

Визначення специфіки початку кримінального провадження щодо певного виду злочинів надасть можливість використовувати результати оперативно-розшукової діяльності як докази, забезпечить повноту досудового слідства та перспективу судового розгляду матеріалів таких кримінальних проваджень. З огляду на особливий комплексний і транснаціональний характер злочинної діяльності в кіберпросторі, спираючись на запропоновані нами класифікаційні групи та підгрупи таких злочинів, охарактеризуємо організаційні форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі.

1. Кримінальне провадження розпочинають в результаті отримання заяви потерпілого/повідомлення особи про кримінальне правопорушення.

Типово заява складається власником певного інформаційного продукту/майна, особи, що став предметом злочинного посягання, жертвою насильницько-дискримінаційних дій у кіберпросторі, повідомлення особи про кримінальне правопорушення – представником установи-жертви, Інтернет-сервісу, власником веб-сайту, що зазнав злочинного впливу. В арсеналі способів дії слідчого є опитування, огляд місця події та організаційні заходи у формі звернення до відкритих джерел інформації з метою підтвердження отриманих відомостей.

Така форма властива кожній класифікаційній підгрупі злочинів, вчинених у кіберпросторі, зокрема: інтелектуальному піратству та злочинам, пов’язаним із комунікаційними діями (90 % аналізованих проваджень); злочинам, пов’язаним із насильницько-егоїстичними діями (70 %); злочинам, пов’язаним з анархістськими діями в кіберпросторі (40 %); злочинам, що спрямовані на заволодіння чужим майном, і пов’язаним із ними злочинам у сфері функціонування електронних розрахунків (40 %); злочинам, що пов’язані з насильницько-дискримінаційними діями (40 %); злочинам, що порушують механізми захисту від монополізму та недобросовісної конкуренції (25 %); злочинам, що порушують встановлений порядок обігу певних речей (10 %), і злочинам, що пов’язані з антидержавницькими діями (10 %).

Часто після відкриття кримінального провадження за ознаками тяжкого або особливо тяжкого злочину, вчиненого в кіберпросторі, суб'єкт, який зазнав шкоди, через небажання розголошувати свою неспроможність захистити інформацію, перспективу втратити довіру клієнтів не бажає співпрацювати зі слідчим. Аналогічно й потерпілі, які на момент подання заяви про кримінальне правопорушення не були обізнані, що «близька» людина (чоловік (дружина), інший член сім'ї), найманий працівник вчинили тяжкий злочин проти них. Це провокує створення потужних важелів протидії розслідуванню, для подолання яких в умовах наявності неперевіреної, первинної, інформації про злочин слідчому вкрай потрібно налагоджувати взаємодію із оперативними підрозділами, використовувати арсенал засобів оперативно-розшукової діяльності.

2. Кримінальне провадження розпочинають в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації.

Аналіз матеріалів слідчо-судової практики дає підстави для визначення специфіки цієї форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі. З одного боку, можливість встановлення первинної кваліфікації події за результатами ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації надали можливість слідчому внести відповідні дані до ЄРДР і розпочати розслідування щодо:

– 40 % злочинів, що спрямовані на заволодіння чужим майном, і пов'язаних із ними злочинів у сфері функціонування електронних розрахунків;

– 40 % злочинів, пов'язаних з анархістськими діями в кіберпросторі (розділ XVI КК України);

– 10 % злочинів, що порушують встановлений порядок обігу певних речей, і злочинів, пов'язаних із насильницько-егоїстичними діями (ст. 301 КК України);

– 10 % злочинів, пов'язаних із насильницько-егоїстичними діями (ст. 301 КК України). З іншого боку, ці показники поширеності форми мають бути вищими за рахунок показників безальтернативної форми початку провадження, адже в половині аналізованих матеріалів кримінальних проваджень констатовано формалізовану наявність повідомлення про вчинення злочинів, попередження, виявлення та припинення яких належать до завдань Департаменту кіберполіції

Національної поліції України. Цей умовивід засвідчують результати анкетування співробітників оперативних підрозділів, 90 % з яких визнали складність реалізації матеріалів перевірки щодо нетяжких і середньої тяжкості злочинів, вчинених у кіберпросторі. Зазначене зумовлено декількома чинниками.

По-перше, у регіонах України досі немає слідчих або прокурорів, які були б спроможні оцінити достовірність інформації, отриманої під час перевірки оперативної інформації про злочин у кіберпросторі. Спеціалізація слідчих щодо розслідування злочинів цієї категорії регламентована лише на рівні ГСУ Національної поліції України.

По-друге, в умовах надмірного навантаження слідчого/прокурора суб'єкт початку провадження не має часу на пізнання сутності джерела інформації в кіберпросторі. Тому він з підстав «неможливості здійснити первинну кваліфікацію події» повертає такі матеріали в оперативний підрозділ з вказівками щодо конкретизації певних обставин події (особи злочинця та мотиву, наслідків вчинення правопорушення, розміру шкоди та інших).

По-третє, оскільки оперативні підрозділи фактично позбавлені можливості здійснювати оперативно-розшукові заходи під час перевірки оперативної інформації щодо вчинення невеликої або середньої тяжкості злочинів, а попередження, виявлення та припинення більшості таких злочинів належать саме до завдань Департаменту кіберполіції Національної поліції України, то повернення матеріалів перевірки інформації про них дедалі частіше зводиться до віднесення їх до категорії «латентна злочинність».

Внесення відповідної інформації до ЄРДР цілком залежить від майстерності слідчого/прокурора оцінювати матеріали первинної перевірки. На жаль, уже в розпочатих у такий спосіб провадженнях ініціаторами взаємодії зі слідчим залишаються оперативні співробітники, що здійснювали перевірку інформації про злочин. Вони вже під час проведення досудового слідства надають слідчому в не процесуальний спосіб усні рекомендації щодо провадження тих чи тих негласних слідчих (розшукових) дій, які потім самі проводять за дорученням слідчого.

Із цих позицій важливим є значення прийнятого Верховною Радою України 22 листопада 2018 року Закону України «Про внесення змін до деяких законодавчих актів України щодо спрощення

досудового розслідування окремих категорій кримінальних правопорушень». Із 1 січня 2020 року кримінальні правопорушення поділяються на кримінальні проступки і злочини, невеликої та середньої тяжкості злочини буде об'єднано в нову кримінально-правову категорію – «нетяжкі кримінальні правопорушення». Згідно із змінами ст. 12 КК України, кримінальним проступком буде дія чи бездіяльність, за вчинення якої передбачено основне покарання у виді штрафу в розмірі не більше ніж три тисячі неоподатковуваних мінімумів доходів громадян або інше покарання, не пов'язане з позбавленням волі. Такі правопорушення розслідуватимуть за спрощеною процедурою здійснення досудового розслідування.

Це нововведення призначене розвантажити слідчих правоохоронних органів, адже провадження щодо проступків здійснюватиме спеціальний суб'єкт – дізнавач, який буде співробітником новоствореного органу дізнання або іншого підрозділу Національної поліції, уповноваженим на здійснення дізнання. З метою спрощення процесу розслідування буде логічним уповноважити на це співробітника оперативного підрозділу, який виявив відповідний факт вчинення проступку та знає обставини його події краще, ніж будь-хто з працівників правоохоронного органу. Утім аналіз санкцій статей КК України засвідчує, що злочини, попередження, виявлення та припинення яких належать до завдань Департаменту кіберполіції Національної поліції України, не будуть проступками, більшість із них визначаються як «нетяжкі злочини». Тому вони не підслідні суб'єкту здійснення дізнання.

Розв'язанню окресленої вище проблеми реалізації цієї форми початку провадження щодо виявлених кіберполіцейськими злочинів могла б сприяти новація законодавця щодо створення можливостей здійснення розслідування у формі дізнання не лише стосовно проступків, а й щодо нетяжких злочинів. Адже за такої умови кіберполіцейський щодо виявлених ним нетяжких злочинів буде вправі відкривати кримінальне провадження та здійснювати розслідування у формі дізнання.

3. Кримінальне провадження розпочинають в рамках реалізації матеріалів ОРС.

Робота слідчого в межах ОРС здійснюється в умовах викриття 90 % злочинів, вчинених у кіберпросторі з антидержавно-політичних мотивів, 40 % злочинів, що порушують встановлений порядок обігу

певних речей, і 10 % злочинів, пов'язаних з анархістськими діями в кіберпросторі (ч. 2 ст. 361, ч. 3 ст. 362 КК України) та з насильницько-егоїстичними діями (ч. 3 ст. 120; ч. 3–5 ст. 301 КК України). Матеріали оперативно-розшукових заходів, що проводять за такими справами, слідчий використовує надалі як докази. Це дає підстави стверджувати, що, крім слідчих (розшукових) дій, до комплексу пізнавальних засобів слідчого під час розслідування тяжких та особливо тяжких злочинів, вчинених у кіберпросторі, належатимуть й оперативно-розшукові заходи. Обґрунтовано обрати слідчому найбільш доцільні комплекси слідчих (розшукових) дій та організаційних заходів на криміналістичних етапах розслідування злочинів, вчинених у кіберпросторі, надасть можливість налагоджена на момент початку кримінального провадження взаємодія із оперативними підрозділами.

4. Кримінальне провадження розпочинають внаслідок виявлення безпосередньо слідчим іншого кримінального правопорушення під час здійснення досудового розслідування в уже дорученому для здійснення розслідування кримінальному провадженні.

Лише 16 % кримінальних проваджень щодо досліджуваної категорії злочинів відкриває слідчий унаслідок здійснення розслідування в іншому кримінальному провадженні, як правило, випадково, під час виявлення ознак вчинення злочину іншої кваліфікації під час провадження обшуку, в результаті отримання результатів судової експертизи (зокрема так виявляються 50 % злочинів, що порушують механізми захисту від монополізму та недобросовісної конкуренції, або злочини, пов'язані з насильницько-дискримінаційними діями; 20 % злочинів, що спрямовані на заволодіння чужим майном, і пов'язаних із ними злочинів у сфері функціонування електронних розрахунків; 10 % злочинів, що порушують встановлений порядок обігу певних речей, злочинів, пов'язаних із насильницько-егоїстичними діями, і злочинів, пов'язаних з анархістськими діями в кіберпросторі). Тому таку форму початку кримінального провадження складно вважати типовою стосовно злочинів, вчинених у кіберпросторі. З огляду на те, що фактично в кіберпросторі триває багатоепізодна злочинна діяльність, така ситуація спричинена формальним ставленням слідчих до планування розслідування, незалученням до цього процесу потенціалу оперативних підрозділів або перекладанням своїх повноважень щодо здійснення слідчих (розшукових) дій у таких справах на оперативного працівника.

Така форма початку провадження реалізується в межах одного з основних завдань розслідування – виявлення всієї сукупності епізодів злочинної діяльності в кіберпросторі, – яке виконують шляхом здійснення комплексу слідчих (розшукових) дій та організаційних заходів. Зазначене призводить до реєстрації додаткових епізодів кримінального правопорушення певної правової кваліфікації (залежно від типового поєднання злочинів у злочинну технологію або всієї множини одиничних схожих злочинів).

Підсумовуючи, потрібно відзначити, що наведені форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі, свідчать про ключову роль взаємодії слідчого і спеціалізованих оперативних підрозділів, особливо у визначенні оптимального моменту початку досудового розслідування. Останнє обумовлено тим, що в більшості випадків кримінальні провадження даної категорії відкриваються саме за матеріалами оперативно-розшукової діяльності.

3.2. Суб'єкти взаємодії зі слідчим підчас розслідування злочинів, вчинених у кіберпросторі

Взаємодією слідчого з оперативними підрозділами, підприємствами, установами, громадськістю та засобами масової інформації є спільна та взаємопогоджена діяльність, спрямована на розслідування й попередження злочинів[1]. Це такий взаємозв'язок у їхній діяльності, що забезпечує правильне поєднання повноважень, методів і засобів, притаманних кожному з учасників взаємодії.

Сутність взаємодії полягає в узгодженій діяльності різних складових однієї чи декількох систем. Кожний суб'єкт взаємодії діє в межах своїх повноважень, методів і засобів. Вважається, що провідна роль організації взаємодії належить слідчому як координатору діяльності, певні способи зв'язку між слідчим і суб'єктами взаємодії називають формами взаємодії.

[1] Криміналістика : підручник / [А. Ф. Волобуєв, О. О. Волобуєва, О. А. Самойленко та ін.] ; за ред. А. Ф. Волобуєва. Київ : КНТ, 2011. 504 с. С. 327-329.

Узагальнення наукових поглядів щодо форм взаємодії слідчого із суб'єктами взаємодії дозволяє конкретизувати такі підстави їх класифікації:

1) нормативно-правова регламентація: а) процесуальні форми (передбачені КПК України): надання доручень співробітникам оперативних підрозділів щодо проведення С(Р)Д та НС(Р)Д (ч. 3 ст. 39, ч. 4 ст. 40, ч. 3 ст. 41 КПК України); залучення до участі в процесуальній дії співробітників оперативних підрозділів як спеціалістів чи інших учасників кримінального провадження, залучення інших спеціалістів, які мають спеціальні знання та навички (психологи, перекладачі), зокрема підчас огляду місця події, обшуку, одержання зразків для експертизи тощо (ст. ст. 40, 228, 236, 237 та інші); б) непроцесуальні (організаційно-тактичні) форми: створення слідчо-оперативних груп (тимчасових чи постійно діючих); забезпечення слідчим методичного супроводження ведення ОРС; залучення співробітників до забезпечення організаційних умов проведення охорони, конвоювання, затримання тощо; спільне планування слідчих (розшукових) та негласних слідчих (розшукових) дій, розслідування в цілому; взаємний обмін інформацією; узгоджених спільних дій та заходів кримінального провадження; обмін інформацією; залучення громадськості до участі у проведенні процесуальних дій та організаційних заходів);

2) рівень взаємодії: а) міжнародна взаємодія; б) міжвідомча взаємодія; в) внутрішньовідомча взаємодія (між різними підрозділами одного відомства);

2) стадія кримінально-процесуальної діяльності: а) взаємодія до початку кримінального провадження (в рамках ОРС та підчас попередньої перевірки інформації про злочин); взаємодія в ході здійснення досудового розслідування; б) взаємодія на стадії судового розгляду.

Взаємодія слідчого із оперативним підрозділом. Оперативний працівник, згідно зі ст. 7 Закону України «Про оперативно-розшукову діяльність», зобов'язується для своєчасного виявлення і припинення злочинів уживати необхідних оперативно-розшукових заходів, тим самим здійснювати оперативно-розшукову діяльність. Термін «оперативно-розшукова діяльність» означає, відповідно до дефініції, що містить тлумачний словник, що розшук здійснюють практично,

швидко, завчасно й таємно, і це може змінити перебіг справи[1]. Деякі процесуалісти акцентують на інформаційно-забезпечувальній функції оперативно-розшукової діяльності щодо кримінального процесу[2]. Утім форми та засоби оперативно-розшукової діяльності є чітко визначеними законом, що також засвідчує виключно правовий характер такої діяльності й самостійність відповідної галузі знань.

Сутність оперативно-розшукової діяльності науковці та практичні працівники тлумачать по-різному. Так, М. А. Погорецький дійшов висновку, що оперативно-розшукова діяльність є самостійною рівноправною державно-правовою функцією, яка виконує поряд з іншими завдання щодо протидії злочинності, спрямована на збирання даних, які можуть бути використані в кримінальній справі як докази за умов, передбачених КПК України[3].

Зміст оперативно-розшукової діяльності С. С. Овчинський розглядає у вузькому та широкому значеннях[4]. У вузькому значенні оперативно-розшукова діяльність – це вид соціально корисної юридичної державної діяльності уповноважених на те законодавством суб'єктів, що становить систему актів поведінки конспіративного й гласного застосування спеціальних сил, засобів і методів, а також здійснення оперативно-розшукових дій та прийняття оперативно значущих рішень, спрямованих на захист людини й суспільства від

---

[1] Новий тлумачний словник української мови : у 3 т. Т. 2. Київ : Аконіт, 2003. 928 с.

[2] Доброродній О. А. Оперативно-розшукове забезпечення розслідування вбивств на замовлення, вчинених з корисливих мотивів у сфері підприємництва : автореф. дис. … канд. юрид. наук : 12.00.09. Дніпропетровськ : ДДУВС, 2011. 20 с..; Горбачевський В. Я. Теоретико-прикладні засади розкриття умисних вбивств з кваліфікуючими ознаками : автореф. дис. … д-ра юрид. наук : 12.00.09. Київ, 2009. 34 с; Долженков С. О. Оперативно-розшукове забезпечення кримінального судочинства підрозділами боротьби з економічною злочинністю : автореф. дис. … канд. юрид. наук : 12.00.09. Львів : ЛьвДУВС, 2011. 20 с.; Рудік В. М. Оперативно-розшукове забезпечення кримінального судочинства у справах про корисливо-насильницькі злочини : дис. … канд. юрид. наук : 21.07.04. Дніпропетровськ, 2006. С. 187-189

[3] Погорецький М. А. Оперативно-розшукова діяльність: правове визначення поняття. *Право України.* 2001. № 11. С. 122.

[4] Овчинский С. С. Оперативно-розыскная информация. М. : Спарк, 2000. 220 с.

злочинних посягань, за наявності об'єктивних труднощів, за неможливості досягнення цієї мети шляхом реалізації інших законних засобів. У широкому значенні в дефініції оперативно-розшукової діяльності змінюється зміст одного з основних її суб'єктивних елементів – мети. Крім її широкої спрямованості (забезпечення безпеки людини, суспільства, держави), метою такої діяльності є захист конкретних суб'єктів, що охороняються законом, від злочинних посягань.

Аналізуючи подвійну сутність оперативно-розшукової діяльності, Г. В. Остафійчук доходить висновку, що функції кримінального процесу й оперативно-розшукової діяльності взаємопов'язані та взаємозалежні. Це цілком відповідає сучасній практиці розслідування окремих видів злочинів, адже кримінальне процесуальне доказування за окремими видами злочинів забезпечують методами та засобами саме оперативно-розшукової діяльності. Згідно з ч. 2 ст. 99 КПК України, матеріали, у яких зафіксовано фактичні дані про протиправні діяння окремих осіб і груп осіб, зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», можуть бути використані в кримінальному провадженні як докази. Однією з таких умов застосування оперативно-розшукової діяльності з метою доказування є неможливість використання під час отримання фактичних даних, які містять джерела доказів, гласних засобів. Тому питання діяльності працівників оперативних підрозділів у криміналістичній науці розглядають саме крізь призму їхньої взаємодії зі слідчими[1], яка по-суті пронизує весь процес діяльності останнього.

[1] Бекетов М. Ю. Следователь органов внутренних дел и милиция: взаимодействие при расследовании преступлений : учеб. пособие. М. : Щит-М, 2004. 96 с.; Иванов В. В. Методические рекомендации по совершенствованию взаимодействия следователя с оперативными подразделениями органов внутренних дел при раскрытии и расследовании преступлений. Чернигов, 1997. 34 с.; Озерський І. В. Взаємодія слідчого з органом дізнання (організаційно-правовий та психологічний аналіз) : монографія. Київ, 2004. 217 с.; Пивоваров В. В., Щербина Л. І. Взаємодія органів досудового слідства та дізнання при розслідуванні кримінальних справ : монографія. Харків : Право, 2006. 176 с.; Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с.

Злочини в кіберпросторі, особливо з огляду на специфічний і недостатньо вивчений механізм їх вчинення, становлять значну небезпеку для суспільства. Тому, відповідно п. 21 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України», окремим напрямом функціонування кібербезпеки визнано здійснення оперативно-розшукових, розвідувальних, контррозвідувальних та інших заходів, спрямованих на запобігання, виявлення, припинення й розкриття злочинів проти миру та безпеки людства, які вчиняються з використанням кіберпростору, розслідування, переслідування, оперативного реагування та протидія кіберзлочинності, розвідувально-підривній, терористичній та іншій діяльності в кіберпросторі, що завдає шкоди інтересам України, використанню мережі Інтернет у воєнних цілях. Виходячи зі змісту законів України «Про оперативно-розшукову діяльність»[1], «Про Національну поліцію»[2], «Про Службу безпеки України»[3], наказах НП України [4], до суб'єктів оперативно-розшукової діяльності, перед якими стоїть завдання щодо протидії злочинам, вчиненим у кіберпросторі, відносяться Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки СБ України (далі – ДКІБ) та Департамент кіберполіції НП України (далі – ДКП).

Підрозділи ДКІБ є суб'єктом здійснення оперативно-розшукової діяльності щодо більшості злочинів, вчинених у кіберпросторі з політичних мотивів. Ідеться про злочини, що зазвичай підслідні слідчим органів безпеки (передбачені ст. 109, 110, 110-2, 111, 112, 113, 114, 114-1, 258-258-5, 330, 436 КК України). Стратегією кібербезпеки України, затвердженої Указом Президента України від 15 березня

[1] Про оперативно-розшукову діяльність: Закон України від 18 лю. 1992 р. № 2135-XII URL: https://zakon.rada.gov.ua/laws/show/2135-12

[2] Про Національну поліцію України : Закон України від 2 лип. 2015 р. №580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19.

[3] Про Службу безпеки України : Закон України від 25 берез. 1992 р. №2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

[4] Про затвердження Положення про Департамент кіберполіції НП України : наказ Національної поліції України від 10 листоп. 2015 р. № 85. *Офіційний матеріал Департаменту Документального забезпечення Національної поліції України*.

2016 року за № 96/2016[1], на СБ України покладено широкий спектр завдань щодо протидії злочинам проти миру й безпеки людства, які вчиняються в кіберпросторі, кібертероризму та кібершпигунству, а також щодо перевірки готовності об'єктів критичної інфраструктури до можливих кібератак і кіберінцидентів щодо державних електронних інформаційних ресурсів та у сфері державної безпеки.

У цьому контексті варта уваги діяльність наявного в структурі ДКІБ Ситуаційного центру забезпечення кібербезпеки. Технічне обладнання та програмне забезпечення Центр отримав 2017 року в межах виконання першого етапу Угоди про реалізацію трастового фонду Україна-НАТО з питань кібербезпеки. За час функціонування Центру його спеціалісти зафіксували й заблокували понад 50 кібератак різного ступеня потужності, окремі з яких за руйнівними наслідками могли бути набагато гіршими, ніж вірус «Petya-A», який 27 червня 2017 року призвів до тимчасового блокування роботи обчислювальних систем об'єктів критичної інфраструктури. Начальник ДКІБ О. В. Климчук у своєму інтерв'ю повідомив ЗМІ про локалізацію Центром у квітні 2018 року кібератаки на об'єкти оборонно-промислового комплексу країни. Атаку було спрямовано на дискредитацію України на міжнародній арені та розповсюдження в інформаційному просторі недостовірної інформації щодо низки об'єктів критичної інфраструктури, зокрема ненадійності української сторони в співпраці в науковій та інженерній сферах[2]. Також у травні цього самого року СБ України за підтримки представників міжнародних ІТ-компаній вдалося попередити масштабну кібератаку з використанням шкідливого програмного забезпечення VPNFilter, яку мали здійснити на державні структури та приватні компанії з метою дестабілізації ситуації під час проведення в м. Києві фіналу Ліги чемпіонів Союзу європейських футбольних асоціацій. Причому, як зазначив О. В. Климчук, географічно кібератака була спрямована виключно на український сегмент Інтернету; зупинили її завдяки роботі ситуаційного центру забезпечення кібербезпеки СБ України

[1] Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96/2016. URL: http://zakon.rada.gov.ua/laws/ show/96/2016#n11.

[2] Климчук А. Информационная и кибербезопасность в современном мире: опыт СБУ. *Ліга :* [сайт]. URL: https://www.liga.net/politics/ opinion/informatsionnaya-i-kiberbezopasnost-v-sovremennom-mire-opyt-sbu.

Підрозділи ДКП, згідно з п. 2.1. Положення про ДКП НП України, уповноважені щодо протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку. Ця сфера діяльності іменується в Положенні «протидія кіберзлочинності». В Україні правові основи боротьби з кіберзлочинами визначаються передусім Конвенцією Ради Європи про кіберзлочинність. Тому оперативні підрозділи ДКП прямо зобов'язані здійснювати оперативно-розшукову діяльність властивими їм методами з метою протидії конвенційним злочинам (відповідальність за які фактично передбачена ст. 163, 176, 185, 190, 200, 301, 361–363-1 КК України). В структкруі ДКП є підрозділи, діяльність яких прямо спрямована на забезпечення здійснення досудового розслідування та виконання доручень слідчого, пов'язаних з отриманням цифрових (електронних) доказів. Такий напрям діяльності в наукових колах називають «комп'ютерна криміналістика» або «форензика»[1]. Саме вони як спеціалісти з комп'ютерних технологій забезпечують проведення С(Р)Д та інших заходів.

Слід зауважити, що НП України, відповідно до § 3 Стратегії кібербезпеки України, належить до Національної системи кібербезпеки як орган, що забезпечує захист прав і свобод людини та громадянина, інтересів суспільства й держави від злочинних посягань у кіберпросторі та здійснює заходи із запобігання, виявлення, припинення та розкриття таких злочинів. Протидія іншим, альтернативним Конвенції, злочинам, що вчиняються у кіберпросторі та підслідні слідчим НП України, завдання ДКП визначається як «сприяння в порядку, передбаченому чинним законодавством, іншим підрозділам НП України у попередженні, виявленні та припиненні кримінальних правопорушень»[2]. Ураховуючи те, що здійснення оперативно-розшукової діяльності щодо альтернативних Конвенції злочинів, належить до компетенції інших департаментів НП України (Департаменту карного розшуку,

[1] Федотов Н. Н. Форензика – компютерная криминалистика. М. : Юрид. мир, 2007. 360 с.

[2] Про затвердження Положення про Департамент кіберполіції НП України : наказ Національної поліції України від 10 листоп. 2015 р. № 85. *Офіційний матеріал Департаменту Документального забезпечення Національної поліції України*

Департаменту протидії наркозлочинності тощо), то оперативно-розшукова діяльність співробітників структурних підрозділів ДКП обмежується щодо них застосуванням відповідних своїй компетенції засобів і методів, спрямованих на своєчасне отримання інформації про злочини, що вчинені в кіберпросторі.

М. А. Погорецький та А. С. Кумичко наголошують на тому, що під час здійснення заходів оперативного пошуку оперативні працівники повинні докладати зусиль для отримання саме фактичних даних про кримінальні правопорушення, а не оперативну інформацію, що має ймовірний характер, оскільки лише фактичні дані можуть бути використані в кримінальному процесуальному доказуванні, набути статусу процесуального доказу в спосіб і форму, визначені кримінальним процесуальним законом для кожного з видів доказів[1]. Фактичні дані, отримані під час ОРД, повинні мати значення доказу в кримінальному провадженні. Водночас це дещо суперечить конфіденційному характеру окремих засобів оперативного пошуку. Саме цим пояснюється складність реалізації матеріалів первинної перевірки щодо невеликої та середньої тяжкості злочинів і відповідна проблема реалізації альтернативної форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі.

Тож, на мемент до початку кримінального провадження слідчі й оперативно-розшукові підрозділи також повинні функціонувати в спільному режимі, зокрема в межах перевірки оперативної інформації про злочин. Лише за таких обставин суб'єкт перевірки набуває якостей, не притаманних йому окремо[2]. Наприклад, якщо з огляду на сутність встановлюваної події можна дійти висновку про наявність багатьох джерел доказів – засобів комп'ютерної техніки (що містять сліди злочину), то оперативний працівник спільно зі слідчим визначатимуть, місцерозташування якого з пристроїв потрібно підтвердити документально під час перевірки інформації. Це потрібно для прискорення процесу збирання доказів слідчому, адже в момент початку провадження слідчий одразу буде мати підстави для обґрунтування

[1] Погорецьким М. А., Кумичко А. С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства*. 2015. № 4. С. 60.

[2] Хомколов В. П. Организация управления оперативно-розыскной деятельностью: системный поход. М. : Закон и право ; ЮНИТИ, 1999. С. 71–72.

клопотання до слідчого судді з метою забезпечення доступу до речей і документів, проведення обшуку чи комплексу НС(Р)Д.

В цьому сенсі також можна сформулювати такі рекомендації слідчому щодо оцінки матеріалів первинної перевірки про злочин, вчинений у кіберпросторі.

По-перше, недоцільно намагатися персоналізувати в матеріалах перевірки інформацію про користувача (можливого злочинця) з гласного джерела. Адже децентралізовані технології обміну й зберігання інформації, технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплекси програм), віртуальних приватних мереж (VPN-технологій) інших засобів-анонімайзерів) ускладнюють можливість підтвердження персональних даних користувача-злочинця – володільці інформаційних систем та інформації часто фізично перебувають за межами держави або ж нададуть таку інформацію лише на підставі ухвали слідчого судді.

По-друге, інформацію, викладену в рапорті інспектора ДКП, слідчий може оцінити як достовірну на момент внесення її до ЄРДР. Адже суб'єкт перевірки є особою, що має спеціальні знання у сфері інформаційних (комп'ютерних) технологій, а в слідчого й оперативного підрозділу, якщо говорити про нетяжкі/середньої тяжкості злочини, немає на цей час іншого засобу перевірки інформації, пов'язаного із застосуванням спеціальних знань. Щодо окремих видів кіберзлочинів підлягає перевірці лише її повнота, що здійснюється в межах оперативно-розшукових заходів із методичним супроводженням з боку слідчого (в рамках ОРС).

Взаємодія слідчого із іншими державними та недержавними підприємствами, установами та організаціями. Для деталізації суб'єктів взаємодії слідчого в цьому сенсі варто акцентувати увагу на особливостях організації національного сегменту кіберпростору[1].

[1] Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15; Про захист нформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 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; Про Національну комісію, що здійснює державне регулювання у сфері зв'язку та інформатизації : Указ Президента України від 23 листоп. 2011 р. № 1067/2011. URL: https://zakon.rada.gov.ua/laws/show/1067/2011

По-перше, в огляду на географічне розташування України, її телекомунікаційні мережі є точками транзиту трафіка щодо передачі даних Європи, Росії та Азії. Саме тому самостійну роль на ринку телекомунікаційних послуг в Україні виконують організації, що надають послуги з обміну трафіком (зазвичай використовують термін «піринг» (від англ. peering – сусідство) – угода про обмін трафіком). Їхня мережева інфраструктура призначена для оперативної організації з'єднань провайдерів, міжоператорського обміну Internet Protocol (IP-трафіком) між незалежними мережами в Інтернеті. Цей крок мав на меті знизити вартість послуг IP-транзиту для всіх типів Інтернет-провайдерів від локальних до магістральних мереж, для хостинг-провайдерів і CDN (*content distribution network*, що в перекладі означає «мережа доставки контенту»). Так звані точки обміну трафіком фактично забезпечують своєрідне об'єднання мереж в одній глобальній мережі через регіональні й закордонні точки доступу. На території України функціонують три структури, що надають послуги з обміну трафіком: 1) дочірнє підприємство «UA-IX», створене Інтернет-асоціацією України 2000 року; 2) комерційна структура ТОВ «Українські магістральні мережі» (Giganet.com); 3) корпорація Dtel-IX[1]. Натомість не в усіх європейських країнах є навіть одна така структура.

По-друге, у технічному аспекті магістральна мережа Інтернет огортає всю планету, поєднуючи континенти, країни й окремі міста. Інтернет, згідно зі ст. 1 Закону України «Про телекомунікації», є всесвітньою інформаційною системою загального доступу. Вона об'єднує між собою різні види мереж (магістральні, регіональні, локальні комп'ютерні мережі й окремі комп'ютерні системи)[2] на основі TCP/IP (Transmission Control Protocol/ Internet Protocol) протоколів, що визначені міжнародними стандартами міжнародних організацій. Магістральні мережі, що забезпечують трафік між регіонами України та за кордон обслуговують великі оператори та провайдери. Адже для передавання трафіка кожного абонента до точки обміну переважно використовують магістральні оптоволоконні мережі, будівництво й обслуговування яких потребує значних коштів. Великі оператори та

[1] Бізнес расследование «Угроза с востока». URL: http://project.liga.net/projects/eastern_threat.

[2] Воробієнко П. П., Нікітюк Л. А., Резніченко П. І. Телекомунікаційні та інформаційні мережі : підручник. Київ : Саммит-Книга, 2010. 708 с.

провайдери мають Інтернет-вузли й магістральні лінії в Україні та за її межами; регіональні оператори та провайдери охоплюють своєю мережею регіон, декілька або одну область. Причому більшість з них не мають своєї магістральної мережі; локальні оператори та провайдери – один або кілька населених пунктів.

По-третє, суб'єкт господарювання традиційно отримує право на здійснення діяльності у сфері телекомунікацій після включення Національною комісією, що здійснює державне регулювання у сфері зв'язку та інформатизації (далі – НКРЗІ), зі статусом «провайдер» або «оператор» до відповідного реєстру операторів, провайдерів телекомунікацій[1]. Статус «оператор», на відміну від «провайдер», дає право суб'єктові обслуговувати власні мережі на чітко визначеній території своєї діяльності (місто, район). За умови отримання в НКРЗІ ліцензії на надання послуг з технічного обслуговування та експлуатації телекомунікаційних мереж, мереж ефірного теле- і радіомовлення, провідного радіомовлення та телемереж оператор може здійснювати також обслуговування чужих мереж (інших операторів або провайдерів). Така ліцензована діяльність щодо обслуговування оператором буде обмежена визначеною в ліцензії територією (регіоном, містом) і часом дії (не менш як п'ять років).

Діяльність провайдера обмежується географічною територією дії конкретного оператора (фактичної діяльності як зареєстрованого суб'єкта або тієї, що передбачена ліцензією на обслуговування телекомунікацій). Причому немає жодних обмежень щодо співпраці оператора з іншим оператором. Так, один з операторів може мати ліцензії зв'язку (фіксованого чи рухомого), а інший, – не маючи ліцензії та сплачуючи єдиний податок, працювати через його мережі, навіть на іншій території[2]. Варто зауважити, що нині не всі провайдери зареєстровані в НКРЗІ, зустрічаються й так звані сірі провайдери, які під виглядом користувачів підключаються до великих інтернет-провайдерів і надають послуги на рівні провайдера іншим користувачам.

[1] Реєстр операторів, провайдерів телекомунікацій. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk.

[2] Регистрация оператором, провайдером в НКРЗІ. URL: https://ogp.ua/ru/razresheniya-na-deyatelnost/registratsiya-operatorom-provajderom.

Станом на 31 грудня 2017 року в НКРЗІ зареєстровано 3430 операторів телекомунікацій і 2581 провайдер телекомунікацій[1]. Великі оператори та провайдери можуть пропонувати своїм клієнтам комплексні рішення доступу до Інтернету, телефонного зв'язку, Інтернет-телефонії, передачі та зберігання даних на віддалених серверах в Україні та за її межами тощо. Рішеннями НКРЗІ в лютому 2018 року публічне акціонерне товариство «Укртелеком» було визнано оператором телекомунікацій з істотною ринковою перевагою на ринку послуг транзиту трафіка на мережах фіксованого й рухомого (мобільного) зв'язку. У масштабах ринку телекомунікаційних послуг варто також відмітити таких операторів як «Укртелеком», «Датагруп», «Київстар», «МТС-Україна», Lifecell. Їхні транспортні мережі охоплюють усі регіони України та мають міжнародні переходи. В інших країнах вони підключені до іноземних точок обміну трафіком, що забезпечує українцям обмін трафіком не тільки всередині країни, а й у всьому світі[2].

По-четверте, на ринку телекомунікаційних (інформаційних) послуг також присутні й володільці інформації в системах. Володілець інформації – це фізична або юридична особа, якій належать права на інформацію в інформаційній системі. У значенні інформації вона набуває форми інформаційного продукту або інформаційного ресурсу (сукупності продуктів, об'єднаних технологією зберігання або передачі даних). У підрозділі 2.2 праці ми зазначали, що таким ресурсом є веб-сайт та електронно-інформаційні системи різного призначення (платіжні системи, автоматизовані системи технологічного виробництва, інформаційно-пошукові, робочі автоматизовані місця тощо), розглядали природу права власності на інформаційний продукт/ресурс в інформаційній системі[3]. Так, Національний банк України веде відкритий Реєстр щодо платіжних

[1] Презентація звіту Про роботу Національної комісії що здійснює державне регулювання у сфері зв'язку та інформатизації за 2017 рік. URL: https://nkrzi.gov.ua/images/upload/142/7598/Presentation 2017.pdf.

[2] Бізнес расследование «Угроза с востока». URL: http://project.liga.net/projects/eastern_threat/.

[3] Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2018. Т. 29 (68). № 4. С. 165–169. (Серія «Юридичні науки»).

організацій, систем та операторів послуг платіжної інфраструктури в Україні[1]. У ст. 1 Закону України «Про платіжні системи та переказ коштів в Україні» платіжну організацію визначено як юридичну особу, що визначає правила роботи платіжної системи, а також виконує інші функції із забезпечення діяльності платіжної системи та несе відповідальність згідно із Законом і договором; оператор послуг платіжної інфраструктури – це клірингова установа, процесингова установа та інші особи, уповноважені надавати окремі види послуг у платіжній системі або здійснювати операційні, інформаційні й інші технологічні функції щодо переказу коштів[2]. Вони як власники інформації в системі володіють інформацією про її користувачів. Тож, оператор, провайдер, організації, що надають послуги з обміну трафіком або контент-сервісів, власник веб-сайту, 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, організації) є володільцями інформації.

Також слід звернути увагу на організації (представництва, українські офіси глобальних Інтернет-сервісів), що забезпечують CDN, тобто мережі доставки контенту українському користувачеві. Ідеться про мережу географічно розподілених серверів, за допомогою яких користувачу надають доступ до контенту сайту або програми залежно від його місця розташування. Корпорації, що надають Інтернет-послуги (наприклад, Google, Facebook, колись Mail.ru, Ok, або «Одноклассники»), зацікавлені в тому, щоб їхній трафік був близьким для клієнтів, тому відкривають представницькі структури й організовують трафік на території України.

Наведене дає можливість визначити наступних суб'єктів взаємодії слідчого в процесі розслідування злочинів, вчинених у кіберпросторі:

1) державні органи (мають контрольні й ліцензійні функції, можуть надати копії документів про діяльність підприємств, установ та організацій, виявлені порушення процесів, що контролюються

[1] Реєстр щодо платіжних організацій, систем та операторів послуг платіжної інфраструктури. URL: https://bank.gov.ua/control/uk/publish/article?art_id=8436153.

[2] Про платіжні системи та переказ коштів в Україні : Закон України від 5 квіт. 2001 р. № 2346-III. URL: https://zakon.rada.gov.ua/laws/show/2346-14.

державою): спеціально уповноважені державні органи у сфері телекомунікацій, зокрема орган виконавчої влади з питань організації спеціального зв'язку та захисту інформації (Державна служба спеціального зв'язку та захисту інформації України і підпорядковані їй регіональні органи – управління в областях); орган державного регулювання у сфері телекомунікацій, інформатизації, користування радіочастотним ресурсом, що здійснює також повноваження органу ліцензування, дозвільного органу, регуляторного органу й органу державного нагляду (контролю) (Національна комісія, що здійснює державне регулювання у сфері зв'язку та інформатизації); Національна рада України з питань телебачення і радіомовлення; Державне підприємство «Український державний центр радіочастот»; Національний банк України;

2) громадські об'єднання/організації (можуть надати офіційні аналітичні огляди; статистичні дані, поінформувати щодо виявлення факту вчинення злочинів), наприклад, Інтернет асоціація України; Всеукраїнська громадська організація «Всеукраїнське агентство з авторських та суміжних прав»; Державна організація «Українське агентство з авторських та суміжних прав»; Асоціація «Телекомунікаційна палата України» та інші;

3) суб'єкт господарювання (оператори та провайдери) у сфері зв'язку та телекомунікацій (можуть документально підтвердити реєстраційні й технічні відомості, що дозволяють ідентифікувати власника, розробника, адміністратора Інтернет-ресурсу, факт надання послуг зв'язку конкретному користувачу/відправнику/отримувачу, надання послуг хостингу; надати відомості про фінансово-господарську діяльність, технічні аспекти функціонування мережі тощо);

4) комерційні банківські установи, суб'єкти господарювання у сфері платіжних систем (можуть документально підтвердити рух (обіг) коштів на рахунках підприємств, установ та організацій, окремих громадян, поточні й депозитні рахунки; надати інформацію про штат співробітників, їхні характеристики тощо);

5) засоби масової інформації (можуть документально підтвердити факт реклами, оголошення, динаміку розвитку ринку товарів і послуг, проведення офіційних заходів (виступів, спортивних заходів, ярмарків та аукціонів); надати результати журналістських розслідувань);

6) міжнародні правоохоронні організації (можуть документально підтвердити місце розташування адміністратора та користувачів Інтернет-ресурсу, що використовується під час вчинення злочину на території України, причому фізично розміщується на серверах, розташованих поза її межами);

7) інші власники (розпорядники) систем та володільці інформації (структури, що надають послуги з обміну трафіком; представники контент-сервісів, власник веб-сайту, а також будь-який власник чи розпорядник електронно-інформаційної системи (державні й недержавні установи, платіжні організації та оператори послуг платіжної інфраструктури, будь-які підприємства, організації).

Таким чином, особливості організації протидії кіберзагрозам в Україні та організації національного сегменту кіберпростору зумовлюють суб'єктів взаємодії зі слідчим в процесі розслідування злочинів, вчинених у кіберпросторія. Взаємодія слідчого із оперативними підрозділами, власниками (розпорядниками) телекомунікаційних систем, володільцями інформації в системах та іншими суб'єктами на ринку телекомунікаційних послуг є невід'ємною складовою процесу виявлення та розслідування злочинів, вчинених у кіберпросторі.

РОЗДІЛ 4
ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

4.1. Періодизація розслідування й типові слідчі ситуації в криміналістичній методиці

Для структурування кожної окремої криміналістичної методики виключно важливе значення має періодизація розслідування, з огляду на динамічність його обстановки та ступінь вирішення його завдань. Термін «періодизація» означає дію, що полягає в поділі процесів на основні періоди, що якісно відрізняються один від одного. Словом «період» позначають проміжок часу, обмежений певними датами, подіями тощо[1].

Попри те, що процес діяльності слідчого з розслідування злочину чітко визначений часовими межами здійснення досудового розслідування як стадії кримінального провадження, науковці-криміналісти та практики уникають використання терміна «період» щодо періодизації процесу розслідування, віддаючи перевагу категорії «етап розслідування». Зазначене обумовлено складністю виокремлення чітких меж об'єкта, який досліджують як наукову абстракцію. Діяльність слідчого щодо здійснення розслідування поза специфікою конкретного виду злочину і є абстракцією. Поняття «етап» (від франц. etape – перехід, перегін) означає місце зупинки (етапний пункт), окремий момент, стадію процесу, тому науковцям зручніше обирати ключовий момент для розслідування задля стандартизації дій слідчого до настання його та після.

Розмаїття підходів до визначення критеріїв поділу розслідування на етапи та кількості останніх потребувало систематизації в криміналістичних дослідженнях наукових позицій. Чіткість встановлення етапів розслідування сприяє оптимізації діяльності слідчого з розслідування окремого виду злочину.

На підставі узагальнення поглядів учених-криміналістів станом на 2000 рік А. Ф. Волобуєв дійшов слушного висновку щодо наявності ситуаційного та процесуального підходів до періодизації

[1] Словник української мови : в 11 т. / [редкол.: І. К. Білодід (гол.) та ін.]. Київ : Ін-т мовознавства НАН УРСР, 1975. Т. 6 : П– Поїти. С. 325.

розслідування[1]. Відповідно до першого підходу (С. А. Голунський, Р. С. Бєлкін, В. В. Тіщенко та інші), розмежування етапів передбачає спрямованість слідчих та оперативно-розшукових дій початкового етапу розслідування на невідкладність виконання поставлених слідчим завдань. Невідкладними вважають ті слідчі дії, які потрібно здійснювати невідкладно у зв'язку із ситуацією, що склалася (зволікання призводить до втрати можливості отримати докази)[2]. Момент завершення проведення невідкладних слідчих дій розмежовував початковий і наступний етапи розслідування.

Другий підхід ґрунтується на процесуальному рішенні, що пов'язане з розкриттям злочину. Науковці А. Ф. Волобуєв, І. Ф. Герасимов, І. М. Лузгін, Є. Д. Лук'янчиков та інші вважали таким пред'явлення обвинувачення особі принаймні за одним епізодом злочину[3]. Із цього приводу А. Ф. Волобуєв зауважував, що етапом розслідування є певний проміжний пункт у процесі розслідування злочину, який характеризує стан слідства з позиції повноти виконання його завдань і визначається прийнятими процесуальними рішеннями в кримінальній справі[4]. Ураховуючи тільки дії, що спрямовані на збирання доказів (криміналістичний аспект), автор виокремив два етапи розслідування – початковий і наступний. Для їх розмежовування вчений використовував перелік завдань, притаманних для певного етапу, і ступінь їх виконання, мотивуючи це тим, що їх можна чітко визначити залежно від предмета доказування (обставин, що підлягають встановленню). Для початкового етапу розслідування окреслено такий перелік завдань:

1) встановлення місця, часу й інших обставин вчинення злочину, його суті, а також виявлення, фіксація та вилучення його

[1] Волобуєв А. Ф. Етапи розслідування в криміналістичній методиці. *Вісник Університету внутрішніх справ.* 1999. Вип. 5. С. 28–37.

[2] Криминалистика: техника и тактика расследования преступлений / под ред. А. Я. Вышинского. М. : Юрид. изд-во, 1938. 540 с.

[3] Лузгин И. М. Методологические проблемы расследования. М. : Юрид. лит., 1973. 216 с.; Герасимов И. Ф. Этапы раскрытия преступлений. *Следственные ситуации и раскрытие преступлений.* Свердловск, 1975. С. 10–16; Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : монографія. Київ : Нац. акад. внутр. справ України, 2005. С. 39.

[4] Волобуєв А. Ф. Етапи розслідування в криміналістичній методиці. *Вісник Університету внутрішніх справ.* 1999. № 5. С. 36.

слідів, які з часом під впливом несприятливих умов можуть зникнути або бути знищеними;

2) встановлення, розшук і затримання особи (або вибір запобіжного заходу), підозрюваної у вчиненні злочину;

3) збирання доказів, достатніх для пред'явлення обвинувачення особі принаймні за одним епізодом злочинної діяльності. Тому вчений обґрунтовував, що закінчення початкового етапу пов'язано зі встановленням особи, що вчинила злочин, і збиранням доказів, достатніх для пред'явлення їй обвинувачення принаймні за одним епізодом злочинної діяльності. Згодом майже аксіоматичного значення для дослідників окремих криміналістичних методик набула теза цього автора, відповідно до якої формування переліку типових слідчих ситуацій для кожного етапу розслідування надає чіткості структурі відповідної методики розслідування[1].

Деякі науковці додавали до перших двох етапів третій – завершальний, що пов'язаний із процесуальними діями, спрямованими на закінчення провадження у справі[2]; інші виокремлювали чотири етапи: 1) реагування на привід до порушення кримінальної справи, перевірка отриманої заяви або повідомлення про злочин і порушення кримінальної справи за наявності для того підстав; 2) здійснення початкових слідчих дій; 3) проведення подальшого розслідування; 4) завершення розслідування й складання обвинувального вироку[3]. П'ять етапів розслідування пропонував

[1] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 204.

[2] Образцов В. А. Выявление и изобличение преступника. М. : Юристъ, 1997. С. 17; Белкин Р. С. Курс криминалистики : в 3 т. М., 1997. Т. 3 : Криминалистические средства, приёмы и рекомендации. С. 331–335; Возгрин И. А., Вандышев В. В., Дербенев А. П. Криминалистическая методика расследования преступлений. Минск : Вышэйш. шк., 1983. С. 125.

[3] Танасевич В. Г. Проблемы раскрытия и расследования преступлений. *Советская криминалистика. Теоретические проблемы.* М., 1978. 245 с.; Строгович М. С. Уголовный процесс : учеб. пособие. М., 1938. С. 50–100; Шурухнов Н. Г. Криминалистика : учебник. 2-е изд., испр. и доп. М., 2008. 720 с.

виокремлювати Ю. П. Гармаєв, а саме: перевірочний, версійний, планування, реалізації плану та перевірки версій[1].

Після набрання чинності КПК України 2012 року інститут пред'явлення обвинувачення було скасовано, що ініціювало нові криміналістичні розробки з питань періодизації розслідування. У криміналістичній науці запропоновано нові системи поділу розслідування на етапи, які ґрунтуються на «змішаному» критерії – напрямі розслідування, що обумовлений обсягом виконання ситуаційних тактичних завдань розслідування злочинів і прийняттям відповідних процесуальних рішень[2].

При періодизації досудового розслідування В. А. Журавель вважає за доцільне визначати чотири етапи: 1) відкриття кримінального провадження (вихідний етап); 2) початок кримінального провадження (початковий етап); 3) продовження кримінального провадження (наступний етап); 4) завершення кримінального провадження (завершальний етап)[3]. Автор виокремлює дві ситуації початкового етапу – неперсоніфікований (початок провадження за фактом) і персоніфікований (початок провадження стосовно особи); метою початкового етапу розслідування вважає встановлення наявності або відсутності події кримінального правопорушення та відшукання достатніх доказів для оголошення підозри особі у вчиненні злочину (ст. 276 КПК України). Здійснення цієї процесуальної дії є підставою для розмежування початкового й наступного етапів. Наступний етап пов'язаний зі збиранням необхідних доказів для встановлення винуватості особи та завершенням досудового розслідування (ст. 283 КПК України). Як концептуальний підхід у криміналістиці таку періодизацію можна вважати цікавою.

Дослідниця О. В. Пчеліна спрощує чотирьохепізодну структуру розслідування й визначає три етапи в розслідуванні злочинів у сфері службової діяльності, а саме: збирання та перевірку первинної

[1] Гармаев Ю. П. Теоретические основы формирования криминалистических методик расследования преступлений : автореф. дис. … д-ра юрид. наук : 12.00.09. М., 2003. 39 с.

[2] Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. … дис. д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с.

[3] Журавель В. Проблеми періодизації досудового розслідування. *Вісник Національної академії правових наук України*. 2014. № 2 (77). С. 141.

інформації про зазначені правопорушення, початковий та наступний етапи[1].

На наше переконання, питання щодо кількості етапів розслідування та моментів їх розмежування досі залишаються невирішеними. Традиційний поділ розслідування на початковий і наступний етапи потребує поглибленого аналізу. Визначення чинників правового спрямування, що чинять суттєвий вплив з криміналістично значущих позицій на фактичну діяльність суб'єктів здійснення досудового розслідування, надасть можливість сформувати оптимальний погляд на сучасну структуру діяльності слідчого під час розслідування злочинів певного виду. Небезпідставно Б. В. Щур стверджує, що процес розслідування необхідно розглядати не в статиці, а в динаміці[2]. Тому він визнає обґрунтованою думку окремих науковців, які доводять важливість встановлення інформаційно-пізнавального аспекту конкретного етапу розслідування[3].

За своїм змістом діяльність з розслідування злочину є процесом пізнання, об'єктом якого виступає злочин. Його пізнання, як і будь-кого об'єкта здійснюють шляхом діяльності та через діяльність – практичну й теоретичну[4]. Перша складова реалізується за допомогою системи пізнавальних засобів: 1) чуттєвого спостереження; 2) повсякденної практики; 3) експерименту; 4) моделі; 5) математичного апарату; 6) методологічної основи[5]. На думку Р. С. Бєлкіна, В. І. Гончаренка, В. В. Тіщенка та інших криміналістів, у розслідуванні можна використовувати всі зазначені засоби, зокрема логіко-математичний

[1] Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. … дис. д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с.

[2] Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. 407 с.

[3] Криминалистика: расследование преступлений в сфере экономики : учебник / под ред. В. Д. Грабовского, А. Ф. Лубина. Н. Новгород : Нижегор. ВШ МВД России, 1995. С. 70.

[4] Аверьянов А. Н. Системное познание мира. М. : Политиздат, 1985. С. 213–214; Симонян Е. А. Единство теории и практики: философский анализ. М. : Наука, 1980. С. 105.

[5] Проблема связей и отношений в материалистической диалектике / отв. ред. В. С. Тюхтин. М. : Наука, 1990. С. 177.

апарат[1]. Реалізує ці пізнавальні засоби безпосередньо слідчий з моменту початку кримінального провадження, винятком є лише їх здійснення в межах огляду місця події. Оскільки його проведення до внесення інформації в ЄРДР є переважно винятком, а не правилом, а за окремими видами злочинів його взагалі не проводять (більшість злочинів, що вчинені в кіберпросторі), то моментом початку пізнавальної діяльності слідчого можна однозначно вважати внесення інформації про злочин до ЄРДР.

Друга складова реалізується через процес кримінально-процесуального доказування шляхом допустимого законом поєднання зазначених вище засобів, унаслідок якого процес збирання й дослідження доказів не відокремлений від оцінки отриманої інформації, а оцінка доказів лише забезпечує встановлення обставин події, що є об'єктом пізнання слідчого. Саме під час процесуального доказування посадові особи, що здійснюють пізнавальну діяльність у кримінальному процесі, перетворюють «факти в собі» на «факти для всіх»[2]. Оскільки слідчий є одним з основних суб'єктів доказування в кримінальному провадженні, а процес доказування також поєднує дві пов'язані складові – пізнавальну (розумову) та практичну (процесуальну), то пізнавальна діяльність слідчого підпорядкована законам логіки та нормам кримінального процесуального права. Чимало науковців саме це намагаються залишати поза межами криміналістичних досліджень, хоча обумовленість окремих методик розслідування положеннями галузевих юридичних наук, зокрема положеннями кримінального процесу, належить до принципів криміналістичної методики[3].

У контексті регулювання пізнавальної діяльності слідчого нормами процесуального права доцільно апелювати до кримінально-процесуальної форми загалом і правових форм діяльності органів

[1] Белкин Р. С. Курс криминалистики : учеб. пособие. 3-е изд., доп. М. : ЮНИТИ-ДАНА ; Закон и право, 2001. С. 232–236; Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. Киев : Вища шк., 1980. С. 75; Селиванов Н. А. Математические методы в собирании и исследовании доказательств. М. : Юрид. лит., 1974. 120 с.; Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. С. 91.

[2] Копнин П. В. Диалектика, логика, наука. М. : Наука, 1973. С. 166.

[3] Чурилов С. Н. Криминалистическая методика: история и современность. М. : Маркетинг, 2002. С. 282.

досудового слідства та прокурора зокрема. Вони можуть бути використані для інтерпретації сучасних меж початкового та наступного етапів розслідування злочину й обґрунтування сукупності умов, за яких діє слідчий.

Кримінально-процесуальна форма – це визначений законом порядок кримінального провадження, порядок виконання окремих процесуальних дій і прийняття процесуальних рішень[1]. Після набрання чинності КПК України 2012 року порядок кримінального провадження зазнав кардинальних змін, що було предметом дослідження процесуалістів[2] та безпосередньо позначилося й на прикладних розробках криміналістичної науки.

На підставі узагальнення наукових публікацій та ознайомлення з матеріалами судово-слідчої практики ми вважаємо, що є елементи кримінально-процесуальної форми, які суттєво впливають на організацію пізнавального процесу в стадії досудового розслідування, зокрема, до них належать:

1) обов'язковість реєстрації процесуальних рішень, прийнятих під час досудового розслідування, в ЄРДР;

2) ліквідація інституту оперативно-розшукового супроводження досудового розслідування (роботу оперативного підрозділу після внесення інформацій про злочин до ЄРДР ініціюють лише в межах, що визначені дорученням слідчого);

3) розгляд низки процесуальних питань слідчим суддею (призначення судової експертизи; тимчасовий доступ до речей і документів, обшук, НС(Р)Д, що пов'язані з втручанням у приватне спілкування, інші дії, пов'язані із проникненням до житла чи іншого володіння; за певних обставин з дотриманням змагальної процедури);

4) узгодження слідчим більшості своїх рішень у провадженні з прокурором (повідомлення про підозру; заходів забезпечення кримінального провадження, окремих слідчих (розшукових) дій);

---

[1] Лобойко Л. М. Кримінальний процес : підручник. Київ : Істина, 2014. 432 с.

[2] Власова Г. П. Співвідношення кримінальних процесуальних проваджень та диференціації кримінальних процесуальних форм. *Науково-інформаційний вісник*. 2015.№11. С. 153-157.

5) прийняття окремих важливих рішень виключно прокурором (наприклад, про об'єднання або виділення матеріалів досудового розслідування; здійснення контролю за вчиненням злочину);

6) можливість учасників процесу оскаржувати до слідчого судді більшість рішень, дій та бездіяльність слідчого і прокурора, зокрема щодо повідомлення про підозру після спливання терміну, визначеного законом;

7) суттєве розширення інструментарію діяльності слідчих завдяки НС(Р)Д та ОРЗ, що проводили із залученням слідчого до методичного супроводження оперативної розробки в межах ОРС; практики характеризують сучасний стан розслідування так: «ОРД увійшла до складу кримінальної процесуальної діяльності»[1];

8) наявність особливих (диференційованих) кримінально-процесуальних форм (за наявності визначеної законом специфіки проваджень, зокрема на підставі угод (глава 35 КПК України); у формі приватного обвинувачення (глава 36); щодо окремої категорії осіб (глава 37); щодо неповнолітніх (глава 38); щодо застосування примусових заходів медичного характеру (глава 39); яке містить державну таємницю (глава 40); на території об'єктів, що належать Україні, але перебувають за її межами (глава 41 КПК України).

Аналіз зазначених правових форм діяльності органів досудового слідства дає змогу визначити момент повідомлення особі про підозру як вирішальний для процесу розслідування. Саме це процесуальне рішення впливатиме на подальшу організацію слідчим пізнавального процесу в стадії досудового розслідування. Адже законна й обґрунтована підозра, висунута у встановленому порядку як процесуальний акт, закладає основу змагальної процедури кримінального судочинства. Із цього моменту суттєво розширюється коло суб'єктів доказування, до нього вже входять підозрюваний, його захисник і законний представник, які мають важелі впливу на процес розслідування.

Термін «обґрунтована підозра» має кримінально-процесуальний зміст, що висвітлено в практиці Європейського суду з прав людини як «існування фактів або інформації, які можуть переконати

[1] Шевчишен А. В. Легальні дефініції слідчих (розшукових) та негласних слідчих (розшукових) дій. *Формування правових позицій щодо розслідування міжнародних злочинів :* зб. наук. пр., матеріали конф. (семінарів, круглих столів). Київ : КНУВС, 2016. С. 262.

об'єктивного спостерігача в тому, що особа, про яку йдеться, могла вчинити це правопорушення» («Нечипорук, Йонкало проти України» № 42310/04 від 21 квітня 2011 року, «Фокс, Кемпбелл і Хартлі проти Сполученого Королівства» № 12244/86, 12245/86, 12383/86 від 30 серпня 1990 року, «Мюррей проти Сполученого Королівства» № 14310/88 від 28 жовтня 1994 року тощо)[1].

Криміналістично значуща складова обґрунтованої підозри пов'язана з комплексом завдань, які були виконані слідчим для переконання прокурора як об'єктивного спостерігача у встановленні таких обставин:

– факт вчинення кримінального правопорушення наявний у реальності (подія злочину);

– це правопорушення вчинене особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру;

– це суспільно небезпечне діяння містить склад конкретного кримінального правопорушення.

Момент започаткування змагальної процедури кримінального судочинства як основа поділу на криміналістичні етапи дозволить забезпечити чіткий поділ етапів розслідування, що, як обґрунтовано доводить А. Ф. Волобуєв, слід використовувати для розроблення окремих криміналістичних рекомендацій[2].

На нашу думку, першим етапом розслідування потрібно вважати традиційний *початковий етап*, що триває з моменту внесення інформації про злочин у ЄРДР до моменту висунення принаймні одній особі законної й обґрунтованої підозри у вчиненні кримінального правопорушення (одного або декількох). На початковому етапі обов'язковим для виконання є такий перелік завдань:

– встановлення відсутності/наявності події кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення);

– встановлення складу визначеного кримінального правопорушення (час, місце, спосіб, мета/мотив, повторність,

[1] PRECEDENTUA–2016 / [В. Лужковська, В. Щепотка, В. Капустинський та ін.]. Київ : КВІЦ, 2017. 326 с.

[2] Волобуєв А. Ф. Загальні положення криміналістичної методики : лекція. Харків : Ун-т внутр. справ, 1996. С. 29–30.

вчинення групою осіб/організованою групою, наслідки й інші обставини вчинення кримінального правопорушення);

– встановлення фактичних даних, які вказують на конкретну особу, що могла вчинити кримінальне правопорушення (форма вини, мотив і мета вчинення кримінального правопорушення особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру);

– забезпечення здійснення кримінального провадження.

Наступний етап розслідування доцільно залишити традиційним: триває він до закриття кримінального провадження або направлення до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності. З огляду на запровадження в Україні особливих (диференційованих) кримінально-процесуальних форм, вважаємо можливим виокремити такі основні завдання наступного етапу розслідування:

– встановлення злочинної діяльності в повному обсязі (усіх ознак складу/ів правопорушень);

– встановлення характеру й тяжкості обвинувачення щодо кожного суб'єкта злочину (зміни повідомлення про підозру особи/осіб);

– встановлення характеристик особи/осіб, яких обвинувачують, зокрема, ступеня та характеру сприяння підозрюваного/обвинуваченого в проведенні кримінального провадження щодо нього або інших осіб;

– встановлення інших обставин, які враховує прокурор під час вирішення питання про укладення угоди про визнання винуватості (суспільного інтересу в запобіганні, виявленні чи припиненні більшої кількості кримінальних правопорушень або інших більш тяжких кримінальних правопорушень, у забезпеченні швидшого досудового розслідування, викритті більшої кількості кримінальних правопорушень).

Втім, варто підкреслити *особливе значення початкового етапу розслідування злочину в методиках розслідування окремих видів злочинів*. Існуюча в практиці слідчої діяльності проблематика оцінювання прокурором правильності кваліфікації дій підозрюваної особи та достатності доказів для складання обґрунтованого повідомлення про підозру призводить до суттєвого навантаження початкового етапу розслідування.

З одного боку, під час встановлення складу конкретного кримінального правопорушення, що вчинене в дійсності, й особи, яка

його вчинила, прокурор повинен погодити повідомлення про підозру. З іншого боку, повідомлення особі підозри створює фактичні перепони для реалізації в межах кримінального провадження негласних методів роботи (у формі провадження НС(Р)Д), що заважає встановленню всіх обставин, які належать до предмета доказування (ст. 91 КПК України). Наслідком окресленої проблеми стає складання повідомлення про підозру особи максимально наближене в часі до моменту завершення досудового розслідування. В умовах багатоепізодного кримінального провадження така практика позначається на розширенні переліку основних завдань початкового етапу розслідування за рахунок завдань наступного етапу.

Аналіз матеріалів слідчої практики свідчить, що слідчий і прокурор на початковому етапі типово реалізують обумовлений ситуацією розслідування комплекс заходів забезпечення кримінального провадження та комплекс НС(Р)Д. Проведенням останніх на початковому етапі розслідування розв'язуються такі завдання наступного етапу як:

– встановлення злочинної діяльності в повному обсязі;

– встановлення характеру й тяжкості обвинувачення щодо кожного суб'єкта злочину (зміни повідомлення про підозру особи/осіб).

Саме тому ми повинні акцентувати увагу на початковому етапі розслідування злочинів, вчинених у кіберпросторі. Це дасть змогу відобразити динаміку розслідування злочинів різної складності, типізувати слідчі ситуації конкретної групи/підгрупи таких злочинів, сформулювати тактичні завдання розслідування й деталізувати комплекс засобів з їх розв'язання, тим самим створити з прагматичних міркувань теоретичну базу для розслідування злочинів зазначеної категорії.

Теоретичні питання слідчих ситуацій порушує кожний дослідник, сфера наукових інтересів якого стосується методики розслідування, адже озброєння слідчого знаннями про те, які ситуації можуть скластися під час розслідування злочинів окремого виду і як необхідно в них діяти, щоб досягти успіху, є одним з головних завдань методики розслідування злочинів.

Вагомий внесок в обґрунтування позицій щодо змісту слідчих ситуацій, їх класифікації зробили Р. С. Бєлкін, О. М. Васильєв, С. В. Веліканов, А. Ф. Волобуєв, Т. С. Волчецька, В. К. Гавло, І. Ф. Герасимов, В. Г. Гончаренко, Н. Л. Гранат, Г. Л. Грановський,

Г. А. Густов, Л. Я. Драпкін, А. В. Дулов, В. А. Журавель, А. В. Іщенко, О. Н. Колесніченко, В. О. Коновалова, В. О. Образцов, В. Г. Танасевич, В. В. Тіщенко, В. Ю. Шепітько, М. П. Яблоков та ін.

У межах процесу розслідування злочину слідча ситуація традиційно зводиться до сукупності відомостей про злочин та умови його розслідування на певному етапі цього процесу[1]. Науковці В. О. Коновалова, О. Н. Колесніченко слідчу ситуацію визначають як характеристику стану розслідування злочину, що обумовлена наявністю (відсутністю) доказової та оперативної інформації про обставини предмета доказування та компоненти криміналістичної характеристики, які обумовлюють систему безпосередніх завдань та напрямків розслідування[2]. Згодом В. О. Коновалова конкретизує розуміння слідчої ситуації до змісту «процесуального і непроцесуального характеру наявної інформації про злочин»[3]. Хоча таку думку було висловлено майже двадцять років тому, проте вчена фактично спрогнозувала сучасний зміст слідчої ситуації розслідування, адже наявність інформації, що має доказове значення, є нині нормою як для наступного етапу розслідування так й для початкового, тобто на момент відкриття кримінального провадження. Зазначене стало можливим через прогресивний погляд законодавця щодо використання в кримінальному провадженні як доказів матеріалів, що були зібрані оперативними підрозділами з дотриманням вимог Закону України «Про оперативно-розшукову діяльність», за умови відповідності вимогам КПК України. Інформація доказового значення (або процесуальна) дає підстави визначити ступінь повноти відомостей про злочин, що мінімізує

[1] Волобуєв А. Ф. Загальні положення криміналістичної методики : лекція. Харків : Ун-т внутр. справ, 1996. С. 29–30; Гавло В. К. О следственной ситуации и методике расследования хищений, совершаемых с участием должностных лиц. *Вопросы криминалистической методологии, тактики и методики расследования*. М., 1973. С. 90–94; Филиппов А. Г. К вопросу об особенностях расследования отдельных видов и групп преступлений. *Особенности расследования отдельных видов и групп преступлений*. Свердловск, 1980. С. 23–27; Шевчук В. М. Тактичні операції у криміналістиці: теоретичні засади формування та практика реалізації : монографія. Харків : Апостиль, 2013. 440 с.

[2] Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. ин-т, 1985. С. 64.

[3] Коновалова В. Е. Версия: концепция и функции в судопроизводстве : монография. Харьков : Консум, 2000. С. 50.

тактичні ризики слідчого при обранні конкретних засобів пізнання події злочину.

Традиційним в криміналістиці можна визнати поділ слідчих ситуацій на типові та конкретні. Якщо останні є відображенням стану досудового розслідування конкретного кримінального провадження, то типові ситуації є результатом наукового узагальнення слідчої практики [1].

Типова слідча ситуація – це наукова абстракція, утворена на підставі апріорних знань, є результатом узагальнення й аналізу емпіричного матеріалу, у ній відображено найбільш загальні риси, що характеризують перебіг і стан розслідування на певному етапі (вихідному, початковому, наступному)[2]. Високий ступінь наукової абстракції зумовлює її вагоме теоретичне та методичне значення для розроблення низки питань методики розслідування окремих видів злочинів, зокрема:

1) дає можливість виокремити і звести воєдино обставини, оцінка яких є необхідною для прийняття слідчих рішень за кримінальним провадженням[3];

2) дозволяє забезпечити повноту розслідування на кожному з криміналістичних етапів – доказування події злочину, винуватості конкретної особи у вчиненні кримінального правопорушення (форми вини, мотивів і мети вчинення кримінального правопорушення) й інших обставин, коло яких має релевантне значення залежно від ознак певного складу кримінального правопорушення;

3) характеризує процес формування стратегічних і тактичних завдань розслідування й визначення оптимальної послідовності проведення слідчих дій або тактичних операцій, що спрямовані на виконання цих завдань[4].

Ми поділяємо думку більшості вчених, які вважають, що саме слідчі ситуації зумовлюють тактичні завдання розслідування.

---

[1] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. 328 с.

[2] Белкин Р. С. Криминалистическая энциклопедия. М. : Мегатрон XXI, 2000. С. 106.

[3] Одерій О. В. Теорія і практика розслідування злочинів проти довкілля : монографія. Харків, 2015. С. 278.

[4] Журавель В. А. Криміналістичні методики: сучасні наукові концепції : монографія. Харків : Апостиль, 2012. 304 с.

А. Ф. Волобуєв пише про тактичні завдання як окреме завдання на шляху вирішення загального (стратегічного) завдання кримінального судочинства, пов'язаного із застосуванням криміналістичних засобів і прийомів[1].

В результаті аналізу підходів науковців до визначення поняття «тактичне завдання» В. А. Журавель обґрунтовано приходить до висновку про поділ завдань досудового розслідування за обсягом вирішуваних завдань на основні (загальні, стрижневі) й локальні (проміжні), а за сферою реалізації – на стратегічні й тактичні[2]. Основні завдання, як зазначає автор, за своєю сутністю є стратегічними, такими, що випливають із обставин, котрі підлягають з'ясуванню в цілому в ході розслідування окремого різновиду злочинів. Вони спрямовані на досягнення правової мети, за своєю природою є більш усталеними та меншою мірою піддаються впливу ситуаційних чинників. Локальні завдання є тактичними, такими, що мають чітко визначену ситуаційну зумовленість[3]. Криміналіст резюмує, що тактичне завдання – це ситуаційно зумовлене складне питання (проблема), що виникає на певний момент розслідування, яке має обмежену, локальну сферу реалізації, має проміжний характер, призначене для встановлення одиничних фактів про окремі елементи або обставини події злочину через застосування виключно тактичних засобів вирішення[4]. Тож, по суті, визначення тактичних (локальних чи проміжних) завдань розслідування, є важливим у тандемі з типовою слідчої ситуацією початкового чи наступного етапів розслідування. Це відіграватиме ключову роль для планування розслідування, дозволить слідчому конкретизувати необхідний комплекс слідчих дій, оперативно-розшукових та інших заходів, спрямований на розв'язання основних завдань розслідування в межах кожного з його етапів.

[1] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : автореф. дис. … д-ра юрид. наук : 12.00.09. Харків, 2002. С. 18

[2] Журавель В. А. Тактичні завдання розслідування та механізм їх вирішення. *Теорія та практика судової експертизи і криміналістики.* 2017. Вип. 17. С. 11–18.

[3] Там само. С. 12.

[4] Там само. С. 16.

Визначені в цьому підрозділі положення ми використовуємо як передумову подальшого дослідження початкового етапу розслідування злочинів, вчинених у кіберпросторі.

4.2. Типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі, відповідні їм тактичні завдання та засоби їх розв'язання

У криміналістичній науці типові слідчі ситуації початкового етапу розслідування злочинів, вчинених у кіберпросторі, висвітлено не комплексно, у контексті злочинів у сфері новітніх технологій або транснаціональних злочинів.

Першу спробу типізувати слідчі ситуації початкового етапу розслідування злочинів, що вчинені з використанням комп'ютерної техніки, здійснив В. Б. Вєхов[1]. Спираючись на положення про причини виникнення суспільно небезпечних діянь, спосіб вчинення комп'ютерного злочину, дослідник визначив такі три слідчі ситуації:

1) коли немає інформації про причини виникнення суспільно небезпечного діяння, способи вчинення й особу правопорушника;

2) коли є відомості про причини виникнення злочину, способи його вчинення за браку даних про особу злочинця;

3) коли є інформація про виникнення злочину, спосіб його вчинення та приховування, особу злочинця й інші обставини.

Ці ситуації є максимально узагальненими, що пов'язані з недостатністю на той час слідчої практики щодо розслідування таких злочинів. Саме тому автор не намагається розробити комплекс тактичних завдань і засобів їх виконання відповідно до конкретної ситуації, лише пропонує перелік первинних слідчих дій та організаційних заходів[2].

Звужений підхід до типізації слідчих ситуацій початкового етапу розслідування транснаціональних комп'ютерних злочинів

[1] Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М. : Право и Закон, 1996. С. 28.

[2] Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. С. Смагоринского. Волгоград : ВА МВД России, 2004. С. 172.

відображений у дисертації Л. В. Борисової[1]. За результатами аналізу типових (найпоширеніших) обставин вчинення злочину авторка визначає ситуації одного з видів комп'ютерного злочину на початковому та наступному етапах розслідування, зокрема:

1) встановлено час несанкціонованого доступу до комп'ютерної інформації, однак немає відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

2) встановлені час і місце несанкціонованого доступу до комп'ютерної інформації, проте особи, які володіють необхідними професійними знаннями, заперечують свою причетність до злочину;

3) встановлено час несанкціонованого доступу до комп'ютерної інформації, відома особа (особи), яка зацікавлена в цій інформації; бракує відомостей про спосіб доступу й особу (осіб), яка вчинила злочинні діяння;

4) встановлено час несанкціонованого доступу до комп'ютерної інформації; є сліди, що вказують на конкретного підозрюваного, але він заперечує свою причетність до вчиненого злочину;

5) визначено місце злочинного заволодіння комп'ютерною інформацією, для здійснення якого використовували механічний вплив; немає відомостей про особу (осіб), яка вчинила це діяння.

Дослідники М. Г. Шурухнов, Ю. В. Гаврилів визначають типові слідчі ситуації початкового етапу розслідування комп'ютерного злочину на підставі врахування характеру первинного матеріалу[2], зокрема характеризують такі ситуації:

– кримінальну справу порушено за матеріалами перевірок за наявності ознак злочину у сфері інформаційної безпеки;

– кримінальну справу порушено за заявою чи скаргою фізичної чи юридичної особи;

– кримінальну справу порушено за матеріалами друку, інших засобів масової інформації, матеріалами публічних виступів;

[1] Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. С. 70.

[2] Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации : учеб. пособие / под ред. Н. Г. Шурухнова. М. : ЮИ МВД РФ ; Кн. мир, 2001. С. 53.

– кримінальну справу порушено за фактом наслідків технологічного характеру з матеріальними збитками або людськими жертвами;

– кримінальну справу порушено щодо особи (осіб), яка затримана під час вчинення дій з ознаками інформаційних злочинів.

Колектив авторів науково-дослідного центру з проблем боротьби з організованою злочинністю залежно від джерела та змісту повідомлення про злочини у сфері використання комп'ютерної техніки зауважує про наявність інших п'яти ситуацій, зокрема:

1) неправомірний доступ виявлений під час реалізації комп'ютерної інформації незаконним користувачем (наприклад, під час поширення відомостей, що мають конфіденційний характер);

2) неправомірний доступ до комп'ютерної інформації виявлений законним користувачем за записами, які автоматично ведуться в комп'ютері (журнал контролю доступу), але особу, яка вчинила це, не встановлено;

3) неправомірний доступ виявлений законним користувачем із фіксацією на комп'ютері даних про особу, яка здійснює «перекачування» інформації через мережу;

4) неправомірний доступ виявлений оператором, програмістом унаслідок того, що злочинця захоплено на місці злочину;

5) є інформація про те, що здійснено неправомірний доступ до комп'ютерної інформації («зламано» паролі компанії, правопорушники незаконно користуються послугами, наприклад, зв'язку, наданими цією компанією). Останню ситуацію автори вважають найскладнішою, адже вона вимагає проведення оперативно-розшукових заходів[1].

У більшості праць із цієї тематики, які опубліковано до 2005 року, під час типізації слідчих ситуацій автори залишали поза увагою особу злочинця. Вони акцентувались на несанкціонованому доступі до предмета посягання, оскільки потерпілій стороні простіше заявити про несанкціонований доступ, ніж визнати свою неспроможність забезпечити максимально захищений санкціонований доступ, обрати висококваліфікований, без кримінальних схильностей

[1] Особливості виявлення та розслідування злочинів у сфері використання комп'ютерних технологій : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за ред. І. Є. Лазарєва, Б. В. Романюка. Київ, 2001. С. 11.

персонал мережі. В цьому контексті дослідник М. В. Богомолов зазначає, що спеціалізовані інформаційні системи дедалі частіше намагаються ізолювати у мережі Інтернет, тому приховати вчинення злочину внутрішнім користувачем стало значно складніше[1]. За таких умов під час висвітлення питань типізації слідчих ситуацій початкового етапу розслідування досліджуваної категорії злочинів факт або можливість персоналізації відомостей про користувача-злочинця сьогодні не можна ігнорувати. Розширення спектру злочинів, вчинених у кіберпросторі, також зумовило потребу продовження наукового пошуку оптимального підходу до типізації слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі.

Особливості криміналістичної характеристики злочинів, що вчиняють у кіберпросторі, дають підстави вважати такий злочин комплексом/системою поступових злочинних дій, що об'єднані одним мотивом та призводять до настання єдиного злочинного результату. Складність злочинної діяльності в кіберпросторі зумовлює особливу значущість у системі інформації про такий злочин кінцевого мотиву діяльності особи. Д. А. Іллюшин був одним із перших, хто окреслив у такий спосіб слідчі ситуації початкового етапу розслідування злочинів, вчинених у сфері надання послуг Інтернет. Він визначив комплекс інформації про мотив та особу злочинця, спосіб вчинення злочину як підставу виділення трьох слідчих ситуацій:

1) повна інформаційна невизначеність через брак інформації про мотиви, спосіб вчинення злочину й особу злочинця;

2) часткова інформаційна невизначеність (є відомості щодо мотиву, способу вчинення злочину, але немає даних про особу злочинця);

3) інформаційно визначена ситуація (є відомості про мотиви злочину, способи його вчинення та приховання, особу злочинця й інші обставини)[2].

---

[1] Богомолов М. В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации : дис. … канд. юрид. наук : 12.00.08. Красноярск, 2002. С. 15. URL: https://legalns.com/download/books/lib/criminalistics/book-001.pdf.

[2] Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет : дис. … канд. юрид. наук : 12.00.09. Волгоград, 2008. С. 15.

Обираючи тим самим для типізації слідчих ситуацій початкового етапу розслідування такий критерій, як інформаційна визначеність, автор, по суті, описує повноту вихідної інформації про злочин. Аналогічно й інші науковці, посилаючись на інформаційну визначеність як критерій типізації слідчих ситуацій початкового етапу розслідування, аналізують ситуації з різним набором інформації про злочин, зокрема: зміст джерела інформації про злочин[1], очевидні та неочевидні вихідні умови вчинення злочину[2], специфіку зв'язків між елементами криміналістичної характеристики окремого виду кіберзлочинів[3] тощо.

Як було доведено у третьому розділі роботи можливість персоналізувати особу конкретного користувача як злочинця-користувача дозволяє визначеність у матеріалах, що передані слідчому в рамках процесу початку кримінального провадження, відомостей про користувача веб-сторінки соціальної мережі, дошці оголошень чи іншій технології, що використовується у механізмі вчинення злочину, дані абонентського номеру користувача, його IP-адреси, MAC-адреси обладнання, що використовувалась при вчиненні або готуванні злочину в кіберпросторі. Тож, в момент відкриття кримінального провадження ступінь повноти вихідної інформації про готування або вчинення злочину визначається перш за все характером інформації про злочинця, зокрема, що визначається:

1) наявністю персоналізованих відомостей (розгорнуті анкетні дані особи імовірного злочинця);

2) наявністю неперсоналізованих відомостей (IP-адреси, MAC-адреси, сторінка у соціальній мережі тощо);

3) відсутністю персоналізованих та неперсоналізованих відомостей (через використання злочинцем технологій анонімізації доступу до ресурсів Інтернет, індивідуальної географічної мобільності).

---

[1] Пазиніч В. І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. С. 120.

[2] Анапольська А. І. Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2008. С. 79.

[3] Паляничко Д. Г. Методика розслідування злочинів, пов'язаних із дитячою порнографією : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2013. С. 95.

Ступінь повноти (обсяг) та достовірність іншої інформації про злочин, зокрема, спосіб підготовки та вчинення злочину, настання злочинних наслідків, особа потерпілого знаходиться у прямій залежності від форми початку кримінального провадження, яка відображає специфіку відкриття кримінального провадження щодо класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі.

Таким чином, типізувати слідчу ситуацію на початковому етапі розслідування злочинів, вчинених у кіберпросторі, дають змогу два взаємопов'язані чинники: 1) характер інформації про особу злочинця; 2) форма початку кримінального провадження. Останній, відображаючи повноту іншої інформації, специфіка якої зумовлена класифікаційною групою/підгрупою злочинів, вчинених у кіберпросторі, буде використаний нами з метою визначення особливостей типових слідчих ситуацій груп/підгруп досліджуваних злочинів.

За результатами узагальнення матеріалів слідчо-судової практики розслідування злочинів, вчинених у кіберпросторі, можна виокремити три групи типових слідчих ситуацій початкового етапу розслідування:

1) ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця;

2) ситуації, що характеризуються наявністю неперсоналізованих відомостей про користувача як імовірного злочинця;

3) ситуації, що характеризуються відсутністю будь-яких відомостей про особу злочинця.

Відобразити особливості типових слідчих ситуацій класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі, дозволить характеристика в межах кожної з вказаних груп типових слідчих ситуацій їх різновидів, зокрема, коли:

1) кримінальне провадження розпочато в результаті отримання заяви потерпілого/повідомлення особи про кримінальне правопорушення;

2) кримінальне провадження розпочато в результаті ознайомлення з матеріалами оперативного підрозділу щодо перевірки оперативної інформації;

3) кримінальне провадження розпочато в рамках реалізації матеріалів ОРС.

Охарактеризуймо типові слідчі ситуації у комплексі з тактичними завданнями та засобами їх розв'язання.

1. Ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця.

Ситуація 1.1. *Кримінальне провадження розпочато в результаті отримання заяви/повідомлення особи про кримінальне правопорушення, матеріали містять персоналізовані відомості про особу злочинця.* Ця ситуація типова при розслідуванні злочинів, вчинених внутрішнім користувачем мережі, що спрямовані на заволодіння чужим майном, у сфері функціонування електронних розрахунків, і таких, що порушують механізми захисту від монополізму та недобросовісної конкуренції. Потерпіла сторона, як правило, є юридичною особою. Матеріали внутрішньої перевірки (аудит, технічна перевірка, моніторинг мереж тощо) містяться в первинних матеріалах, що значно спрощує планування початкового етапу розслідування.

Прикладом є кримінальне провадження щодо гр. А., який, обіймаючи посаду головного спеціаліста сектору оформлення й обліку банківських операцій відділення № 8 ПАТ «Всеукраїнський акціонерний банк» у м. Р., у період з 26 квітня 2012 року до 4 липня 2014 року, маючи умисел викрасти чуже майно, діючи з корисливих мотивів, за попередньою змовою з начальником відділення № 8 ПАТ «Всеукраїнський акціонерний банк» гр. Б. шляхом вільного доступу, скориставшись послугою інтернет-банкінгу, таємно викрали грошові кошти з розрахункових банківських рахунків клієнтів банку. Дії злочинців було виявлено службою безпеки банку. Орган досудового слідства кваліфікував дії обвинувачених за ч. 2 ст. 185, ч. 2 ст. 200, ч. 3 ст. 362 КК України[1].

Суть злочину зводилася до того, що А., будучи, відповідно до посадової інструкції, особою, яка володіє інформацією клієнтів, діючи з корисливих мотивів, за попередньою змовою з начальником відділення № 8 ПАТ Б. з метою заволодіння коштами клієнта підробили документи на переказ грошових коштів в електронному вигляді, за допомогою яких здійснили незаконний переказ грошових коштів.

На початковому етапі розслідування основними тактичними завданнями в цій ситуації були:

[1] Вирок Рівненського міського суду Рівненської області від 15 лип. 2015 р. Справа № 569/10370/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/49017035.

– забезпечення збереження документів, у яких фіксують роботу комп'ютерної мережі банку й осіб, що її обслуговують;

– встановлення обставин проходження фіктивного електронного переведення коштів;

– встановлення режиму роботи комп'ютерної системи банку для здійснення незаконних дій у мережі;

– встановлення кола осіб, що мали змогу здійснити зазначений електронний переказ (у конкретний час і дату мали доступ до комп'ютерної системи, паролі для входу у внутрішню мережу банку);

– встановлення фактів приховування злочину (внесення змін в електронну базу даних банку, особистого впливу на свідків);

– встановлення зв'язків Б. з представниками інших комерційних структур і даних про його особу (попереднє місце роботи, коло знайомих та інтересів, наявність судимостей тощо);

– забезпечення відшкодування матеріальних збитків;

– встановлення злочинних зв'язків між А. та Б.;

– встановлення зв'язку А. та Б. з представниками компаній-жертв;

– встановлення того, як і ким були використані викрадені кошти;

– виявлення ознак вчинення несанкціонованої зміни інформації, яку опрацьовують в автоматизованих системах і зберігають на носіях такої інформації, вчинені особою, яка має право доступу до неї, за попередньою змовою групою осіб.

Окреслені тактичні завдання виконують шляхом проведення комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого:

1) допит службовців і посадових осіб відділення ПАТ «Всеукраїнський акціонерний банк», які проводили перевірку та виявили ознаки злочину;

2) тимчасовий доступ до речей і документів (інформація в електронній системі банку; нормативні акти та документи, що регламентують операційну роботу банку, бухгалтерський облік, внутрішньобанківський контроль; функціональні обов'язки працівників; журнали й інші документи, у яких фіксують роботу оператора операційного дня банку, журнали перевірки технічного стану системи банку тощо);

3) слідчий огляд вилученого;

4) призначення ревізії діяльності ПАТ «Всеукраїнський акціонерний банк»;

5) допит інших осіб як свідків злочину (керівництва та рядових працівників ПАТ «Всеукраїнський акціонерний банк»), які можуть пояснити обставини вчинення фіктивного електронного платежу;

6) затримання та обшук за місцем мешкання А. та Б. з метою встановлення наявності злочинних зв'язків з представниками інших комерційних структур, виявлення цінностей, одержаних злочинним шляхом;

7) опитування А. та Б. про обставини вчинення злочину;

8) слідчий огляд вилученого під час обшуку (грошові кошти, документи на переказ, чорнові записи, банківські платіжні картки, ноутбук);

9) призначення комп'ютерно-технічної експертизи;

10) накладення арешту на майно і вклади А. та Б.;

11) доручення оперативному підрозділу в порядку ст. 40 КПК України з метою встановлення майнового становища А. та Б., злочинних зв'язків А. та Б. з іншими посадовими особами банку;

12) оголошення підозри А. та Б., допит їх як підозрюваних.

Цій ситуації не завжди властива висока кваліфікація безпосереднього злочинця. Злочинець – користувач-професіонал може діяти на замовлення іншої особи, яка, будучи організатором, не є користувачем, але безпосередньо пов'язана з юридичною особою – жертвою. Так, гр. Н., надаючи послуги з перекладу тексту та доставлення подарунків, квітів, привітань, солодощів, парфумів тощо, на підставі робочого договору, укладеного з компанією «Dating.com Group Limited», у період часу з грудня 2012-го до вересня 2016 року, будучи обізнаною про діяльність автоматизованих систем цієї компанії, її баз даних, зокрема інтернет-сайтів компанії, з метою заволодіння грошовими коштами компанії «Dating.com Group Limited», перебуваючи в м. Черкасах, залучила через Інтернет-мережу гр. В. (оголошений у розшук в іншому кримінальному провадженні), який має спеціальні комп'ютерні навички, для проведення DDoS-атак на сайти цієї компанії[1]. Діючи за попередньою змовою групою осіб з корисливих мотивів, В. через мережу Інтернет здійснив DDoS-атаки на сайт anastasiadate.com, що належить зазначеній компанії, це

[1] Вирок Придніпровського районного суду м. Черкаси від 29 січ. 2018 р. Справа № 711/9946/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/71848933.

призвело до повного зупинення атакованого сервера внаслідок надіслання на нього надмірної кількості неправдивих запитів. На електронну скриньку компанії надсилали повідомлення щодо унеможливлення здійснення підприємницької діяльності цією компанією, допоки представники компанії не виконають їхні протиправні майнові вимоги. Після декількох атак і погроз через платіжні системи «QIWI» та «Яндекс Деньги» у формі біткоїну гр. В. було перераховано 940 422 грн, унаслідок чого компанії «Dating.com Group Limited» завдано майнової шкоди в особливо великих розмірах.

Порівняно з попереднім прикладом, тактичні завдання цієї ситуації можна доповнити такими:

– встановлення фактичного місцеперебування користувача, який здійснив напад на комп'ютерну мережу з метою унеможливлення доступу до ресурсу й завдання матеріальних збитків його власнику;

– встановлення механізму отримання та розподілу здобутих унаслідок вчинення злочину грошових коштів. Для виконання поставлених завдань можна здійснити такі слідчі (розшукові) дії та заходи:

1) доручення оперативному підрозділу в порядку ст. 40 КПК України з метою встановлення шляхів розподілу між членами групи злочинного прибутку;

2) тимчасовий доступ до речей і документів, що містять інформацію на серверах операторів зв'язку, інформацію банківських установ про конкретний рахунок, що використаний для переведення коштів злочинцю під час контролю за вчиненням злочину;

3) тимчасовий доступ до речей і документів, що містять інформацію на серверах операторів платіжних систем «QIWI» та «Яндекс Деньги» у зв'язку з потребою ідентифікувати А. та Б. як отримувачів конкретних платежів від компанії «Dating.com Group Limited»;

4) слідчий огляд отриманого під час тимчасового доступу до речей і документів.

Ситуація 1.2. *Кримінальне провадження розпочато в результаті перевірки оперативної інформації, матеріали первинної перевірки містять персоналізовані відомості про особу злочинця. С*итуація типова при розслідуванні тяжких конвенційних кіберзлочинів злочинцем-користувачем і злочинцем – упевненим користувачем. Кримінальне провадження розпочинають типово у

зв'язку з докладним рапортом співробітника ДКП НП України, при цьому особа або група осіб у визначеному складі вже затримана під час вчинення злочину.

Вказану ситуацію можна проілюструвати на прикладі. Так, гр. Д. та Ч., які, діючи за попередньою змовою з метою вчинення розпусних дій щодо малолітньої особи Н., виготовляли, зберігали з метою розповсюдження та розповсюджували зображення, що містять порнографію. З матеріалів справи вбачається, що законний представник малолітньої потерпілої (її мати М.) звернула увагу на незвичну збентежену поведінку доньки. Донька розповіла матері, що два тижні тому спочатку із цікавості почала спілкуватися через соціальну мережу «Вконтакте» зі співрозмовником «Х», а потім до спілкування долучився користувач «К». Невдовзі спілкування набрало непристойного характеру, їй надсилали фото відповідного змісту. Із заявою про вчинення злочину представник потерпілої звернулася до правоохоронного органу. Під час подальшого спілкування під контролем матері та правоохоронців на соціальну сторінку малолітньої продовжували надсилати фотографічні зображення та відеофайли порнографічного змісту, текстові та голосові повідомлення з пропозицією вступити в традиційні та нетрадиційні статеві відносини, що завершилося призначенням зустрічі та подальшим затриманням злочинців.

На початковому етапі розслідування основними тактичними завданнями в цій ситуації є:

– затримання Д. та Ч. й одночасна реєстрація в ЄРДР кримінального правопорушення;

– персоналізація акаунтів користувачів як злочинців;

– забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу Д. та Ч. в мережі;

– встановлення факту обізнаності Д. та Ч. щодо малолітнього віку потерпілої;

– встановлення інших фактів розповсюдження продукції порнографічного характеру;

– встановлення психологічного контакту з малолітньою;

– встановлення осіб, яким стало відомо про таку діяльність Д. та Ч.;

– встановлення фактів створення продукції порнографічного змісту;

– встановлення способів створення та виготовлення продукції порнографічного характеру.

Основні тактичні завдання розслідування виконано шляхом проведення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого:

1) особистий огляд Д. і Ч., під час якого вони видали мобільні телефони, за допомогою яких відбувалося користування соціальною мережею «Вконтакте»;

2) опитування Д. та Ч.;

3) доручення оперативному підрозділу Департаменту кіберполіції Національної поліції України в порядку ст. 40 КПК України на проведення оперативно-розшукових заходів з метою персоналізації відомостей про користувачів;

4) слідчий огляд телефонів Д. та Ч.;

5) проведення обшуків за місцем мешкання Д., унаслідок чого вилучено 30 оптичних дисків для лазерних систем зчитування;

6) проведення обшуку за місцем мешкання Ч.;

7) проведення огляду електронної сторінки потерпілої в соціальній мережі, під час якого встановлено багаторазове листування з окремими користувачами (Д. та Ч.), відеозапис;

8) допит потерпілої, свідків (близьких родичів Н.);

9) слідчий огляд вилучених під час обшуку предметів;

10) оголошення підозри Д. і Ч.

Ситуація була ускладнена неможливістю залучити в кримінальне провадження всіх свідків поширення предметів дитячої порнографії, їх створення, виготовлення, адже через малолітній вік свідків їхні представники були проти допиту. Момент затримання Д. і Ч. є ключовим моментом виявлення злочинців, адже на той час зміст листування та поширена ними продукція повинні містити ознаки порнографічної продукції та вказувати на навмисні розпусні дії щодо малолітньої особи, тому внаслідок слідчих дій та ОРЗ чітко фіксують момент надіслання користувачем під нік-неймом потерпілої текстового повідомлення про малолітній вік потерпілої – 10 років, у непроцесуальний спосіб до моменту початку кримінального провадження отримують консультацію фахівця з мистецтвознавства та психолога.

Ситуація 1.3. *Кримінальне провадження розпочато в рамках реалізації матеріалів ОРС; персоналізація особи злочинця для слідчого є закономірною (в результаті діяльності оперативних підрозділів*

згідно спільного зі слідчим плану реалізації матеріалів ОРС). Ситуація є типовою при розслідуванні тяжких та особливо тяжких злочинів, вчинених з корисливих мотивів, тяжких конвенційних злочинів, вчинених злочинцем – досвідченим користувачем.

Таку слідчу ситуацію демонструє кримінальне провадження щодо обвинувачення гр. А., який здійснював за попередньою змовою з гр. Б. неправомірне використання електронних грошей. У процесі судового розгляду незаперечно було доведено вину лише у вчиненні кримінального правопорушення, передбаченого ч. 2 ст. 200 КК України[1]. Унаслідок здійснення контролю за телефонними розмовами та зняття інформації з каналів зв'язку (як ОРЗ протягом року) на момент початку кримінального провадження було відомо, що А. і Б., діючи в порушення чинного законодавства України, а також Закону України «Про платіжні системи та переказ коштів в Україні», постанови Правління Національного банку України від 4 листопада 2010 року № 481, якою затверджене Положення «Про електронні гроші в Україні», застосовували та використовували у фінансово-господарській діяльності фізичної особи – підприємця А. електронні гроші платіжних систем «WebMoney Transfer» і «Liberti Reserve». Ці особи надавали послуги з введення/виведення, обміну, конвертації (переведення в готівку та навпаки) електронних грошей (українська гривня, долар США, євро, російський рубль) за допомогою платіжних систем. Переведення (конвертація) електронних грошей на готівку обвинуваченими відбувалося так: замовники (споживачі, фізичні особи), власники електронних грошей, за допомогою мережі Інтернет через сайт підприємця А. здійснювали замовлення, переважно в телефонному режимі, про виведення (конвертацію) електронних грошей у готівку (здебільшого це долар США, українська гривня) та пересилали необхідну суму електронних грошей зі свого електронного гаманця на електронні гаманці, які знаходилися в користуванні Б. та фізичної особи – підприємця А. Протягом однієї доби споживачі (фізичні особи), власники електронних грошей приходили за адресою здійснення фінансово-господарської діяльності фізичної особи – підприємця А.

[1] Вирок Шевченківського районного суду м. Чернівці від 5 трав. 2014 р. Справа № 727/11024/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/ Review/46270509.

(у м. Чернівцях, різні офіси), на вимогу А. та/або Б. пред'являли паспорт, з якого робили копію й отримували взамін на перераховані електронні гроші електронних платіжних систем «WebMoney Transfer» та «Liberty Reserve» особисто від Б. та/або А. готівку в сумі перерахованих електронних грошей (мінус 3–5 % від перерахованої суми) як плату за надану послугу. У справі фігурують інші особи, на яких було відкрито банківські рахунки, що за дорученням надані в користування гр. А. та Б., загальний оборот коштів лише на одному з рахунків становив 520 360 доларів США.

На початковому етапі розслідування основними тактичними завданнями в цій ситуації будуть:

– забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу в мережі фізичної особи – підприємця А.;

– встановлення якомога більшої кількості споживачів (фізичних осіб), власників електронних грошей, що користувалися послугами А. та Б., які можуть бути свідками в провадженні;

– встановлення фактів фіктивного підприємництва, що супроводжували злочин;

– встановлення інших осіб, вирішення питання про причетність їх до злочину, зокрема осіб, на які було відкрито банківські рахунки, що використовували в механізмі злочинної діяльності;

– встановлення фактів створення продукції порнографічного характеру;

– встановлення походження грошових коштів на рахунках фірм А. та Б., грошових коштів, що вилучено під час розслідування;

– встановлення фактів вчинення підроблення документів, які подають для здійснення державної реєстрації юридичної особи та фізичних осіб – підприємців;

– встановлення фактів легалізації (відмивання) доходів, одержаних злочинним шляхом;

– встановлення розміру матеріального збитку державі.

Тактичні завдання розслідування виконуються шляхом проведення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого:

1) доручення оперативному підрозділу в порядку ст. 40 КПК України проведення заходів з метою отримання орієнтувальних відомостей про чітко визначені рахунки в «WebMoney Transfer»,

«Liberti Reserve»», а також у Національному банку України щодо реєстрації платіжних систем «WebMoney Transfer», «Liberti Reserve», їх учасників, операторів послуг цих систем, комерційних агентів, правил використання електронних грошей «WebMoney Transfer», «Liberti Reserve»;

2) тимчасовий доступ до речей і документів щодо руху коштів банківськими рахунками, що використовували А. та Б. для переведення в готівку електронних грошей клієнтів;

3) обшук в офісі фірми «Вебмані-Буковіна» та за місцями мешкання А. та Б.;

4) допити осіб-клієнтів фірми «Вебмані-Буковіна»;

5) тимчасовий доступ до речей і документів цих осіб (зокрема квитанції під час здійснення операцій);

6) слідчі огляди вилученого під час обшуків (банківські картки, заяви, копії паспортів, графік і правила роботи офісу, чорнові записи з іменами та сумами коштів, номерами телефонів, квитанції, акти, рахунки, виписані банком «Хрещатик» на ім'я інших осіб, бланк «Вестерн-Юніон» на отримання готівки А., журнал обліку доходів і витрат, грошові кошти в сумі 11 719 доларів США, 1755 євро, 643 леїв румунських, 3248 грн, ноутбук та інша оргтехніка);

7) затримання, оголошення підозри й допит А. та Б.

Для забезпечення ефективного розслідування в таких кримінальних провадженнях є потреба у своєчасному налагодженні взаємодії слідчого з оперативним підрозділом, створенні спільної слідчо-оперативної групи з кількох слідчих й оперативних працівників.

2. Ситуації, що характеризується наявністю неперсоналізованих відомостей про користувача як імовірного злочинця.

Ситуація 2.1. *Кримінальне провадження розпочато в результаті отримання заяви/повідомлення особи про кримінальне правопорушення, матеріали звернення містять неперсоналізовані відомості про особу злочинця.* Зазначена ситуація є характерною для розслідування злочинів, вчинених злочинцем-користувачем початкового рівня з насильницько-егоїстичних чи насильницько-дискримінаційних мотивів, деяких злочинів у сфері функціонування електронних розрахунків. Наслідок злочину є конкретизований заявою про злочин особи (якій спричинено матеріальний чи

моральний збиток), тому на момент відкриття кримінального провадження мотив злочину не піддається сумніву.

Таку слідчу ситуацію можна проілюструвати кримінальним провадженням з обвинувачення гр. І.[1], який протягом двох років, маючи намір заволодіти чужим майном шляхом обману за допомогою здійснення електронних операцій з використанням електронно-обчислювальної техніки, перебуваючи за місцем свого мешкання, зареєструвався на сайті інтернет-аукціону, використовуючи логін «v» та електронну адресу (зареєстровану на іншу особу), виставляв на аукціон лоти (електронне обладнання), після отримання пропозиції придбати товар пропонував відправити завдаток або повну оплату за товар, якого насправді не мав, у формі електронного платежу, отримавши гроші, уникав спілкування з потерпілими та змінював контакти. Унаслідок звернення представництва інтернет-аукціону (ТОВ) та заяви потерпілого від злочинів до правоохоронних органів інформацію про злочин було внесено до ЄРДР. У заяві ТОВ було зазначено таку інформацію: кількість жертв злочинів, суть злочинів, відомості про акаунт «v», зокрема контактні e-mail, телефони, IP-адресу провайдера, номер карткового рахунку, що використовував суб'єкт.

На початковому етапі розслідування основними тактичними завданнями будуть:

– персоналізація акаунта користувача Інтернет-аукціону;

– встановлення особи/осіб, що заволоділа/ли грошовими коштами громадян, місце їх мешкання;

– встановлення зі списку потерпілих від злочинів тих, що оплатили, але не отримали товар;

– забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу злочинця в мережі;

– встановлення кола осіб, що могли діяти в групі;

– встановлення та підтвердження факту/ів здійснення операцій з використанням електронно-обчислювальної техніки, що забезпечили доведення злочину до кінця;

[1] Вирок Київського районного суду м. Одеси від 12.06.2015 р. Справа № 520/3455/15-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: http://reyestr.court.gov.ua/Review/45059214

– встановлення фактів фізичної відсутності товару, який був запропонований у лоті для продажу;

– забезпечення відшкодування заподіяних злочином матеріальних збитків і можливої конфіскації майна.

Основні тактичні завдання розслідування виконуються шляхом здійснення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого:

1) доручення на проведення оперативним підрозділам слідчих (розшукових) дій з метою персоналізації відомостей про користувача як злочинця та встановлення всіх потерпілих;

2) отримання інформації в КП «ЖКС Чорноморський», ТОВ «Теннет» з метою персоналізації особи (адреса фактична та IP-адреса, що була виділена суб'єкту);

3) допити потерпілих (у різних областях України);

4) тимчасовий доступ до речей і документів (у банках отримання виписок за особистими рахунками потерпілих, копія заяв на оформлення кредитної картки);

5) протокол тимчасового доступу до речей і документів (в м. Одесі щодо відомостей про користувачів, яким були присвоєні динамічні IP-адреси для виходу в Інтернет у конкретні дату та час);

6) слідчий огляд отриманого з метою визначення конкретного користувача;

7) обшук за місцем мешкання гр. І. (вилучено роутер, банківські платіжні засоби, документи на мобільні телефони, чорнові записи, апарати мобільних телефонів із сім-картами);

8) опитування І. про обставини вчинення злочину;

9) допит як свідків осіб, які мешкають за адресою проведення обшуку (членів сім'ї можливого злочинця);

10) слідчий огляд вилученого майна;

11) оголошення підозри І. та допит його як підозрюваного.

Необхідно акцентувати увагу на такій суттєвій у контексті методик розслідування злочинів у кіберпросторі обставині – моменті оголошення підозри щодо одного епізоду злочину, що є початком нового кримінального провадження в ініціативній формі щодо інших епізодів злочину, про які стало відомо після огляду вилучених джерел електронної інформації. З формулюванням «під час здійснення досудового розслідування в кримінальному провадженні встановлено особу» реєструють нові кримінальні провадження, які потім

об'єднують під єдиним провадженням за одним реєстраційним номером ЄРДР. Оскільки на початку такого кримінального провадження склалася ситуація, що характеризується наявністю достатніх відомостей про злочин і підозрюваного, що отримані в першому провадженні, ми вважаємо за потрібне не визначати такі умови ситуації як окремий тип, адже тактичні завдання й засоби їх виконання пов'язані з появою підозрюваного, чим зумовлений наступний етап розслідування.

Ситуація 2.2. *Кримінальне провадження розпочато в результаті перевірки оперативної інформації, матеріали первинної перевірки містять неперсоналізовані відомості про особу злочинця.* Ситуація притаманна при розслідуванні вчинення злочинцем – досвідченим користувачем конвенційних кіберзлочинів (злочинів, пов'язаних з анархістськими діями в кіберпросторі; інтелектуальне піратство) або злочинцем-користувачем злочинів з антидержавно-політичних мотивів, що становлять елементарну дію (як-от розміщення інформації певного змісту в кіберпросторі). Способи конспірації своєї діяльності у мережі злочинець не застосовував, тому дані, що дозволяють його в подальшому персоналізувати, були встановлені за допомогою спеціальних знань працівників ДКП НП України. Кримінальне провадження розпочинається у зв'язку з рапортом співробітника оперативного підрозділу про виявлений ним злочин, що вчинений невстановленою особою.

Показовим є кримінальне провадження стосовно гр. Н., що поширював шкідливий програмний засіб «NotPetya», основним функціональним призначенням якого є несанкціоноване блокування та шифрування інформації, яку опрацьовують комп'ютери, і вимагання грошових коштів для розблокування зашифрованих даних[1]. Внаслідок перевірки оперативної інформації співробітники кіберполіції встановили обліковий запис (акаунт), розміщений на відеохостингу «YouTube», власник якого виклав відеозапис з детальними інструкціями про розповсюдження шкідливого програмного засобу «NotPetya» на акаунті в соціальній мережі «Google Plus», де, крім цього, вивантажив у вільний доступ із власного комп'ютера сам вірус-

[1] Вирок Нікопольського міськрайонного суду Дніпропетровської області від 30.08.2018 р. Справа № 182/4213/18. *Єдиний державний реєстр судових рішень* : [сайт]. URL: http://reyestr.court.gov.ua/Review/76270022.

вимагач. Як відомо, до цього моменту, а саме 27 червня 2017 року електронно-обчислювальні машини (комп'ютери) підприємств, установ та організацій України шляхом автоматичного оновлення комп'ютерної програми «M.E.Doc», призначеної для реєстрації та подання податкових накладних, електронної звітності контролюючим органам, обміну податковими накладними, рахунками, актами, договорами й іншими юридично значущими документами з контрагентами чи партнерами, зазнали масового ураження шкідливим програмним засобом – вірусом-вимагачем «NotPetya». До правоохоронних органів України надходили повідомлення про те, що після оновлення комп'ютерної програми «M.E.Doc» та автоматичного перезавантаження операційної системи відбулося ураження електронно-обчислювальних машин, на їхніх екранах з'явилося повідомлення про блокування машини та необхідність сплати 300 доларів США в біткоїнах. Інформація, яка містилася на уражених машинах, була зашифрована, без можливості розшифрування, що призвело до її втрати та блокування. Зазначену подію активно висвітлювали в засобах масової інформації, що спричинило резонанс у суспільстві.

На початковому етапі розслідування в описаній ситуації основними тактичними завданнями будуть:

– персоналізація акаунта й визначення Н. як користувача-злочинця;

– забезпечення збереження електронних носіїв інформації, у яких зафіксовано роботу Н. у мережі;

– встановлення шляхів отримання Н. шкідливого програмного засобу;

– встановлення його обізнаності в призначенні програмного засобу «NotPetya»;

– встановлення кола осіб, що мали змогу здійснити розповсюдження шкідливих програмних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів) і комп'ютерних мереж;

– встановлення та підтвердження фактів розповсюдження програмного засобу «NotPetya» (їх кількості);

– встановлення дій Н., спрямованих на пошук та отримання шкідливого програмного засобу – вірусу-вимагача «NotPetya»;

– встановлення осіб, які здійснили скачування шкідливого програмного засобу.

Основні тактичні завдання розслідування можна виконати шляхом проведення такого комплексу слідчих (розшукових) дій та інших заходів пізнання слідчого:

1) доручення оперативному підрозділу в порядку ст. 40 КПК України на проведення оперативних заходів і слідчих (розшукових) дій;

2) проведення огляду місця події в осіб, які в електронному зверненні повідомили про факт розповсюдження та завантаження ними шкідливого програмного засобу;

3) слідчий огляд отриманої електронної інформації, яку записано на оптичний диск;

4) допит свідків;

5) доручення оперативному підрозділу в порядку ст. 40 КПК України з метою встановлення фактичного місця здійснення розповсюдження шкідливого програмного засобу;

6) витребування відомостей від комунального підприємства «Н» щодо права власності на об'єкт нерухомості за фактичною адресою розповсюдження;

7) здійснення обшуку на підставі ухвали слідчого судді за адресою фактичного розповсюдження;

8) слідчий огляд вилучених під час обшуку предметів, що мають значення речових доказів, а саме: системний блок, ноутбук марки «HP», оптичні носії;

9) опитування Н. про обставини злочину;

10) витребування відомостей щодо Н. (про непритягнення до кримінальної відповідальності; про перебування на медичних обліках; побутової характеристики);

11) призначення судової комп'ютерно-технічної експертизи;

12) оголошення підозри Н. та його допит як підозрюваного.

Унаслідок комплексу засобів виконання поставлених слідчим завдань було встановлено, що 1 липня 2017 року, діючи з метою подальшого незаконного розповсюдження, Н. отримав від невстановленої досудовим розслідуванням особи під нік-неймом «S» шкідливий програмний засіб. Н. достовірно знав, що атака вірусу «NotPetya» вразила ІТ-системи компаній в Україні, з метою підвищення відвідуваності та просування створених ним відеоканалів

(акаунтів), використовуючи власний досвід і будучи обізнаним із принципами роботи комп'ютерів і комп'ютерних мереж, за допомогою власних комп'ютерів у всесвітній інформаційній системі загального доступу Інтернет попередньо вчинив дії, спрямовані на пошук та отримання шкідливого програмного засобу – вірусу-вимагача «NotPetya», які полягали в розміщенні оголошень, відвідуванні форумів і використанні пошукових систем. Він о 19 год 39 хв завантажив і зберіг цей шкідливий програмний засіб на накопичувачі жорсткого магнітного диска, а наступного дня, перебуваючи за місцем свого мешкання в м. Нікополі, створив відеозапис й о 20 год 49 хв розмістив його на власному акаунті разом з посиланням на вірус. Протягом липня 2018 року вірус завантажили невстановлені користувачі 373 рази. Будучи обізнаним, Н. надав користувачам Інтернету доступ до шкідливого програмного забезпечення, розповсюдивши шкідливі програмні засоби, призначені для несанкціонованого втручання в роботу комп'ютерів і комп'ютерних мереж.

Акцентуємо, що оскільки негласні слідчі (розшукові) дії проводяться лише щодо тяжких та особливо тяжких злочинів, а поширення вірусу не виступає таким злочином, то фактично слідчий не мав можливість вирішити завдання щодо встановлення всіх осіб, що брали участь у процесі поширення вірусу.

Ситуація 2.3. *Кримінальне провадження розпочато в рамках реалізації матеріалів ОРС; матеріали справи містять неперсоналізовані відомості про особу злочинця.* Ситуація є характерною при виявленні ознак готування до злочинів, пов'язаних зі сферою захисту інформації з обмеженим доступом, яку обробляють в автоматизованих системах, до злочинів, що порушують встановлений порядок обігу певних речей**.** На момент початку кримінального провадження інформація, що містить ознаки готування до вчинення злочину зафіксована під час установлення місцезнаходження радіоелектронного засобу; контролю за телефонними розмовами; зняття інформації з електронних інформаційних систем. Ініціативний рапорт є формальним кроком на шляху реалізації матеріалів ОРС, основним завданням слідчого в цій ситуації вбачається фіксація мотиву злочинної діяльності встановленої особи та, у разі спроби вчинення нею злочину, виявлення інших співучасників. Такі особи традиційно належать до типу злочинців – упевнених користувачів, які

зазвичай були колись або на момент вчинення пов'язані з організацією, через яку можуть отримувати інформацію з обмеженим доступом, цю інформацію вони використовують з різною метою, що й вимагає проведення НС(Р)Д.

Такий злочинець майже в половині випадків діє в складі корпоративної організованої групи як виконавець злочину або співвиконавець, тому в подальшому типово бере на себе зобов'язання співпрацювати з правоохоронними органами щодо попередження та викриття кримінальних правопорушень, вчинених іншими особами, про які йому відомо або стане відомо згодом, пов'язані з несанкціонованим збутом інформації з обмеженим доступом, яка зберігається в автоматизованих системах, мережах або комп'ютерах, створеної та захищеної відповідно до чинного законодавства, зокрема викритті осіб, які безпосередньо йому збули або сприяли отриманню інформації з обмеженим доступом. Показовим у цьому контексті є кримінальне провадження щодо гр. Н., який 2016 року з корисливих мотивів, реалізуючи свій злочинний умисел, на інтернет-форумі «Darkmoney.cc» розмістив оголошення про продаж інформації з обмеженим доступом, а саме баз даних НП України, ДФС, Головного сервісного центру МВС України, Інтерполу, ДМС України, Державної прикордонної служби України, ПАТ КБ «Приватбанк», ПАТ «Укрпошти», ТОВ «Нова пошта», а також деталізовані телефонні з'єднання всіх мобільних операторів України[1].

29 березня 2018 року на мобільний телефон Н. надійшло смс-повідомлення від абонента з нікнеймом І. про бажання придбати інформацію з обмеженим доступом (відомості з ДФС щодо ТОВ «ІІН», відомості з Інформаційно-телекомунікаційної системи прикордонного контролю «Гарт-1» щодо перетину державного кордону України конкретною особою та відомості з клієнтської бази даних ПАТ КБ «Приватбанк» про неї). Зазначену інформацію Н. оцінив в 1850 доларів США, які необхідно перерахувати у вигляді відсотка криптовалюти біткоїн на електронний онлайн-гаманець Bitcoin. Покупець погодився, і 29 березня 2018 року на мобільний номер телефону абонента з нікнеймом І. було надіслано текстове

[1] Вирок Херсонського міського суду Херсонської області 09.08.2018 р. Справа № 766/9634/18. *Єдиний державний реєстр судових рішень* : [сайт]. URL URL: http://reyestr.court.gov.ua/Review/75817657.

повідомлення з файловим розширенням «.pdf» за допомогою програмного забезпечення «Telegram», у якому містилися відомості з бази «Гарт-1», які належать до інформації з обмеженим доступом та охороняються законом. 30 березня 2018 року о 14 год 10 хв Н. відправив у такий самий спосіб відомості з бази даних ПАТ КБ «Приватбанк» (ID клієнта, серію та номер паспорта особи). Цього дня о 18 год на зазначений номер електронного онлайн-гаманця Bitcoin від абонента з нікнеймом І. надійшла частина обумовленої суми. Невдовзі Н. надіслав І. відомості з ДФС, за що І. перерахував 1 (один) біткоїн криптовалюти, що еквівалентно 7000 доларів США. У березні 2018 року між прокурором й обвинуваченим Н. було укладено угоду про визнання винуватості.

На початковому етапі розслідування визначено такі основні тактичні завдання:

– встановлення фактичного наміру Н. вчинити злочин певної кваліфікації;

– виявлення інших осіб, причетних до вчинення несанкціонованого збуту інформації з обмеженим доступом, та інших злочинів, що пов'язані із зазначеним;

– здійснення документування злочинної діяльності;

– встановлення та подолання засобів конспірації злочинної діяльності.

Окреслені основні тактичні завдання розслідування можна реалізувати шляхом проведення такого комплексу НС(Р)Д, С(Р)Д та інших заходів:

1) зняття інформації з електронних інформаційних систем;

2) контроль за вчиненням злочину у формі оперативної закупки інформації з обмеженим доступом;

3) доручення оперативним підрозділам у порядку ст. 40 КПК України отримати та проаналізувати інформацію від операторів зв'язку щодо конкретного абонента й точки доступу, а також офіційну інформацію з ДФС, Державної прикордонної служби України, ПАТ КБ «Приватбанк» та інших структур про віднесення визначеної групи інформації до інформації, що підлягає захисту державою (у межах виконання вимог ст. 93 КПК України);

4) тимчасовий доступ до речей і документів, що містять інформацію на серверах операторів зв'язку; інформацію банківських установ про конкретний рахунок, що був використаний для

переведення коштів злочинцю під час контролю за вчиненням злочину;

5) обшуки за місцем роботи та мешкання Н.;

6) затримання, повідомлення підозри й допит підозрюваного Н.

Після оголошення підозри Н. зобов'язався співпрацювати з правоохоронними органами щодо викриття осіб, які безпосередньо збули йому інформацію з обмеженим доступом, у зв'язку з чим було укладено угоду про визнання винуватості.

Вчинення злочину службовою особою або залучення її до вчинення злочину обумовлює виконання специфічних тактичних завдань під час розслідування такої діяльності, зокрема:

1) виявлення причиново-наслідкових зв'язків, що засвідчують наявність корупційної складової злочинної діяльності;

2) виявлення причиново-наслідкових зв'язків, що засвідчують наявність міжрегіональних або транснаціональних злочинних зв'язків.

Тому можна вважати перспективним розроблення окремих методик розслідування кіберзлочинів, що пов'язані з отриманням неправомірної вигоди, або службових злочинів, пов'язаних із втручанням у роботу автоматизованих систем. У практичній діяльності правоохоронних органів дедалі частіше виявляють комплекс злочинів, передбачених ч. 2 ст. 362, ч. 3 ст. 362 та ч. 1 ст. 368 КК України або іншими статтями, що пов'язані із вчиненням злочину службовою особою. Прикладом можна вважати кримінальне провадження щодо обвинувачення О., який, працюючи на посаді оперуповноваженого сектору кримінальної поліції в м. Вінниці, з корисливих мотивів розповсюджував інформацію з обмеженим доступом з використанням месенджера «Телеграм», яку отримував за допомогою інформаційно-пошукових системи МВС України. Тактичні завдання та засоби їх виконання аналогічні вже розглянутому порядку. В аналізованій ситуації активно використовують під час проведення НС(Р)Д несправжні (імітаційні) засоби (у порядку ст. 273 КПК України), наприклад, у кримінальному провадженні з обвинувачення О., секретаря Бабушкінського районного суду м. Дніпропетровська, для викриття злочинної діяльності якого в

процесі проведення контролю за вчиненням злочину було використано імітаційні гроші[1].

3. Ситуації, що характеризується відсутністю будь-яких відомостей про особу злочинця.

Ситуація 3.1. *Кримінальне провадження розпочато в результаті отримання заяви/повідомлення особи про кримінальне правопорушення, в матеріалах відсутні будь-які відомості про особу злочинця.* Наявність такої ситуації в практиці правоохоронних органів продиктована необхідністю реалізації оперативної інформації про нетяжкі та середньої тяжкості злочини, що вчиняються з соціально-економічних мотивів, пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі. Окреслюючи цю ситуацію, слід враховувати, що інформація про злочин, отримана при негласній роботі інспектора міжрегіональних управлінь ДКП НП України спеціальними методами, досить часто оцінюється слідчим з правових позицій як недостовірна, а тому заява особи, по суті, виконує роль «завіси» для початку кримінального провадження та отримання правових засобів викриття злочинної діяльності. Заявник найчастіше є фізичною особою, яка шляхом співробітництва з оперативним підрозділом формально складає повідомлення про організовану злочинну діяльність, її персональні дані можуть бути «вигаданими» з метою приховання її фактичних даних, слідчий допитує її як свідка, який виявив підозрілу з його точки зору інформацію в мережі Інтернет. На цьому робота слідчого із заявником закінчується.

Показовим у цьому контексті є кримінальне провадження, яке розслідували щодо організованої групи осіб, які на території м. Одеси організували «порностудію». Відповідно до матеріалів справи, гр. Я., що мешкав у м. Києві, наділений рисами лідера, сильним і стійким характером, переслідуючи корисливі цілі, маючи за мету використовувати злочинну діяльність як постійне й основне джерело прибутку та усвідомлюючи, що для виконання функцій із забезпечення діяльності з організації виготовлення з метою збуту, збуту і розповсюдження порнографічних предметів, у вигляді відеопродукції шляхом її прямої трансляції (демонстрування) за

[1] Вирок Жовтневого районного суду м. Дніпропетровська від 11 серп. 2016 р. Справа № 1-кп/201/169/2016. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/59701953.

допомогою електронних систем і передання інформації у всесвітню інформаційну мережу Інтернет у режимі реального часу на спеціалізованих інтернет-ресурсах створив організовану групу, учасників якої об'єднав планом з розподілом функцій для кожного, а також особисто вповноважив себе брати участь у діяльності організованої групи та керувати нею. Спочатку він створив інтернет-ресурс як засіб пошуку на всій території України осіб жіночої статі – моделей для подальшого виготовлення порнопродукції. За допомогою цього ресурсу й особистих зустрічей з моделями він розподілив функції між усіма учасниками групи (обрав для себе співорганізатів М. та Б., а також 8 виконавців (моделей). В арендованих квартирах встановили спеціальне обладнання, здійснювали дії, спрямовані на пошук і добір осіб жіночої статі для участі в прямих трансляціях порнопродукції за допомогою електронних систем і передання інформації в Інтернет, а також саму трансляцію порнопродукції шляхом її демонстрування. Щоб запобігти викриттю працівниками правоохоронних органів злочинної діяльності організованої групи, особи використовували заходи й методи конспірації, зокрема псевдоніми, спілкування з абонентських номерів, спеціально придбаних із цією метою, системи електронних платежів, не зареєстрованих на території України.

На початковому етапі розслідування слідчий може визначити такі основні тактичні завдання:

– встановлення фактичних місць розташування студій в Україні;

– отримання вичерпної інформації про власників цих приміщень і користувачів мережею, провайдерів, операторів зв'язку, що забезпечують надання телекомунікаційних послуг, послуг зв'язку; встановлення організаторів студій та інших осіб, причетних до вчинення поширення порнопродукції мережею Інтернет;

– персоналізація відомостей про користувачів визначених соціальних сторінок і встановлення наявності в них засобів платежів; здійснення документування злочинної діяльності кожного учасника злочинної групи;

– встановлення та подолання засобів конспірації, які використовують учасники групи; з'ясування наявності грошових коштів на розрахункових рахунках членів групи;

– встановлення отримання та відправлення співорганізаторами поштових відправлень у межах України та за кордоном; виявлення ознак інших злочинів, вчинених у кіберпросторі.

Окреслені завдання розслідування виконують шляхом проведення такого комплексу С(Р)Д та інших заходів:

1) допит заявника як свідка про виявлене ним кримінальне правопорушення;

2) здійснення контролю за вчиненням злочину у формі оперативної закупки порнопродукції на компакт-дисках (тим самим було окремо зафіксовано в реальному часі факт вчинення збуту та розповсюдження продукції порнографічного характеру кожною особою, що виконувала в групі роль виконавця; візуальна інформація, яка відображалася на екрані монітора, була зафіксована під час проведення контролю за вчиненням злочину на окремий носій);

3) призначення та проведення мистецтвознавчої експертизи матеріалів, що містяться на поданих на дослідження CD-R дисках (відеозаписи, отримані внаслідок здійснення контролю за вчиненням злочину);

4) доручення підрозділам ДКП НП України в порядку ст. 40 України з метою встановлення фактичного місця організації порностудії та проведення ОРЗ;

5) проведення обшуків за місцем розташування порностудії та мешкання співорганізаторів;

6) відбирання пояснень у спів організаторів та осіб, які виконували роль «моделі»;

7) слідчий огляд вилученого майна та його арешт;

8) огляд соціальних сторінок з метою перевірки інформації, що була надана в поясненнях М. та Б. про організатора злочинної діяльності;

9) доручення підрозділам ДКП НП України в порядку ст. 40 КПК України отримати та проаналізувати інформацію від провайдерів, операторів зв'язку і телекомунікацій щодо конкретного абонента й точки доступу (у межах виконання вимог ст. 93 КПК України);

10) зняття інформації з транспортних телекомунікаційних мереж (електронних інформаційних систем) конкретного абонента (організатора та співорганізаторів) з метою встановлення характеру його дій (опис змісту електронних поштових відправлень);

11) обшук за місцем мешкання Я. (у м. К);

12) проведення ОРЗ з метою встановлення шляхів розподілу між членами групи прибутку від збуту продукції порнографічного характеру (у межах виконання вимог ст. 93 КПК України);

13) тимчасовий доступ до речей і документів для отримання: а) інформації, що зберігається на серверах провайдерів, які забезпечували телекомунікаційний зв'язок за адресами порностудії; б) інформації в операторів зв'язку про телефонні дзвінки за сім-картами співучасників, розташування базових станцій, типи з'єднань, ідентифікаційні ознаки кінцевого обладнання, сеанси зв'язку; в) інформації в банківських установах про конкретних власників карток і рух коштів на рахунках;

14) призначення комплексу експертиз: комп'ютерно-технічної, програмних продуктів, судової портретної за експертною спеціальністю 6.2 «Ідентифікація особи за ознаками зовнішності за матеріальними зображеннями», мистецтвознавчої

14) затримання Я., допит підорзрюваних.

Усі дії після проведення обшуку зумовлені змістом версій, які висвітлюють: особу організатора; злочинні зв'язки між членами групи, діяльність яких була задокументована шляхом проведення контролю за вчиненням злочину; обрані механізми конспірації злочинної діяльності.

З матеріалів провадження вбачається, що до моменту персоналізації кожного учасника групи та документування мотиву його діяльності в кіберпросторі не було оголошено підозру жодному учаснику групи. Співорганізаторам й організатору оголошено підозру першими, одночасно обрано запобіжні заходи.

Ситуація 3.2. *Кримінальне провадження розпочато в результаті перевірки оперативної інформації, в матеріалах відсутні будь-які відомості про особу злочинця.* Ситуація є типовою при розслідуванні організованої злочинної діяльності, що пов'язана із заволодінням майном шляхом незаконних операцій з використанням електронно-обчислювальної техніки. На момент внесення інформації до ЄРДР наявні відомості про потерпілих у інших кримінальних провадженнях, їх допитано, відомий механізм вчинення злочину, однак через методи конспірації майже немає інформації про членів організованої групи, їх кількість, кількість епізодів злочинної

діяльності. Слідчий, об'єднуючи кілька кримінальних проваджень в одне, отримує широкий спектр основних завдань розслідування.

Розглянемо показове в цьому контексті кримінальне провадження щодо багато чисельної організованої групи, які на території Одеської області вчинили близька 120 епізодів шахрайства з використанням комп'ютерної техніки. Загалом злочини було кваліфіковано за сукупністю ч. 4 ст. 190, ч. 2 ст. 205, ст. 358 КК України. Так, з початку 2015 року гр. Г. за попередньою змовою з гр. Щ., П., С., Л. та іншими встановленими й невстановленими слідством особами, використовуючи мережу Інтернет, створивши під різними доменами фіктивні сайти (кожний сайт діяв від 10-ти до 40 днів), що були електронними магазинами з продажу різної електронної побутової техніки, мобільних телефонів й аксесуарів до них, не маючи в наявності жодного товару, розміщували на сайтах завідомо неправдиву інформацію у вигляді оголошень щодо продажу цієї техніки. Унаслідок цього шахрайським шляхом під приводом продажу техніки заволодівали грошовими коштами, які жертви перераховували на рахунки фіктивно зареєстрованих підприємств. Загальний збиток потерпілих сягає 1 300 000 гривень. З матеріалів провадження вбачається розподіл ролей учасників організованої групи, де чітко визначено ролі: організатор; виконавці («дропи» (від англ. drop «скидати, упускати»), які фізично через банкомати знімали гроші з карткових рахунків фіктивних фірм); «спеціалісти» (програміст, що забезпечував технічний аспект функціонування сайтів).

З квітня 2014 року Г., виконуючи роль керівника організованої групи, організував відкриття фіктивних підприємств з використанням підроблених паспортів, персональних даних, що були отримані від невстановленої в процесі розслідування особи. Фіктивні підприємницькі структури використовували для введення в оману жертв, на їх банківські рахунки надходили платежі від потерпілих. Також на фіктивні підприємницькі структури оформлювали договори про отримання послуг IP-телефонії з метою підтримання постійного телефонного зв'язку з потенційною жертвою та як засіб конспірації діяльності членів організованої групи, яка, будучи технологією, що дає змогу використовувати будь-яку IP-мережу як засіб організації та ведення телефонних розмов, передання відеозображень і факсів у режимі реального часу, надає можливість здійснювати підміну

абонента (перенаправляти дзвінки), організовувати віддалений доступ до інфраструктури IP-телефонії.

На початковому етапі розслідування перед слідчим постають такі основні тактичні завдання:

– встановлення всіх осіб, які входять у злочинну групу;

– з'ясування фактів вчинення інших злочинів, не пов'язаних із відомим механізмом злочинної діяльності;

– виявлення суб'єктного складу щодо кожного з епізодів злочинної діяльності;

– встановлення осіб у складі групи, які не були обізнані щодо вчинення злочину (виконували дії, які не заборонені законодавством України (наприклад, адміністративні або технічні функції, розроблення сайту, надання послуг з його розміщення тощо);

– виявлення зв'язків між учасниками групи;

– визначення ролей кожного учасника групи щодо кожного окремого епізоду злочину;

– подолання методів конспірації злочинної діяльності групи; встановлення механізмів легалізації незаконно отриманих доходів;

– здійснення документування злочинної діяльності.

Окреслені завдання реалізуються шляхом проведення такого комплексу С(Р)Д та інших заходів:

1) допити потерпілих;

2) слідчий огляд веб-сторінки;

3) тимчасовий доступ до речей і документів для отримання відеозаписів камер спостереження та електронних копій інформації:

- щодо банківських послуг конкретній підприємницькій структурі (від ДФС України);

- щодо аспектів адміністрування шахрайських сайтів інтернет-магазинів (від провайдерів, що забезпечували послугу хостингу);

- щодо власників сім-карток, розташування їх базових станцій, типи їх з'єднань, ідентифікаційні ознаки їх кінцевого обладнання, сеанси зв'язку; записів сеансів зв'язку (від операторів IP-телефонії);

- щодо власників та інших персоналізованих даних стосовно фірм, які використовували в механізмі злочинної діяльності (від державного реєстратора);

- щодо матеріалів про відкриття банківських рахунків і рух коштів на них (конкретні банківські установи);

4) слідчий огляд отриманих у межах тимчасового доступу до речей і документів матеріалів з метою конкретизації інформації для встановлення злочинця;

5) слідчий огляд паперових та електронних носіїв інформації;

6) доручення підрозділам ДКП НП України в порядку ст. 40 КПК України провести ОРЗ;

7) аудіо-, відеоконтроль особи С. та Л. (що виконували роль «дропів»);

8) контроль за вчиненням злочину у формі оперативної закупки (зафіксований у реальному часі факт зняття «дропом» грошових коштів через банкомат з рахунку фіктивної фірми);

9) призначення комп'ютерно-технічних і почеркознавчих експертиз;

10) затримання «дропів» і спеціаліста та відбирання пояснень від них;

11) груповий обшук за адресами орендованих для забезпечення злочинної діяльності квартир і місць мешкання затриманих й організатора;

12) оголошення підозри всім затриманим особам (організаторові, виконавцям і спеціалістові).

Зіставлення відеозаписів з камер спостереження, доступ до яких був отриманий в інтернет-провайдера з відеозаписами зняття готівки з камер банкоматів дали змогу конкретизувати конткерну особу виконавця злочину. Версії щодо суб'єктного складу кожного епізоду злочину вимагали перевірки шляхом проведення зазначених вище ОРЗ та НС(Р)Д.

Деякі науковці акцентують увагу на стійкості груп, що вчиняють корисливі злочини з використанням комп'ютера[1]. Утім безапеляційне використання цього теоретичного положення в практичній діяльності слідчого може призвести до неповноти розслідування в конкретному кримінальному провадженні. Матеріали обраного як приклад кримінального провадження засвідчують, що постійними учасниками групи є організатор, співорганізатори та спеціалісти. Останній, що є представником типу злочинець –

[1] Шилан Н. Н., Кривонос Ю. И., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации : учеб. пособие. Луганск : РИО ЛИВД, 1999. С. 24.

досвідчений користувач, порівняно з рештою учасників організованої групи, має інший психотип, характеризується конкуренцією мотивів, що можна вдало використати для проведення за його участю подальших слідчих С(Р)Д. Тому ключовим моментом для викриття механізму та кількості «злочинних проектів» таких груп є затримання особи, що виконує роль «спеціаліста».

Ситуація 3.3. *Кримінальне провадження розпочато в рамках реалізації матеріалів ОРС; у ініціативному рапорті оперативного співробітника відсутність відомостей про особу злочинця є формальною.* Співробітник оперативного підрозділу СБ України ініціативним рапортом повідомляє про групу невстановлених осіб з-поміж радикально налаштованих громадян України, що організувалися для вчинення злочинів з антидержавно-політичних мотивів. Ступінь суспільної небезпечності таких злочинів, обов'язкове застосування злочинцем методів конспірації й типова наявність в окремих осіб з групи практичних навиків вчинення злочинів проти основ національної безпеки України вимагають своєчасного виявлення готування до таких злочинів.

Для цієї ситуації не є характерним завдання слідчого щодо встановлення мотивів злочинної діяльності, в Україні типово такі злочини вчиняють злочинці – користувачі початкового рівня, яким не властива конкуренція мотивів. Основна мета слідчого – реалізація завдань оперативного підрозділу, що полягає в недопущенні настання запланованого злочинного результату, чим власне й зумовлене залучення розширеного комплексу НС(Р)Д. Зазначене можна вважати специфікою цієї ситуації.

Як приклад розглянемо кримінальне провадження з обвинувачення А., який, будучи негативно налаштованим стосовно чинної державної влади, на початку серпня 2014 року в м. Запоріжжі за попередньою домовленістю з іншими особами (матеріали щодо них виділено в окреме провадження) під час спілкування в соціальних мережах Інтернет домовився про вчинення терористичного акту (вибуху) з метою дестабілізації суспільно-політичної обстановки та залякування населення м. Запоріжжя[1]. Для реалізації злочинного наміру

[1] Вирок Орджонікідзевського районного суду м. Запоріжжя від 14 січ. 2016 р. Справа № 335/859/15-к 1-кп/335/18/2016. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/54962947.

А. на виконання відведеної йому ролі через Інтернет замовив хімічний набір і вимірювальні прилади, які він використав для виготовлення вибухової речовини. Усі інструкції з виготовлення вибухових речовин і вибухових пристроїв він знайшов у мережі Інтернет. У першій декаді серпня А. виготовив за місцем свого постійного мешкання чотири саморобні вибухові пристрої, після чого їх було переміщено до трамвайної зупинки, де він їх залишив для Б., який для їх зберігання використав своє гаражне приміщення. Також А. та Б. в жовтні 2014 року підшукали об'єкт для вчинення терористичного акту (приміщення виборчого штабу політичної партії) та місце закладання пристрою, яке планували використати напередодні дострокових парламентських виборів. Задумане до кінця не довели у зв'язку із затриманням співробітниками СБ України в Запорізькій області.

На початковому етапі розслідування слідчий визначить такі тактичні завдання:

– здобути точну й об'єктивну інформацію про ступінь небезпечності зазначених осіб (А., Б. та інших осіб, матеріали стосовно яких виділено в окремі провадження);

– виявити організаційні аспекти функціонування групи радикально налаштованих осіб;

– встановити всіх співучасників злочину;

– визначити та подолати засоби конспірації, які використовують учасники групи;

– виявити ознаки вчинення інших злочинів;

– не допустити приведення вибухових пристроїв у готовність та їх запуск;

– забезпечити своєчасність прийняття управлінських й організаційних рішень;

– забезпечити конфіденційність осіб, які співпрацюють з правоохоронними органами, під час здійснення розслідування означеної злочинної діяльності.

Окреслені завдання розслідування реалізують шляхом проведення такого комплексу С(Р)Д та інших заходів:

1) візуальне спостереження за особами А. та Б.;

2) зняття інформації з транспортних телекомунікаційних мереж (контроль А. та Б.).;

3) доручення підрозділам у порядку ст. 40 КПК України з метою встановлення інших осіб, з якими спілкуються А. та Б., проведення відповідно до них ОРЗ;

4) допит свідків (працівників виборчого штабу);

5) проведення обшуків за місцем мешкання А., Б. та іншої особи (виділено в окреме провадження, відбувся обмін особи на полоненого солдата);

6) слідчий огляд вилученого майна (комп'ютерна техніка, мобільні телефони, записники, військова форма тощо);

7) огляд сторінок у соціальних мережах, комп'ютерної техніки, мобільних телефонів;

8) затримання й оголошення підозри А. та Б.

Одночасно з допитом підозрюваних осіб призначають комплекс судових експертиз (комп'ютерно-технічна, судово-почеркознавча, вибухотехнічна, судово-хімічна, комплексна судово-хімічна та вибухотехнічна). Широкий спектр експертиз, пов'язаний з непередбачуваною обставиною, що була наявна в цьому кримінальному провадженні. Так, одразу після обшуку вибухові пристрої було доставлено до експертної установи в м. Запоріжжі. Їх потрібно було знищити на полігоні, а потім за залишками проводити експертизу, однак у зв'язку з поганими погодними умовами експерти візуально оглянули пристрої, і лише наступного дня було заплановано їх вивезення на полігон для знищення. Під час підготовки ці пристрої несанкціоновано вибухнули в приміщенні експертної установи. Після вибуху всі речові докази були зібрані працівниками прокуратури області та направлені на експертизу в експертну установу м. Дніпропетровська для проведення подальших експертиз. Ця обставина суттєво ускладнила перебіг наступного етапу розслідування, проте не завадила встановити обставини вчинення злочину підозрюваними.

Отже, виділені нами типові слідчі ситуації, відповідні їм тактичні завдання та засоби розв'язання останніх спрямовані на встановлення злочинної діяльності в повному обсязі, кожного суб'єкта злочину та тяжкості його обвинувачення. Вказане зумовлює важливість в теоретико-методичному аспекті ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі.

4.3. Тактичні операції розслідування злочинів, вчинених у кіберпросторі

Важливою складовою етапів розслідування окремого виду злочинів у новітніх криміналістичних дослідженнях є тактична операція. На думку А. Ф. Волобуєва, в окремих криміналістичних методиках характеристика слідчих дій на початковому й подальшому етапах доцільна тільки як характеристика їх комплексів – тактичних операцій[1]. У цьому контексті останні розглянуто в роботах В. П. Бахіна, Р. С. Бєлкіна, І. О. Возгріна, А. В. Дулова, В. А. Журавля, О. Н. Колесніченка, В. О. Коновалової, В. К. Лисиченка, Г. А. Матусовського, М. О. Селіванова, В. В. Тіщенка, В. М. Шевчука, В. Ю. Шепітька, М. П. Яблокова та інших науковців.

Нині в криміналістичній науці створено теоретичне підґрунтя для розроблення тактичних операцій як комплексів слідчих (розшукових) дій, оперативно-розшукових й організаційних заходів, що виконують роль засобу вирішення тактичних (проміжних) завдань розслідування окремих видів злочинів. Визначення місця тактичної операції в структурі окремих криміналістичних методик передбачало насамперед вирішення питання щодо їхнього змісту, що стосується зокрема часових меж їх проведення.

Вплив етапності розслідування злочинів на розроблення тактичних операцій досліджує В. М. Шевчук[2]. Автор розподіляє судження науковців стосовно аналізованого питання на три групи. До першої входять дослідники (О. Ю. Головін, О. О. Закатов, О. А. Чебуренков та інші), які визнають потребу виокремлювати початкові та подальші тактичні операції. Другу групу формують науковці (С. Ф. Здоровко, Г. А. Матусовський, М. П. Яблоков, С. Ю. Якушин), які додають до початкових і подальших операцій також підсумкові. До третьої групи дослідник відносить учених (О. О. Михальчук, В. О. Образцов, С. І. Цвєтков, А. В. Шмонін), які визначають так звані дослідчі тактичні комплекси, операції, що проводять до початку досудового розслідування. Обираючи як

[1] Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. С. 260.

[2] Шевчук В. М. Тактичні операції у криміналістиці: теоретичні засади формування та тактика реалізації : монографія. Харків : Апостиль, 2013. С. 235–255.

підставу такого поділу кількість виокремлених науковцями етапів розслідування, В. М. Шевчук констатує, що процес побудови й ефективність застосування тактичних операцій безпосередньо залежить від того, до якого етапу розслідування чи слідчого розгляду їх розробляють і на якому етапі реалізують[1]. Водночас унаслідок формування власного підходу до періодизації розслідування та виокремлення диференційованої та синтезаційної моделі періодизації процесу розслідування науковець резюмує про особливу значущість стадійності кримінального провадження для роботи з тактичними операціями та визнає можливим існування тактичних операцій досудового розслідування й судового провадження[2].

Не применшуючи значення перелічених вище й зумовлених етапністю розслідування чи стадійністю провадження варіацій тактичних операцій, вважаємо за доцільне акцентувати на особливому значенні тактичних операцій початкового етапу розслідування окремих видів злочинів.

По-перше, тактичні операції, що реалізують на цьому етапі розслідування, мають пошуково-пізнавальну спрямованість. Тому, забезпечуючи на початковому етапі розслідування встановлення події злочину, особи злочинця, інших суттєвих обставин його вчинення, зумовлених можливим комплексом вчинюваних кримінальних правопорушень, такі операції виконують роль «фундаменту» для реалізації в майбутньому правозахисної функції держави.

По-друге, розроблення властивих тактичним завданням початкового етапу розслідування тактичних операцій відображає не лише організаційну складову слідчої діяльності, а й тактичну. Не дивлячись на те, що у змісті типових слідчих ситуацій початкового етапу розслідування наявна лише фактична складова інформації про злочин[3], їх оцінювання слідчим зумовлює постановку відповідних ситуації тактичних завдань розслідування, засобом вирішення яких є певний комплекс слідчих (розшукових) дій, оперативно-розшукових й організаційних заходів.

[1] Там само. С. 246

[2] Там само. С. 253.

[3] Волчецкая Т. С. Криминалистическая ситуалогия : монография / под ред. Н. П. Яблокова. М. ; Калининград : Калинингр. ун-т, 1997. 248 с.

Переважна більшість науковців-криміналістів розглядає слідчі (розшукові) дії як обов'язкову складову тактичних операцій[1]. Тактика провадження окремих, найпоширеніших, слідчих (розшукових) дій залишається самостійним структурним елементом криміналістичної методики розслідування злочинів певного виду.

З огляду на зазначене, вважаємо, що кожна запропонована в методиці тактична операція має відображати таке поєднання слідчих (розшукових) дій, організаційних й оперативно-розшукових заходів, яке є ефективним з позицій розв'язання типового тактичного завдання розслідування.

У цьому контексті В. О. Коновалова висвітлює концепцію тактичних операцій як «своєрідну форму розслідування, що об'єднує організаційні, слідчі та оперативно-розшукові дії для швидкого й ефективного вирішення слідчих завдань»[2]. В. В. Тіщенко визначає цю концепцію як «технологічний підхід, що застосовується під час дослідження послідовних процесів реалізації комплексу окремих дій у системі криміналістичної діяльності»[3]. Конкретизуючи питання співвідношення системи слідчих (розшукових) дій з типовими тактичними операціями, В. А. Журавель доходить висновку, що тактичну операцію доцільно тлумачити як своєрідну форму, організаційно-тактичний засіб здійснення розслідування, що передбачає оптимальну сукупність взаємозв'язаних єдиною метою дій (слідчих, оперативно-розшукових, організаційних), які за умови комплексного їх застосування спрямовані на забезпечення найбільш ефективного вирішення тактичних (локальних, проміжних) завдань,

[1] Криміналістика : підручник : у 2 т. / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 1. 456 с.; Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.; Баев О. Я. Криминалистика. Лекционный курс : учеб. пособие. 4-е изд., перераб. и доп. М. : ЮСТИЦИЯ, 2017. 372 с.; Криміналістика : підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін.]. Київ : Центр учб. літ., 2015. 544 с.

[2] Коновалова В. Е. Концепция криминалистической тактики: прогнозы развития. *Актуальні проблеми криміналістики :* матеріали Міжнар. наук.-практ. конф. Харків, 2003. С. 68.

[3] Тіщенко В. В. Технологічний підхід як новаційний напрямок у розвитку криміналістичної науки. *Науковий вісник Львівської комерційної академії*. 2015. Вип. 2. С. 322–323. (Серія «Юридична»).

що виникають у певній слідчій ситуації[1]. Системи слідчих дій і тактичні операції автор розглядає не як конкурентні криміналістичні категорії, а як засоби, що доповнюють один одного та в сукупності створюють єдиний механізм отримання інформації, необхідної для розкриття, розслідування та попередження злочинних виявів[2]. Науковець доводить, що кожна тактична операція повинна мати своє чітко визначене змістове наповнення у вигляді комплексів слідчих дій та оперативно-розшукових заходів, які мали б достатньо вузьку спрямованість і забезпечували реалізацію одного тактичного (проміжного) завдання.

Отже, якщо під час розслідування виникає таке тактичне завдання, розв'язання якого шляхом проведення однієї або декількох слідчих дій є неможливим, що вимагає поєднання в одній категорії організаційних і тактичних заходів, то йдеться про розроблення тактичної операції як засобу розв'язання такого проміжного завдання. Для забезпечення методичної ролі тактичних операцій вони мають бути безпосередньо пов'язаними зі слідчою ситуацією та походити від типового тактичного завдання останньої. Саме тому назви типових тактичних операцій переважно відображають тактичне завдання розслідування, як-от: «Встановлення способу вчинення кримінального правопорушення», «Встановлення мотивів вчинення злочину», «Встановлення особи потерпілого», «Розшук особи злочинця», «Захист доказів» тощо. Утім, слушно зазначає В. А. Журавель, головним залишається не те, яку назву мають тактичні операції, а які слідчі дії та оперативно-розшукові, організаційні заходи належать до їхньої структури, на розв'язання яких завдань вони спрямовані та в якій послідовності їх виконують.

Аналіз криміналістичної літератури та дисертаційних досліджень з проблематики розслідування злочинів, що вчиняють в обстановці кіберпростору, дає підстави для висновку, що більшість науковців віддають перевагу висвітленню традиційних питань тактики проведення окремих слідчих дій. Лише деякі криміналісти визнають потребу застосування інноваційних розробок у криміналістичних методиках і пропонують комплекс/и слідчих дій та організаційних

[1] Журавель В. Системи слідчих дій та тактичні операції в структурі окремої криміналістичної методики розслідування злочинів. *Вісник АПрН України*. 2009. № 2 (57). С. 206.

[2] Там само. С. 206.

заходів. Одними з перших В. Б. Вехов, В. А. Голубєв здійснили спробу визначити програм розслідування на підставі так званих «вихідних» слідчих ситуацій розслідування комп'ютерних злочинів[1]. Автори цілком оминають увагою специфіку тактичних завдань розслідування таких злочинів. Досліджуючи методику шахрайств, вчинених із використанням мережі Інтернет, С. В. Самойлов пропонує інший підхід – докладно на прикладному рівні, уникаючи використання терміна «тактична операція», описує її з назвою «Витребування інформації від установ та організацій під час розслідування шахрайств, вчинених із використанням мережі Інтернет»[2]. У контексті організаційних засад розслідування злочинів, що пов'язані з втручанням у роботу мереж мобільного зв'язку, В. І. Пазиніч характеризує «комплекси першочергових слідчих дій та оперативно-розшукових заходів, спрямовані на встановлення особи (або групи) злочинця(ів) під час затримання злочинця в разі вчинення злочину та за недостатньої кількості інформації для обґрунтованого порушення кримінальної справи» (нині – для початку провадження)[3].

Узагальнення наявних розробок з приводу методик розслідування злочинів, вчинених у кіберпросторі, дає підстави констатувати:

1) відсутність чітко визначеної послідовності слідчих (розшукових) дій та інших заходів у пропонованих науковцями тактичних операціях;

2) відсутність взаємозв'язку між самими операціями в межах конкретного криміналістичного етапу розслідування;

3) спрямовування комплексів на розв'язання не тактичних, а стратегічних завдань, властивих усьому етапу/процесу розслідування будь-якого виду злочинів.

Отже, з метою оптимізації розслідування злочинів, вчинених у кіберпросторі, визнаємо важливість і необхідність розроблення типових тактичних операцій, структура яких відповідатиме типовим

[1] Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. П. Смагоринского. Волгоград, 2004. С. 166–173.

[2] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі Інтернет : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. С. 101–110.

[3] Пазиніч В. І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. С. 117–127.

тактичним завданням розслідування таких злочинів, сучасній практиці протидії кіберзлочинам.

Тактична операція, визнає В. Ю. Шепітько, відрізняється від звичайної сукупності слідчих, оперативних, ревізійних та інших дій такою її властивістю, як комплексність[1]. Комплексність стосується вивчення колективної динаміки, це міждисциплінарна галузь дослідження систем, які охоплюють значну кількість взаємозалежних частин[2]. Вважаємо, що в процесі розроблення тактичних операцій початкового етапу розслідування злочинів, вчинених у кіберпросторі, допустимим є визначення певних особливостей провадження слідчих (розшукових) дій. Ці особливості слід визначити задля відображення специфіки поєднання слідчих (розшукових), оперативно-розшукових та організаційних дій у типовий комплекс як засіб розв'язання типового тактичного завдання в умовах типової слідчої ситуації.

Отже, на підставі виокремлених у попередньому підрозділі типових слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі, відповідних їм тактичних завдань і загалом комплексів засобів їх розв'язання ***доцільно визначити такі типові тактичні операції початкового етапу***:

1) «Персоналізація відомостей про особу/осіб злочинця/ів»;

2) «Збирання електронних (цифрових) носіїв інформації»;

3) «Встановлення кінцевого мотиву злочинної діяльності в кіберпосторі»;

4) «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи»;

5) «Встановлення технології злочинної діяльності з використанням кіберпростору»;

6) «Матеріалізація ідеальних слідів вчинення злочину в кіберпросторі»;

7) «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі».

Схарактеризуймо ці операції в контексті їх взаємозв'язку (послідовності), внутрішньої структури (наповнення), деяких

[1] Шепитько В. Ю. Тактика расследования преступлений, совершаемых организованными группами и преступными организациями. Харьков, 2000. С. 56–57.

[2] Complexity Science – Complexity Science Complexity Science. URL: https://www.crayon.com/; https://www.complexity.org.uk (en-US).

особливостей тактики провадження їхніх компонентів, що засвідчують специфіку поєднання слідчих (розшукових) дій, оперативно-розшукових й організаційних заходів, їх зумовленість типовою слідчою ситуацією.

Тактична операція «Персоналізація відомостей про особу/осіб злочинця/ів». Однойменне тактичне завдання розслідування є першочерговим для більшості слідчих ситуацій (2.1–2.3; 3.1, 3.2). Досліджувана тактична операція передбачає такі поступові слідчі (розшукові) дії, оперативно-розшукові й організаційні заходи:

1) зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту;

3) встановлення місцезнаходження радіоелектронного засобу;

2) оформлення та відправлення запитів про витребування від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових осіб відомостей, що становлять інтерес для кримінального провадження та/або здійснення запитів щодо обміну інформацією між компетентними підрозділами правоохоронних органів іноземних держав з питань реагування на кіберзлочини каналами сектору Національного контактного пункту реагування на кіберзлочини (НПК ДКП НП України).

Зняття інформації з електронних інформаційних систем або її частини, доступ до яких не обмежується її власником, володільцем або утримувачем чи непов'язаний з подоланням системи логічного захисту, є одним з двох видів такої НС(Р)Д, як зняття інформації з електронних інформаційних систем[1]. Ця дія як компонент тактичної операції «Персоналізація відомостей про особу/осіб злочинця/ів» реалізується шляхом пошуку слідчим або інспектором кіберполіції (за

[1] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

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;

– ознака, за якою об'єднують коло осіб, що потрапляють під підозру;

– зв'язки особи, що потрапила під підозру;

– відомості, що можуть сприяти розв'язанню 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 екрану, англ. *screenshot*), 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 через використання злочинцем під час вчинення злочину закордонного сегменту Інтернет). На відповідному фаховому рівні застосовувати таке обладнання (програмні засоби) може спеціаліст, тому в абсолютній більшості випадків доручають проведення цієї НС(Р)Д інспектору кіберполіції. Якщо персоналізацію особи здійснено підчас оперативно-розшукової діяльності, то сенсу в цій дії на початковому етапі розслідування не буде. Водночас на практиці її проводять з метою отримання формальних підстав для обґрунтування подальших С(Р)Д, що вимагають погодження з прокурором або звернення до слідчого судді (обшуку за певною адресою, тимчасового доступу до документів конкретного постачальника Інтернет-послуг тощо).

Встановлення місцезнаходження радіоелектронного засобу. Ця НС(Р)Д, відповідно до ст. 268 КПК України, полягає в застосуванні технічного обладнання для локалізації місцезнаходження радіоелектронного засобу, зокрема мобільного терміналу, систем зв'язку й інших радіовипромінювальних пристроїв, активованих у мережах операторів рухомого (мобільного) зв'язку, без розкриття

змісту повідомлень, що передаються, якщо внаслідок його проведення можна встановити обставини, які мають значення для кримінального провадження. Правовою підставою проведення цієї дії є ухвала слідчого судді, однак у виняткових невідкладних випадках, пов'язаних із врятуванням життя людей і запобіганням вчиненню тяжкого або особливо тяжкого злочину (передбаченого розділами I, II, VI, VII (ст. 201, 209), IX, XIII, XIV, XV, XVII Особливої частини КК України), ця дія може бути розпочата до постановлення ухвали слідчого судді за рішенням слідчого, узгодженого з прокурором, або прокурора.

Фактично ж 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 рамках ОРС або під час перевірки первинної інформації. Зазначене положення є важливим для слідчого з позицій оптимізації процесу розслідування, адже його локальним завданням стосовно цієї НС(Р)Д є своєчасність ініціативи щодо проведення необхідної дії або заходу, і тим самим недопущення дублювання останніх.

Оформлення та відправлення запитів. Згідно з ч. 2 ст. 93 КПК України, сторона обвинувачення здійснює збирання доказів шляхом витребування й отримання від органів державної влади, органів місцевого самоврядування, підприємств, установ та організацій, службових і фізичних осіб речей, документів, відомостей, висновків експертів, висновків ревізій, актів перевірок. Із цих позицій у сучасних публікаціях пропонують певні тактичні рекомендації щодо складання слідчим запиту як одного зі способів збирання доказів. Дослідник С. В. Самойлов розглядає особливості складання таких запитів під час розслідування шахрайства, вчиненого з використанням мережі Інтернет, зокрема характеризує чинники: 1) своєчасності

запиту; 2) законності запиту; 3) переліку інформації, яку необхідно з'ясувати шляхом запиту[1].

У цьому контексті слід виокремити аспекти витребування слідчим інформації, що має значення для персоналізації відомостей про особу злочинця.

По-перше, отримані внаслідок такого запиту матеріали є так званим джерелом фактичних даних, а не «джерелом доказів». Для того щоб фактичні дані про обставини злочину були визнані доказами, їх має бути отримано в передбаченому законом порядку з визначених джерел[2]. Цими джерелами є «процесуальні джерела доказів», які чітко регламентовані в ч. 2 ст. 84 КПК України. Запити можуть бути використані з метою формування доказів, відповіді на них застосовують для обґрунтування процесуальних дій (переважно клопотання про надання тимчасового доступу до речей і документів).

По-друге, у тактичному аспекті не є суттєвим, хто складає такий запит – слідчий після внесення інформації про злочин до ЄРДР чи оперативний працівник під час перевірки оперативної інформації про злочин. Зміст інформації визначає для оперативного співробітника чи слідчого адресата такого запиту. Адресатів та зміст запитуваної інформації щодо таких запитів під час розслідування злочинів, вчинених у кіберпросторі, конкретизовано в попередньому розділі в контексті взаємодії слідчого з державними та недержавними підприємствами та установами.

Завдання щодо персоналізації відомостей про особу злочинця можна вважати розв'язаним, якщо:

– у заяві/повідомленні особи про кримінальне правопорушення міститься персоналізована заявником інформація про особу злочинця (ситуація 1.1);

– злочинця встановлено внаслідок оперативної роботи (ситуація 1.3);

– слідчий встановив анкетні дані про злочинця внаслідок здійснення таких тактичних операцій, як «Персоналізація відомостей про особу/осіб злочинця/ів» (ситуації 2.1–2.3, 3.1, 3.2) та/чи

[1] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі Інтернет : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. С. 101–110.

[2] Лук'янчиков Є. Д., Лук'янчиков Б. Є. Формування доказів у кримінальному провадженні. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2016. № 2. С. 123.

«Організація затримання злочинця» (ситуація 1.2, за відсутності інформації про діяльність особи в складі злочинної групи).

Тактична операція «Збирання електронних (цифрових) носіїв інформації». Аналогічну їй за змістом операцію з назвою «Комп'ютерні технології» вже розглянуто в дослідженні з проблем розслідування викрадень майна, вчинених із використанням комп'ютерних технологій[1]. Ця операція властива будь-якій з типових слідчих ситуацій початкового етапу розслідування злочинів, вчинених у кіберпросторі. Специфічним є лише момент її реалізації, який характеризується обов'язковістю розв'язання на цей час тактичних завдань розслідування щодо персоналізації відомостей про особу/осіб злочинця/злочинців і подолання засобів конспірації, які використовують учасники мережевої злочинної групи. Тому первинною зазначена операція стає в ситуаціях, у яких наявні персоналізовані відомості про користувача як злочинця (ситуації 1.1–1.3), для інших ситуацій вона є вторинною.

Водночас криміналістична наука постійно розширює свою теоретичну базу, зокрема з питань організації аналізованої операції і тактики проведення слідчих (розшукових) дій як її компонентів[2]. Так, 2017 року колектив вітчизняних науковців і практиків ГСУ, ДКП НП України та Державного науково-дослідного експертно-криміналістичного центру МВС України розробив та опублікував методичні рекомендації «Використання електронних (цифрових) доказів у кримінальних провадженнях»[3]. Коментоване джерело містить найбільш повні алгоритми дій слідчого задля збирання електронних (цифрових) носіїв інформації, а також тактичні прийоми та рекомендації

[1] Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ, 2009. С. 164–180.

[2] Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 222 с.; Яремчук В. О. Організація і тактика залучення спеціаліста при проведенні слідчих (розшукових) дій : монографія / за ред. В. Ю. Шепітька. Харків : Апостиль, 2015. 227 с.; Зейкан Я. П. Про недопустимі докази. Харків : Фактор, 2019. 128 с.

[3] Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

для роботи з такими доказами. Тому в межах цього дослідження уваги потребують лише окремі питання законодавчих новел.

З огляду на зміст ст. 99 КПК України, електронні (цифрові) носії інформації можуть виконувати роль документів як процесуальних джерел доказів факту чи обставин, що встановлюють під час кримінального провадження, або речових доказів як матеріальних об'єктів, що були знаряддям вчинення кримінального правопорушення, зберегли на собі його сліди або містять інші відомості, які можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження, зокрема предмети, що були об'єктом кримінально протиправних дій. Саме тому метою проведення слідчих оглядів, обшуків або тимчасових доступів до речей і документів раніше було вилучення електронних носіїв інформації, чим керувалися науковці під час розроблення тактики проведення цих дій.

Утім 16 листопада 2017 року на підставі Закону України «Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування» було доповнено ст. 168 КПК України[1]. Відповідно до цього доповнення, слідчому заборонили тимчасове вилучення електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку, крім випадків, коли їх надання разом з інформацією, що на них міститься, є необхідною умовою проведення експертного дослідження, або якщо такі об'єкти отримані внаслідок вчинення кримінального правопорушення чи є засобом або знаряддям його вчинення, а також якщо доступ до них обмежується їх власником, володільцем або утримувачем чи пов'язаний з подоланням системи логічного захисту. Слідчий або прокурор можуть здійснювати лише копіювання інформації, що міститься в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їх невід'ємних частинах, звісно, із залученням спеціаліста. За такої обставини створена копія інформації є

[1] Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування : Закон України від 16 листоп. 2017 р. № 2213-VIII. URL: https://zakon.rada.gov.ua/laws/show/2213-viii.

додатками до протоколів слідчих дій, будучи дублікатом інформації, з речового доказу отримує значення документа.

З метою використання останніх у процесі доказування на рівних умовах законодавець у ч. 4 ст. 99 КПК України запровадив норму, відповідно до якої дублікат документа (документ, виготовлений таким самим способом, як і його оригінал), а також копії інформації, що містяться в інформаційних (автоматизованих) системах, телекомунікаційних системах, інформаційно-телекомунікаційних системах, їхніх невід'ємних частинах, виготовлені слідчим, прокурором із залученням спеціаліста, суд визнаватиме як оригінал документа. Хоча таке положення є законодавчою новелою лише кримінального процесуального права, воно обґрунтоване специфікою існування електронної інформації. Адже копіювання є одним з видів обробки електронної інформації, побітове копіювання є електронною системою копіювання, яке здійснюють шляхом безпосереднього зчитування інформації біт за бітом[1].

Тому під час обшуку, огляду чи тимчасового доступу до засобів комп'ютерної техніки 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 матеріального сліду злочину не має такого показника. Слід акцентувати, що власник, володілець або утримувач комп'ютерної системи, яку досліджують, можуть застосовувати різні способи захисту від копіювання. За такої умови ідентичне копіювання буде неможливим, що обґрунтовує фізичне вилучення носія електронної інформації під час обшуку або слідчого огляду для його вивчення та подолання систем захисту в процесі проведення відповідної судової експертизи. У разі тимчасового доступу до електронних інформаційних систем або їх частин, мобільних терміналів систем зв'язку вилучення є неможливим, адже, відповідно до ч. 2 ст. 159 КПК України, здійснити цей захід забезпечення кримінального провадження можна лише шляхом зняття копії інформації, що міститься в таких електронних інформаційних системах або їх частинах, мобільних терміналах систем зв'язку, без їх вилучення.

[1] Зайцев А. П., Голубятников И. В., Мешеряков Р. В., Шелупанов А. А. Программно-аппаратные средства обеспечения информационной безопасности : учеб. пособие. М. : Машиностроение-1, 2001. С. 111.

Отже, до структури аналізованої тактичної операції належить такий комплекс дій, зумовлених локальними завданнями (у межах окремих слідчих дій):

1) погодження клопотань про провадження тимчасових доступів до речей і документів, їх провадження з метою фіксації (копіювання) інформації, що становить інтерес для кримінального провадження;

2) погодження клопотання про проведення обшуку, його здійснення з метою фіксації інформації, що становить інтерес для кримінального провадження, або з метою вилучення електронних носіїв інформації (за необхідності подолання систем логічного захисту інформації на носії);

3) слідчий огляд електронних цифрових носіїв інформації (оригінала або дубліката) з метою дослідження носіїв електронної інформації, що становить інтерес для кримінального провадження;

4) призначення судово-бухгалтерської експертизи та/або комп'ютерно-технічної експертизи, мистецтвознавчої експертизи, інших видів судових експертиз з метою дослідження носіїв електронної інформації, що становить інтерес для кримінального провадження.

Особливості тактики проведення слідчого огляду й обшуку розглянуто в численних публікаціях з методики розслідування злочинів, вчинених із використанням комп'ютерних технологій[1]. Процесуальний

[1] Аубакирова А. А. Ошибки, допускаемые в ходе следственного осмотра при расследовании преступлений, связанных с компьютерным терроризмом. *Роль науки в повышении эффективности деятельности правоохранительных органов :* материалы Междунар. наук.-практ. конф. (Алматы, 24 июня 2011 г.). Алматы, 2011. С. 266–272; Виявлення та розслідування злочинів, пов'язаних з використанням засобів доступу до банківських рахунків : метод. рек. / [В. О. Фінагеєв, С. С. Чернявський, О. Ю. Татаров та ін.]. Київ : Нац. акад. внутр. справ, 2013. 79 с.; Лисенко В. В. Використання у доказовому процесі інформації, що міститься в електронному вигляді. *Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвідомчому семінарі-нараді* / відп. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь. Київ, 2009. С. 31–35; Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 624 с.; Фролов О. П. Поняття та основні риси обшуку у формі спеціальної операції. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2. С. 318–324; Протидія кіберзлочинності : бібліогр. покажчик / уклад.: Н. А. Косенкова, Т. О. Сіроштан. 2-ге вид., доповн. Київ : Нац. акад. внутр. справ, 2014. 48 с.

порядок провадження тимчасового доступу до речей і документів схожий з виїмкою, кримінально-процесуальний інститут якої відігравав значну роль під час проведення досудового розслідування ще за часів дії КПК України 1960 року. Тому як компонент цієї тактичної операції провадження тимчасового доступу до речей і документів схоже в тактичному аспекті з численними рекомендаціями щодо провадження виїмки.

Тактична операція «Встановлення кінцевого мотиву злочинної діяльності в кіберпросторі». Розв'язання тактичного завдання щодо персоналізації відомостей про особу/осіб злочинця/ів не означає, що первинна кваліфікація події злочину відповідає дійсності (ситуації 2.3, 3.1, 3.2).

У цьому контексті в попередніх розділах роботи було порушено проблему конкуренції мотивів вчинення злочину в кіберпросторі. Передусім це стосується провадження, яке відкривають у межах реалізації матеріалів ОРС, коли в процесі оперативної роботи було встановлено ознаки готування до вчинення злочину (спроби вчинення). Для викриття злочинця та його злочинної діяльності в сучасних умовах кіберпростору слідчому недостатньо реконструювати подію злочину. Останню має бути прогнозовано, і лише після фіксації подальшої спроби вчинення злочину постає можливість цілком відтворити подію злочинів, які вчинені в минулому, встановити мотиви дій конкретного злочинця, визначити роль кожного суб'єкта, що бере участь у вчиненні злочину. Тому за умови відкриття провадження з підстав виявлення оперативним підрозділом ознак готування до вчинення злочину та після реалізації тактичної операції «Персоналізація відомостей про особу/осіб злочинця/ів» перед слідчим постає завдання щодо встановлення мотивів злочину, яке розв'язують шляхом здійснення такого комплексу дій:

1) зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача;

2) контроль за вчиненням злочину.

Зняття інформації з електронних інформаційних систем без відома її власника, володільця або утримувача передбачено ст. 264 КПК України НС(Р)Д, воно полягає в одержанні інформації, зокрема із застосуванням технічного обладнання, яка міститься в електронно-обчислювальних машинах (комп'ютерах), автоматичних системах, комп'ютерній мережі. Цю НС(Р)Д ініціює слідчий виключно в кримінальному провадженні щодо тяжких або особливо тяжких

злочинів, її проводять на підставі дозволу слідчого судді на втручання в приватне спілкування.

Проведення цієї дії потребує наявності спеціальних знань у галузі інформаційних технологій. Таким спеціалістом нині є інспектор кіберполіції, який за допомогою програмних і технічних засобів призначених для подолання обмежень доступу до електронної інформації, встановлених власником певної електронної інформаційної системи, отримує доступ до електронної інформації в конкретній системі, розшифровує, обробляє, систематизує цю інформацію та копіює її. Увесь документальний обіг щодо її проведення здійснюють з дотриманням режиму секретності. З аналізованого матеріалу вбачається, що в понад половині випадків проведення цієї НСРД протокол проведення дії складає слідчий, при цьому в протоколі зазначають про залучення до її проведення вповноваженого слідчим працівника оперативного підрозділу.

Контроль за вчиненням злочину. Законодавець не сформулював визначення такої самостійної НС(Р)Д, як контроль за вчиненням злочину, обмежившись лише вказівкою на його чотири форми: 1) контрольовану поставку; 2) контрольовану й оперативну закупки; 3) спеціальний слідчий експеримент; 4) імітування обстановки злочину (ст. 271 КПК України). Це пов'язано зі складністю зазначеної дії, адже кожній із форм притаманна низка специфічних організаційних, тактичних й управлінських прийомів.

Акцентуємо, що оперативні підрозділи для документування кінцевої мети злочинної діяльності особи завжди застосовували контрольовану поставку, контрольовану й оперативну закупку товарів, предметів і речовин як заходи ОРД, однак сьогодні їх можна реалізувати лише через контроль за вчиненням злочину як самостійну НС(Р)Д, що проводиться виключно в кримінальному провадженні (згідно з ч. 2 ст. 246 КПК України). Також у ст. 8 Закону України «Про оперативно-розшукову діяльність» ідеться про ще один специфічний ОРЗ – операцію з контрольованого вчинення діянь, передбачених ст. 305, 307, 309, 311, 318, 321, 364-1, 365-1, 368, 368-3, 368-4, 369, 369 КК України. Норма щодо порядку проведення такої операції (як і стосовно інших ОРЗ) є бланкетною, однак до положень КПК України вона відсилає лише щодо порядку проведення операції з контрольованого вчинення корупційного діяння. Однак, у КПК Україні не використано словосполучення «контрольоване вчинення

корупційного діяння» або «операція контрольоване вчинення злочину», а отже, на відповідні ОРЗ не поширюється дія КПК України. Тому результати їх проведення оперативними підрозділами не можна використовувати як докази не лише щодо корупційного злочину, а й стосовно будь-якого іншого. Тож, трьом із чотирьох форм НС(Р)Д притаманні близькі за змістом оперативно-розшукові заходи (контрольованої поставки; контрольованої та оперативної закупки; імітування обстановки злочину).

Аналіз матеріалів практики розслідування злочинів, вчинених у кіберпросторі, дає підстави стверджувати, що найчастіше слідчі з метою встановлення кінцевого мотиву злочинної діяльності в кіберпросторі проводять контроль за вчиненням злочину у формі спеціального слідчого експерименту. Спеціальний слідчий експеримент полягає у створенні слідчим й оперативним підрозділом відповідних умов в обстановці, максимально наближеній до реальної, з метою перевірки реальних намірів певної особи, у діях якої вбачаються ознаки тяжкого чи особливо тяжкого злочину, спостереження за її поведінкою та прийняттям нею рішень щодо вчинення злочину[1]. Під час проведення спеціального слідчого експерименту в умовах невизначеності кінцевого мотиву злочинної діяльності конкретної особи слідчий або оперативний працівник за його дорученням у кіберпросторі як обстановці вчинення злочину створює штучні умови інформаційного характеру, виявляючи зацікавленість у певному результаті дій злочинця. Фактично спеціальний слідчий експеримент стає найефективнішим засобом розслідування всіх класифікаційних підгруп злочинів, що вчиняють у кіберпросторі, за винятком злочинів, які порушують встановлений порядок обігу певних речей, для розслідування яких ефективно використовують контрольовану поставку, контрольовану й оперативну закупки.

Згідно зі ст. 273 КПК України, під час спеціального слідчого експерименту є можливість використовувати імітаційні засоби

[1] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

(готівкові кошти, платіжні картки), тому в теоретичному аспекті науковці акцентують на проблемі визначення критеріїв для розмежування спеціального слідчого експерименту й імітування обстановки злочину. Зокрема, М. В. Багрій таким критерієм вважає встановлення особи злочинця, спеціальний слідчий експеримент здійснюють щодо конкретної особи, імітування – як встановленої, так і невстановленої особи[1]; В. А. Динту – мету й обстановку проведення цих форм контролю за вчиненням злочину[2]. Дослідник М. Л. Грібов слушно зауважує про умовні критерії розмежування зазначених форм контролю за вчиненням злочину. Автор констатує наявність низки спільних рис між спеціальним слідчим експериментом й імітуванням обстановки злочину як різних форм контролю за вчиненням злочину та доводить необґрунтованість їх розмежування в чинному кримінальному процесуальному законодавстві[3]. Саме тому на практиці під час розслідування конкретного кримінального провадження визначення форми контролю за вчиненням злочину є суб'єктивним, ініціатор цієї НС(Р)Д самостійно встановлює ключові в організаційному плані аспекти її проведення, ті, що переважають за кількісним критерієм, що й слугує підставою для віднесення запланованої ним дії до певної форми контролю за вчиненням злочину.

Рішення про проведення контролю за вчиненням злочину приймає виключно прокурор. В організаційному аспекті слідчий або оперативний підрозділ (за дорученням слідчого) складає план або декілька планів під час етапного проведення НС(Р)Д, де визначають мету проведення певного (тактичного або оперативно-розшукового) заходу, учасників, порядок здійснення, імітаційні засоби, які будуть використовувати. Спеціальний слідчий експеримент є неоднорідним, наприклад, може бути поєднаним чи не поєднаним з іншими НС(Р)Д (наприклад, з аудіо-, відеоконтролем особи та/або місця, спостереженням за особою, річчю або місцем). Також контроль за

[1] Багрій М. В. Імітування обстановки злочину: поняття, зміст, місце у системі негласних слідчих розшукових дій. *Порівняльно-аналітичне право.* 2015. № 4. С. 371–374.

[2] Динту В. А. Спеціальний слідчий експеримент як форма контролю за вчиненням злочину. *Порівняльно-аналітичне право*. 2014. № 4. С. 184–186.

[3] Грібов М. Л. Розмежування спеціального слідчого експерименту й імітування обстановки злочину. *Науковий вісник Національної академії внутрішніх спр*ав. 2016. № 4 (101). С. 64–73.

вчиненням злочину може бути як внутрішнім (на території України), так й транзитним (на території інших держав, за домовленістю між правоохоронними органами, на підставі чинних міжнародних договорів України)[294, с. 72][1].

Тактична операція «Встановлення та подолання засобів конспірації, які використовують учасники мережевої злочинної групи». Це тактичне завдання є типовим за наявності інформації про діяльність встановленої/невстановленої особи в складі організованої злочинної групи (ситуації 3.1–3.3). На момент реалізації аналізованої операції персоналізація відомостей про особу/осіб злочинця/ів є закономірною, адже злочинця встановлено шляхом первинної перевірки інформації про злочин. До структури операції «Встановлення та подолання засобів конспірації, які використовують учасники злочинної групи» належать такі дії:

1) контроль за вчиненням злочину;

2) здійснення за дорученням слідчого оперативним підрозділом оперативного (ініціативного) пошуку з метою встановлення характеру дій особи, що становить інтерес для кримінального провадження;

3) зняття інформації з транспортних телекомунікаційних мереж (електронних інформаційних систем) конкретного абонента.

Контроль за вчиненням злочину з метою подолання засобів конспірації в слідчій практиці типово проводять у формах контрольованої поставки, контрольованої та оперативної закупок (як самостійної форми).

Згідно з п. 1.12 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, контрольована поставка полягає в організації та здійсненні слідчим й оперативним підрозділом контролю за переміщенням (перевезенням, пересиланням, передачею, ввезенням, вивезенням з України чи транзитним переміщенням її територією) товарів, предметів і речовин, зокрема заборонених до обігу, з метою виявлення ознак злочину та фіксації фактичних даних про протиправні діяння осіб, відповідальність за які передбачена

[1] Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018 540 с

КК України. З огляду на міжнародний, транснаціональний характер злочинної діяльності в кіберпросторі, контрольована поставка здійснюється з метою визначення складу злочинної групи, учасники якої застосовують засоби конспірації, що заважає визначити їх безпосередню участь (роль) під час вчинення злочинів, пов'язаних з обстановкою кіберпростору (під час придбання через Інтернет зброї, вибухівки, радіоактивних речовин, культурних цінностей, коштовностей). Ця дія згодом зумовлює повідомлення компетентних органів інших держав про проходження їхньою територією предметів посягання в разі вчинення конвенційних кіберзлочинів, організацію подальшої співпраці з ними задля викриття в повному обсязі діяльності мережевої злочинної групи.

Оперативна закупка полягає в імітації придбання або отримання, зокрема безоплатного, у фізичних і юридичних осіб незалежно від форм власності товару, обіг якого обмежений чи заборонений чинним законодавством, з метою викриття і документування факту вчинення злочину й особи, яка його вчинила. Очевидним видається критерій розмежування контрольованої та оперативної закупок – предмет їх здійснення: для першої це товар, який знаходиться у вільному обігу; для другої – товар, обіг якого обмежений чи заборонений законодавством. Тому закріплення законодавцем двох форм як однієї не є цілком виправданим, адже реалізується лише одна з форм – при розслідуванні злочинів у кіберпросторі нею типово виступає оперативна закупка. Реалізацію цієї НСР(Д) здебільшого доручають оперативним підрозділам. Однак, слідчі беруть активну участь на етапі планування, можуть щоденно чи поетапно контролювати результати їх фіксації оперативним підрозділом і відповідно корегувати тактику подальших слідчих (розшукових) дій.

Щодо стадії підготовки зауважимо, що слідчий, оцінюючи слідчу ситуацію, конкретизуючи завдання щодо встановлення та подолання засобів конспірації, приймає рішення про проведення цієї НС(Р)Д, перед прокурором ініціює та обґрунтовує фактичними матеріалами справи необхідність її проведення. Слідчому потрібно зважати на те, чи проводили контрольовану поставку або оперативну закупку (згідно з положеннями ст. 4, 5 Закону України «Про заходи протидії незаконному обігу наркотичних засобів, психотропних

речовин і прекурсорів та зловживанню ними»)[1]. За таких обставин немає сенсу їх дублювати аналогічною дією як формою контролю за вчиненням злочину. Результати останньої будуть нівельовані, адже злочинні наслідки наступного епізоду злочинної діяльності стають передбачуваними, отже, перед слідчим взагалі не постає завдання щодо подолання засобів конспірації.

Засоби тактики проведення цих форм НС(Р)Д достатньо широко представлені в теорії оперативно-розшукової діяльності (О. А. Антоненко, М. Л. Грібов, І. І. Демідов, К. Г. Костенко та інші). Б. І. Бараненко, О. В. Бочкова та К. А. Гусєва акцентують увагу на значенні для тактики проведення всіх НС(Р)Д специфіки й стану навколишнього соціального та фізичного середовища цих предметів, яке формується, зокрема, з комунікативних зв'язків, побуту, інших елементів життєдіяльності, утворюють відповідну інформаційну та соціальну сферу проведення НС(Р)Д[2]. Із цих позицій зазначимо, що для злочинів, що вчинені в кіберпросторі, останній є обов'язковою умовою існування предмета посягання, а отже, проведення контрольованої поставки або оперативної закупки супроводжує проведення іншої НС(Р)Д – зняття інформації з транспортних телекомунікаційних мереж. Застосування саме такого комплексу НС(Р)Д надає можливість слідчому розширити часові межі документального супроводження вчинення злочину, зафіксувати не лише факт придбання, отримання або переміщення забороненого чи обмеженого в цивільному обігу товару, а й обставини його створення, використання, копіювання, поширення в інший спосіб (шляхом застосування певної комп'ютерної технології) тощо.

Зняття інформації з транспортних телекомунікаційних мереж – це НС(Р)Д, що передбачена ст. 263 КПК України та полягає в негласному проведенні із застосуванням відповідних технічних

[1] Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними : Закон України від 15 лют. 1995 р. № 62/95-ВР. URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80.

[2] Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ : навч.-практ. посіб. / [Б. І. Бараненко, О. В. Бочковий, М. Г. Вербенський та ін.] ; за ред. М. Г. Вербенського, Б. І. Бараненка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2014. 416 с.

засобів спостереження, відбору та фіксації змісту інформації, яка передається особою, а також одержанні, перетворенні й фіксації різних видів сигналів, що передаються каналами зв'язку (знаки, сигнали, письмовий текст, зображення, звуки, повідомлення будь-якого виду)[1].

Аналіз матеріалів судово-слідчої практики розслідування злочинів, вчинених у кіберпросторі, дає змогу вважати зняття інформації з каналів зв'язку найпоширенішою формою зняття інформації з транспортних телекомунікаційних мереж. Ця дія полягає в негласному одержанні, перетворенні та фіксації із застосуванням технічних засобів, зокрема встановлених на транспортних телекомунікаційних мережах, у відповідній формі різних видів сигналів, які передають каналами зв'язку мережі Інтернет. За тактичної та організаційної схожості цієї дії зі зняттям інформації в електронних інформаційних системах, слід акцентувати на їх відмінності: під час зняття інформації в електронних інформаційних системах ініціатор має доступ до всієї інформації в системі, а за зняття інформації з каналів зв'язку – лише до тієї інформації, яку передають таким каналом.

Тактична операція «Встановлення технології злочинної діяльності з використанням кіберпростору». У змісті слідчих ситуацій, що характеризуються браком будь-яких відомостей про особу злочинця (ситуації 3.1–3.3) наявна так звана «фактична складова інформації про злочин»[2]. Факт доцільно розглядати як встановлені за допомогою доказів знання про подію кримінального правопорушення й інші обставини, які мають значення для кримінального провадження[3]. Ця фактична складова щодо злочинів, вчинених у

[1] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

[2] Волчецкая Т. С. Криминалистическая ситуалогия : монография / под ред. Н. П. Яблокова. М. ; Калининград : Калинингр. ун-т, 1997. 248 с.

[3] Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : монографія. Івано-Франківськ : Супрун В. П., 2017. С. 146.

кіберпросторі, отримана внаслідок негласної роботи оперативних підрозділів й оформлена згідно з вимогами слідчого до матеріалів перевірки/провадження за ОРС, дає змогу слідчому дійти висновку про наявність технології злочинної діяльності. Цим і зумовлено завдання слідчого щодо встановлення технології злочинної діяльності групи осіб. Однойменна тактична операція має складовими такі дії:

1) аудіо-, відеоконтроль особи та/або місця;

2) спостереження за особою, річчю або місцем / дослідженням публічно недоступних місць, житла або іншого володіння особи;

3) виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації (за певних умов).

Аудіо-, відеоконтроль особи та/або місця (ст. 260 і 270 КПК України) в розслідуванні злочинів, вчинених у кіберпросторі, застосовують у комплексі зі *спостереженням за особою, річчю або місцем* (ст. 269 КПК України) та у випадках, коли є необхідність встановлення технічних пристроїв аудіо-, відеоконтролю в приватному помешканні, з *дослідженням публічно недоступних місць, житла або іншого володіння особи* (ст. 267 КПК України).

Аудіо-, відеоконтроль особи – це передбачена ст. 260 КПК України НС(Р)Д, що полягає в застосуванні технічних засобів аудіо- та відеофіксації певної особи кримінального провадження для фіксування розмов або інших звуків, рухів, дій, пов'язаних з її діяльністю в будь-якому місці (суспільне місце чи приватне, доступне або не доступне для сторонніх осіб), з метою отримання фактичних даних, необхідних для певного кримінального провадження. Аудіо-, відеоконтроль місця як НС(Р)Д передбачена ст. 270 КПК України та полягає в здійсненні прихованої фіксації відомостей за допомогою засобів аудіо-, відеозапису всередині публічно доступних місць без відома їхнього власника або присутніх у цьому місці осіб за наявності відомостей про те, що розмови, поведінка осіб у цьому місці, а також інші події, що там відбуваються, можуть містити інформацію, яка має значення для кримінального провадження. Зазначені НС(Р)Д мають аналоги у формі оперативно-розшукових заходів. У більшості аналізованих кримінальних проваджень аудіо-, відеоконтроль особи та/або місця мають форму НС(Р)Д. Їх виконують тільки на підставі ухвали слідчого судді та в разі вчинення тяжких та особливо тяжких злочинів, тому, за гіпотетичної умови їх виконання на етапі

оперативної розробки, слідчому досить складно буде знайти аргументи для повторної їх ініціалізації під час досудового розслідування. Особливий технічний характер навичок, необхідних для реалізації цих НС(Р)Д, зумовлює залучення слідчим до їх проведення працівників оперативних підрозділів, які, з огляду на традиційні форми їх діяльності, приступають до виконання відповідного доручення слідчого.

Об'єктом аудіо-, відеоконтролю особи або місця в аналізованій тактичній операції є розмови або дії певної особи, зміст яких дає підстави для висновку про технологію злочинної діяльності з використанням кіберпростору. Прикладом є кримінальне провадження щодо колекціонера предметів старовини, який для пошуку потенційних покупців антикваріату зареєструвався на інтернет-аукціоні[1]. 26 лютого 2015 року за допомогою послуг поштового зв'язку «Укрпошта» він відправив поштове відправлення на К. до м. Москви Російської Федерації. У відправленні містилися колекційні нагрудні знаки. 27 лютого за місцем його мешкання працівники СБ України провели обшук, під час якого він добровільно видав предмети колекціонування та поштові квитанції. Він знав, що медалі й інші антикварні речі відправляти за кордон можна лише з дозволу відповідних органів, як і переміщати їх за кордон в інший спосіб. Проведенню обшуку передували такі НС(Р)Д, як аудіоконтроль особи та візуальне спостереження за особою, під час яких було встановлено джерела отримання предметів колекціонування та способи їх відправлення замовникові.

Слідчі ситуації, у яких бракує інформації про особу злочинця, мають динамічний характер, що полягає в постійному розвитку ситуації, переході з одного стану в інший[2]. Щодо злочинів, вчинених у кіберпросторі, цим ситуаціям притаманне виявлення злочину в момент його продовження. Аудіо-, відеоконтроль особи та/або місця в комплексі із спостереженням за особою, річчю або місцем забезпечує пізнання злочинної діяльності в кіберепросторі в реальному часі.

[1] Вирок Бабушкінського районного суду м. Дніпропетровська від 24 черв. 2015 р. Провадження № 1-кс/200/4990/15. URL: http://reyestr.court.gov.ua/Review/45932252.

[2] Драпкин Л. Я. Общая характеристика следственных ситуаций. *Следственная ситуация :* сб. науч. тр. М. : Всесоюз. ин-т по изучению причин и разраб. мер предупреждения преступности, 1985. С. 15–16.

Результат такого пізнання закріплюють у формі протоколу про проведення відповідної НС(Р)Д, у якому вповноважена на це особа відображає зміст розмов, інших звуків, рухів, дій певної особи або в певному місці. За результатами аналізу матеріалів судово-слідчої практики розслідування злочинів, вчинених у кіберпросторі, можна стверджувати, що абсолютна більшість таких протоколів підписана працівником оперативного підрозділу, адже реалізаціється комплекс НС(Р)Д за дорученням слідчого групою оперативних, що діють у складі слідчо-оперативної групи.

Спостереження за особою, річчю або місцем полягає у візуальному спостереженні за певними річчю або місцем слідчим або уповноваженою особою для фіксації її переміщення, контактів з нею певних осіб, подій у певному місці для перевірки відомостей під час досудового розслідування тяжкого або особливо тяжкого злочину чи застосування з цією метою спеціальних технічних засобів для спостереження[1].

Тактична складова діяльності слідчого з реалізації цієї дії концентрується в межах підготовчого етапу її проведення. Слідчому потрібно визначити мету й необхідність проведення спостереження за особою, річчю або місцем, конкретизувати виконавців цієї дії, іноді визначити технічні засоби, які необхідно використовувати для цього.

Під час розслідування злочинів, вчинених у кіберпросторі, цю НС(Р)Д проводять з метою встановлення технології злочинної діяльності з використанням кіберпростору й одночасно задля забезпечення безпеки реалізації інших НС(Р)Д, виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації. Об'єктом візуального спостереження переважно є особи, спостереження за якими надає можливість визначити їх обізнаність у злочинній діяльності групи осіб, роль в організованій групи, а також місця з чітко визначеними

[1] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5 URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

територіальними межами, де найчастіше розміщено техніку, яку використовують злочинці для вчинення злочину.

Спеціальні принципи оперативно-розшукової діяльності відображають тактичні засади проведення цієї НС(Р)Д, зокрема, це безперервність, мобільність, достовірність і повнота відображення фактів[1]. Фактично ж за умови їх дотримання під час виконання спостереження, підтвердження результатів останнього сукупністю інших доказів, протокол щодо проведення спостереження слідчий використовує в процесі доказування.

Виконання спеціального завдання з розкриття злочинної діяльності організованої групи чи злочинної організації як НС(Р)Д регламентовано ст. 272 КПК України[2]. Спеціальне завдання виконують на підставі постанови слідчого, погодженої з керівником органу досудового розслідування, або постанови прокурора зі збереженням у таємниці достовірних відомостей про особу й не потребує дозволу слідчого судді. Фактично виконання такого завдання полягає в проникненні в злочинну групу або організацію штатного або позаштатного негласного співробітника, або наявності члена організованого злочинного формування, який на конфіденційних засадах співробітничає з уповноваженими оперативними підрозділами[3]. Конфіденційне співробітництво регламентовано ст. 275 КПК України.

---

[1] Халілев Р. А. Система принципів оперативно-розшукової політики з протидії злочинності на ґрунті етноконфесійних суперечностей. *Учені записки Таврійського національного університету ім. В. І. Вернадського.* 2010. Т. 23 (62). № 1. 2010. С. 328–336. (Серія «Юридичні науки»); Дудник Л. І. Становлення і розвиток оперативно-розшукової діяльності. *Національний вісник Державної податкової служби України.* 2005. № 3 (30). С. 231–238. (Серія «Економіка і право»).

[2] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 14/1042/516/1199/936/1687/5 URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

[3] Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. С. 75.

Тактика виконання спеціального завдання шляхом проникнення в кримінальне середовище зумовлена конкретною слідчою ситуацією, що склалася на момент організації такої НС(Р)Д, видом організованої групи, до якої впроваджується виконавець, становить алгоритм оперативно-розшукових заходів, які виконують у чіткій послідовності й дають змогу розв'язати поставлене слідчим локальне завдання розслідування. Аналіз практики оперативних підрозділів засвідчує, що для проникнення в кримінальне мережеве середовище правоохоронні органи широко використовують «мережі-пастки» чи «сайти-пастки», які іметують привабливу з погляду злочинця інформацію, забезпечують функцію негласного захоплення (копіювання) ідентифікаційних реквізитів його відвідувача[1]. Вони також сприяють налагодженню «довірливих» стосунків із членами злочинної групи, дозволяють документувати її діяльність, що виходить за межі цього опублікування результатів дослідження.

Аналіз матеріалів кримінальних проваджень щодо розслідування злочинів, вчинених у кіберпросторі, дає змогу констатувати, що тактична операція «Встановлення технології злочинної діяльності з використанням кіберпростору» може бути реалізована й на наступному етапі розслідування за умови встановлення конфіденційного співробітництва принаймні з одним можливим підозрюваним. Саме ця операція буде забезпечувати повноцінність у тактичному аспекті наступного етапу розслідування злочинів, вчинених у кіберпросторі, та, з огляду на гнучкість мережевої організованої групи, відсутність централізованої системи контролю її діяльності, реалізація її надасть змогу встановити особистісний склад організованої групи й епізоди злочинної діяльності окремих її членів.

Тактична операція «Матеріалізація ідеальних слідів вчинення злочину в кіберпросторі». У традиційній криміналістичній концепції слідоутворення подія злочину та його механізм, з одного боку, відображаються на матеріальних об'єктах (предметах, речах), а з іншого – у свідомості людини, створюючи численні «сліди-

[1] Путренко А. М. Мережа Інтернет як об'єкт дослідження при здійсненні оперативно-розшукової діяльності. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф. (17 берез. 2010 р.). Київ : Наук.-вид. відділ НА СБ України, 2010. С. 143–146

відбитки»[1]. Із цього приводу Д. В. Затенацький стверджує, що сліди пам'яті – це тимчасові зв'язки в корі головного мозку, що слугують фізіологічною основою запам'ятовування й відтворення[2]. На думку науковця, виникнення цих зв'язків обумовлене реальними зв'язками предметів і явищ, зокрема їхніми зв'язками в просторі й часі, відносинами подібності й відмінності між ними тощо. Такі відображення матеріальної дійсності в пам'яті людини називають ідеальними слідами (слідами пам'яті)[3].

На початковому етапі розслідування складові тактичної операції «Матеріалізація ідеальних слідів вчинення злочину в кіберпросторі» зумовлена потребою слідчого в перевірці первинної інформації про подію злочину й особу злочинця (із заяви та повідомлення про кримінальне правопорушення), а також встановлення обставин вчинення кримінального правопорушення. Тому до аналізованого комплексу належать численні опитування й допити потерпілих і свідків (службовців, посадових осіб, які проводили перевірку та виявили ознаки злочину; осіб, що обіймають керівні посади, рядових працівників установи-жертви, технічних співробітників, осіб, що входять у коло спілкування підозрюваної особи, очевидців злочину), пред'явлення для впізнання.

З одного боку, одержання інформації слідчим передбачає необхідність комунікації (соціальної взаємодії, спілкування) з охопленням таких функціональних напрямів, як встановлення психологічного контакту, керування спілкуванням, здійснення

[1] Тимошенко П. Ю., Салтевский М. В., Жариков Ю. Ф. Теория и практика использования следов памяти (идеальных отображений) в расследовании преступлений / отв. ред. Р. С. Белкин. Киев : Укр. акад. внутр. дел, 1991. С. 6; Затенацький Д. В. Ідеальні сліди в криміналістиці (технікокриміналістичні та тактичні прийоми їх актуалізації) : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2010. С. 7.

[2] Затенацький Д. В. Ідеальні сліди в криміналістиці (технікокриміналістичні та тактичні прийоми їх актуалізації) : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2010. С. 11.

[3] Шепітько В. Ю. Криміналістика : енцикл. слов. (укр.-рос. і рос.-укр.) : 1500 термінів. / за ред. В. Я. Тація. Харків : Право, 2001. С. 323; Белкин Р. С. Криминалистика: проблемы сегодняшнего дня. *Злободневные вопросы российской криминалистики.* М. : НОРМА–ИНФРА-М, 2001. С. 64. Васильев В. Л. Юридическая психология : учеб. пособие. 5-е изд., доп. и перераб. СПб : Питер, 2005. С. 440.

психологічного впливу, одержання слідчим інформації[1], з іншого, з огляду на широке коло осіб, що підлягають допиту як свідки, – одночасне обрання послідовності опитування та допитування осіб. У зв'язку із цим, перш ніж визначатися з тактичними аспектами проведення допиту конкретного потерпілого чи свідка, слідчий має відповісти на питання: чи призведе попереднє опитування особи до протидії розслідуванню з її боку, чи буде наслідком допиту розголошення таємниці слідства. Аналіз матеріалів слідчо-судової практики розслідування злочинів, вчинених у кіберпросторі, дає змогу визначити чинники, які зумовлюють певну послідовність опитування/допитування свідків, потерпілих у таких провадженнях.

По-перше, особу, яка в процесі вчинення злочину могла стати об'єктом інформаційно-психологічному впливу, перед проведенням допиту бажано опитати задля визначення ступеня такого негативного впливу й обрання відповідної тактики її допиту. Інформаційно-психологічний вплив – це вплив різними методами (навіюванням або переконанням) на свідомість особи та населення з метою внесення змін у їхню поведінку та/або свідомість[2]. Удало для цього використовують кіберпростір. Стосовно цього Є. Д. Скулиш, В. М. Петрик вважають, що важлива особливість такого впливу на індивідуальну свідомість полягає в тому, що його як загрозу може не помічати й не усвідомлювати особа, передусім якщо призводить до зміни установок (орієнтацій) людини[3]. Установка людини – це сформовані під впливом пропаганди, виховання, досвіду стійкі знання, почуття та мотиви, що формують певне ставлення до ідейних, політичних і суспільних явищ у реальній дійсності. Злочини в кіберпросторі, що вчинені з антидержавно-політичних або ідейних мотивів, часто супроводжуються саме інформаційно-психологічним впливом на відповідні установки потерпілих або свідків.

[1] Коновалова В. О., Шепітько В. Ю. Юридична психологія : підручник. 2-ге вид., переробл. і доповн. Харків : Право, 2008. С. 78.; Лукашевич В. Г. Криминалистическая теория общения: постановка проблемы, методика исследования, перспективы использования: Монографія. К. : Издательство Украинской академии внутренних дел, 1993. 194 с.

[2] Скулиш Є. Д., Петрик В. М. Сутність інформаційно-психологічного впливу. *Актуальні проблеми управління інформаційною безпекою* : зб. матеріалів наук.-практ. конф. (Київ, 17 берез. 2010 р.). Київ : Наук.-вид. відділ НА СБ України, 2010. С. 165–169.

[3] Там само. С. 168.

Непроцесуальне спілкування з останніми має шанс нівелювати наслідки інформаційно-психологічного впливу, пропаганди й забезпечити ефективність допиту такого свідка чи потерпілого.

По-друге, черговість допитування осіб, як і характер допитів, обумовлені ступенем усвідомленості свідків та потерпілих, що ґрунтується на професійній компетентності, досвіді, колі повноважень, кваліфікаційних вимогах під час виконання певних видів робіт[1]. Першочергово допиту підлягають особи, які є заявниками про вчинене кримінальне правопорушення та/або виконують функції забезпечення інформаційної безпеки, зовнішнього чи внутрішнього фінансового або технічного контролю юридичної особи, що використовувалася під час вчинення злочину або постраждала від нього. Проведення попереднього їх опитування часто призводить до розголошення цими особами таємниці слідства (повідомлення іншим співробітникам, керівництву про причини та зміст спілкування зі слідчим).

По-третє, у контексті розслідування злочинів, вчинених у кіберпросторі, важливе значення має допит спеціаліста, що брав участь у провадженні інших слідчих (розшукових) дій, та експерта. Науковці М. Г. Щербаковський та Є. Г. Коваленко зазначають про наявність «роз'яснення та доповнення до висновку експерта», яке слід тлумачити як його показання, у яких висвітлено зміст і значення відповідних положень висновку, а саме обраної методики дослідження, причин відмови від інших методик або методів дослідження об'єкта, використання в експертизі науково-технічних засобів, їхніх метрологічних характеристик, величини похибки вимірювання; особливості підготовки об'єктів до дослідження, умови відбору експериментальних зразків, порівняння, кількісних і якісних змін після проведення досліджень; виявлені ідентифікаційні та діагностичні ознаки; критерії оцінювання ознак, яких експерт дотримувався під час формування проміжних й остаточних висновків; окремих термінів і визначень, які є у висновку; можливих суперечностей між дослідницькою частиною (зокрема додатками до висновку) і висновками; причини відмови експерта від дачі висновку або обмеженого вирішення

[1] Журавель В. А. Специфика предмета допроса потерпевшего при расследовании отдельных видов преступлений. *Проблемы социалистической законности*. 1983. Вып. 12. С. 122–125.

окремих питань[1]. Аналіз матеріалів практики розслідування досліджуваної категорії злочинів дає змогу визнати, що близько 80 % проваджень містять допити спеціалістів й експертів. Спеціалістів, що брали участь у слідчих (розшукових) діях, допитують майже одразу після проведення, щодо НС(Р)Д – після скасування відповідного грифу секретності; судових експертів допитують після отримання висновку з метою оцінювання його достовірності.

Детальний аналіз тактики допиту свідків і потерпілих, а також тактичних особливостей його проведення у справах щодо окремих категорій злочинів, вчинених у кіберпросторі, здійснено в численних дисертаціях і наукових публікаціях (А. І. Анапольської, І. М. Горбаньова, В. В. Лисенка, В. Д. Поливанюка, В. Ю. Шепітька та ін.)[2] Тому немає сенсу деталізовано розглядати це питання в нашому дослідженні.

Тактична операція «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі». У цьому комплексі слідчих та організаційних дій фізичному затриманню особи злочинця передують такі дії: 1) здійснення за дорученням слідчого оперативним підрозділом заходів оперативного (ініціативного) пошуку з метою встановлення місцеперебування особи; 2) попереднє опитування особи, яку підозрюють; 3) погодження клопотання про

[1] Коваленко Є. Г. Наукові засади кримінально-процесуального доказування : монографія. Київ : Юрінком Інтер, 2011. С. 371; Щербаковський М. Г. Призначення та провадження судових експертиз. Харків : Фактор, 2011. С. 237.

[2] Шепітько В. Ю. Допит : наук.-практ. посіб. Харків : Крим-Арт, 1998. 214 с.; Анапольська А. І. Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2010. 224 с.; Горбаньов І. М. Особливості проведення допитів окремих категорій свідків при розслідуванні незаконного розповсюдження комп'ютерних програм. *Вісник Академії адвокатури України*. 2005. Вип. 2. С. 114–118; Лисенко В. В. Особливості допиту головного бухгалтера (керівника підприємства) у справах про ухилення від сплати податків. *Вісник прокуратури.* 2007. № 10. С. 109–114; Поливанюк В. Д. Тактичні особливості проведення допиту при розслідуванні злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Теоретичні та практичні проблеми організації досудового слідства* : матеріали Всеукр. наук.-практ. конф. (Запоріжжя, 20–21 трав. 2005 р.) : у 2 ч. Запоріжжя : Юрид. ін-т МВС України, 2005. Ч. 1. С. 79–81.

застосування запобіжного заходу щодо цієї особи, затримання; 4) повідомлення про підозру й допит підозрюваного.

Основною умовою реалізації цієї тактичної операції локально на початковому етапі розслідування є персоналізація відомостей про особу злочинця шляхом здійснення попередньої перевірки інформації, отриманої з гласного джерела (ситуація 1.2) або реалізація в повному обсязі тактичної операції «Забезпечення процесу збирання доказів» (ситуації 1.1, 1.3).

Ця тактична операція передбачає розв'язання й іншого супутнього тактичного завдання розслідування – це визначення зайнятої підозрюваним у кримінальному провадженні позиції. Оскільки зі ставленням підозрюваного до розслідування з криміналістичних позицій корегується слідча ситуація наступного етапу розслідування кримінального провадження, то проведення опитування та/або допитування підозрюваної особи, реєстрація в ЄРДР інформації щодо висунення першої законної та обґрунтованої підозри резюмують ступінь розв'язання тактичних завдань початкового етапу розслідування конкретного кримінального провадження. Дослідник Г. А. Матусовський у цьому контексті використовує такий критерій, як «стан розслідування», трактуючи його як упорядковану сукупність установлених у процесі розслідування обставин, оцінювану слідчим як положення, що сприяє провадженню в справі або створює перешкоди, тому потребує прийняття відповідних слідчих рішень для використання (розвитку) сприятливої ситуації або вирішення (розрядження) ситуації несприятливої (складної, конфліктної). Аналіз матеріалів кримінальних проваджень щодо злочинів, вчинених у кіберпросторі, дає підстави для висновку, що внаслідок реалізації такої операції слідчий зможе визначити слідчу ситуацію наступного етапу розслідування як сприятливу або несприятливу.

Стосовно розслідування злочинів, вчинених у кіберпросторі, *сприятливій ситуації наступного етапу розслідування* притаманна повнота виконання тактичних завдань початкового етапу розслідування та конкретизація зайнятих кожним із підозрюваних у кримінальному провадженні позицій. На нашу думку, однаково поширеними є два її різновиди: 1) неускладнена сприятлива ситуація, що складається за умови збігу позицій підозрюваних осіб і співпраці їх зі слідством; 2) ускладнена сприятлива ситуація, що наявна за

умови розбіжності позицій декількох підозрюваних. У тактичному аспекті ця ситуація вимагатиме виконання нових тактичних завдань розслідування, як-от: подолання протидії розслідуванню; усунення суперечностей між джерелами доказового значення; забезпечення збереження вже отриманих джерел доказів. Засобами виконання цих завдань розслідування стають однойменні тактичні операції, які в різній варіації можуть передбачати комплекс дій:

– повідомлення підозрюваного про проведення НС(Р)Д (використання фактора «раптовості» на наступному етапі розслідування);

– комплекс одночасних допитів декількох осіб (з метою подолання суперечностей у показаннях);

– комплекс слідчих експериментів (з кожним виконавцем злочину);

– допити свідків (понятих і спеціалістів);

– подальші організаційні заходи, спрямовані на збирання матеріалів, що характеризують особу підозрюваного;

– додаткові допити підозрюваних.

Несприятливій ситуації розслідування притаманна невизначеність зайнятої підозрюваним(ми) у кримінальному провадженні позиції, у зв'язку із його (їх) фізичною відсутністю під час фактичного продовження розслідування у формі «спеціального досудового розслідування», регламентованого главою 24-1 КПК України[1]. Спеціальне досудове розслідування є одночасно формою спеціального кримінального провадження поряд зі спеціальним судовим провадженням й екстраординарною формою досудового розслідування, застосування якої пов'язане з необхідністю забезпечити виконання завдань кримінального провадження в умовах чинення протидії розслідуванню з боку підозрюваного у формі ухилення від кримінальної відповідальності шляхом переховування від органів слідства та суду[2]. За

[1] Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини : Закон України від 7 жовт. 2014 р. № 1689-VII. URL: https://zakon.rada.gov.ua/go/1689-18.

[2] Шевчишен А. В. Поняття спеціального досудового розслідування (in absentia) та його функціональне призначення у кримінальних провадженнях щодо корупційних злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг. *Вісник кримінального судочинства*. 2017. № 2. С. 128.

таких умов тактичне завдання щодо затримання й отримання свідчень злочинця, що діє в кіберпросторі, розв'язує слідчий уже на наступному етапі розслідування, відповідно, однойменна тактична операція є типовою у несприятливій ситуації наступного етапу розслідування.

Ситуації наступного етапу розслідування злочинів, вчинених у кіберпросторі, та відповідні тактичні операції можна розглядати лише як орієнтири для слідчого, адже слідчу ситуацію в конкретному кримінальному провадженні зумовлює зміст обставин, викладених в акті повідомлення конкретній особі про підозру. Оскільки останній є початковим моментом реалізації прокурором функції обвинувачення, то момент складання повідомлення особі про підозру засвідчує наявність у провадженні достатніх доказів вини конкретної особи у вчиненні злочину, що й підкреслює особливу значущість у криміналістичній методиці розслідування злочинів, вчинених у кіберпросторі, слідчих ситуацій і відповідних тактичних операцій початкового етапу їх розслідування.

Отже, оптимізація розслідування вказаних злочинів потребує:

а) впровадження таких нових тактичних операцій як «Персоналізація відомостей про особу/осіб злочинця/ів», «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»; внутрішня їх структура та особливості тактики провадження їхніх компонентів визначається в контексті поєднання слідчих та негласних слідчих (розшукових) дій задля досягнення однойменних тактичних завдань розслідування;

б) вдосконалення розроблених тактичних операцій у частині оновлення структурування таких тактичних операцій: «Збирання електронних (цифрових) носіїв інформації», «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі» та «Матеріалізація ідеальних слідів вчинення злочинів у кіберпросторі». Взаємозв'язок усіх тактичних операцій зумовлений характером інформації про особу злочинця, відповідно слідчою ситуацією.

РОЗДІЛ 5
ВИКОРИСТАННЯ СПЕЦІАЛЬНИХ ЗНАНЬ У РОЗСЛІДУВАННІ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

5.1. Спеціальні знання та специфіка залучення спеціаліста під час розслідування злочинів, вчинених у кіберпросторі

Високий рівень технічного забезпечення вчинення злочинів у кіберпросторі та конспірації злочинцем такої діяльності актуалізують необхідність залучення суб'єкта спеціальних знань у процес їх розслідування. Утім специфіку його залучення не можна визначити поза реаліями сучасної трансформації правового інституту «використання спеціальних знань у кримінальному судочинстві» та відповідно конкретизації на теоретичному рівні позицій щодо змісту спеціальних знань і форм їх використання, з чого й варто розпочати аналіз питання.

Категорію «спеціальні знання» більшість науковців тлумачать крізь призму способу набуття останніх, що загалом є виправданим. Однак, намагаючись сформулювати авторські визначення цієї категорії, криміналісти та процесуалісти присвоюють їй додаткові ознаки. Так, В. М. Галкін трактує спеціальні пізнання як знання, набуті внаслідок фахової освіти чи професійного досвіду[1]. На думку О. О. Ейсмана, такі знання не є загальнодоступними та загальновідомими, вони не мають масового поширення; це знання, якими володіє обмежене коло спеціалістів, причому очевидно, що глибокі знання в галузі, наприклад, фізики, є в цьому значенні спеціальними для біолога[2]. Дослідники В. І. Гончаренко та З. М. Соколовський акцентують на їх глибині та фаховості[3]. Науковець В. Д. Юрчишин спеціальними знаннями вважає сукупність

[1] Галкин В. М. Средства доказывания в советском уголовном процессе. М. : ВНИИСЭ, 1968. Ч. 2. С. 8.

[2] Эйсман А. А. Заключение эксперта. Структура и научное обоснование. М. Юрид. лит., 1967. С. 91

[3] Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. Киев : Вища шк., 1980. С. 114; Соколовский З. М. Понятия специальных знаний. К вопросу об основаниях назначения экспертизы. *Криминалистика и судебная экспертиза.* 1969. Вып. 6. С. 202–204.

науково обґрунтованих знань у галузі науки, техніки, мистецтва та ремесла певної особи (спеціаліста) в межах будь-якої професії, які відповідно до норм кримінально-процесуального законодавства є необхідними для повного, усебічного, об'єктивного встановлення обставин, що належать до предмета доказування та виконання інших завдань кримінального процесу[1].

Наукова полеміка щодо трактування цього терміна стала на заваді формуванню єдиного підходу до розв'язання проблеми віднесення юридичної галузі знань до категорії «спеціальних», а слідчого, судді та прокурора – до суб'єктів спеціальних знань. Аналіз літературних джерел засвідчує наявність у літературі двох підходів до вирішення цього питання.

Перший підхід полягає в тому, що юридичні знання належать до спеціальних. Таку позицію обґрунтовано в роботах В. Д. Арсеньєва, В. Г. Заболоцького, Н. І. Клименко, В. М. Реваки, Б. В. Романюка та деяких інших криміналістів[2]. Науковець З. М. Соколовський доводить, що спеціальні знання – це будь-які знання, серед них й окремі правові, проте лише у вузькій (спеціальній) галузі науки, техніки, мистецтва та ремесла, отримані в процесі фахової підготовки та професійної діяльності. На думку цього автора, правові знання для слідчого, які він здобув як юрист, є фаховими, а група окремих правових знань про проведення слідчих дій, доказування, застосування криміналістичної техніки тощо є спеціальними[3]. Обґрунтовуючи такий підхід, науковці посилаються на теоретичні

[1] Юрчишин В. Д. Висновок експерта як джерело доказів у кримінальному процесі України : дис. … канд. юрид. наук : 12.00.09. Івано-Франківськ, 2007. С. 44.

[2] Арсеньев В. Д., Заблоцкий В. Г. Использование специальных знаний при установлении фактических обстоятельств уголовного дела. Красноярск : Краснояр. ун-т, 1986. С. 4–5; Клименко Н. И. Криминалистика как наука : монография. Киев : Правник, 1997. С. 21-22; Ревака В. М. Форми використання спеціальних пізнань у досудовому провадженні : дис. … канд. юрид. наук : 12.00.09. Харків, 2006. 180 с.; Романюк Ю. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : дис. … канд. юрид. наук : 12.00.09. Київ, 2002. 217 с.

[3] Соколовский З. М. Понятия специальных знаний. К вопросу об основаниях назначения экспертизы. *Криминалистика и судебная экспертиза.* 1969. Вып. 6. С. 202–204.

концепції, зокрема значення терміна «спеціалізація», зміст кримінального процесуального доказування або пізнавальної діяльності слідчого.

Другий підхід є діаметрально протилежним і полягає в тому, що юридичні знання не належать до спеціальних. Його обстоюють у своїх працях А. В. Дулов, О. О. Ейсман, М. М. Тертишник, В. І. Шиканов, М. Г. Щербаковський та ін.[1]. Згідно із цією позицією, спеціальними знаннями слідчий чи суддя володіти не може, такі знання слід відрізняти від професійних юридичних. У зазначеному контексті В. І. Шиканов зауважував про можливість використовувати термін «спеціальні пізнання», який у кримінальному процесі буде контрадикторним поняттю «спеціальне знання». Учений застосовує це поняття для позначення будь-якої можливої сукупності знань (практичного досвіду, навичок), за винятком загальновідомих, а також пізнань у галузі права[2]. Ми також поділяємо цей підхід як такий, що відповідає змісту чинних норм кримінального процесуального

[1] Дулов А. В. Права и обязанности участников судебной экспертизы. Минск : МВССПО БССР, 1962. С. 5-39; Зуев Е. И. О понятии специальных познаний в уголовном процессе. *Вопросы теории криминалистики и судебной экспертизы :* материалы науч. конф. (Москва, декабрь 1969 г.). М., 1969. Вып. 1. С. 73–76; Лисиченко В. К., Циркаль В. В. Использование специальных знаний в следственной и судебной практике : учеб. пособие. Киев : КГУ, 1987. 100 с.; Надгорный Г. М. Гносеологические аспекты понятия «специальные знания». *Криминалистика и судебная экспертиза.* 1980. Вып. 21. С. 41–42; Салтевский М. В. Проблема соотношения специальных и профессиональных знаний, используемых при производстве следственных действий. *Становление и развитие органов внутренних дел Украинской ССР.* Киев : КВШ МВД СССР, 1973. С. 134–135; Тертышник В. М. Нетрадиционные способы и формы собирания и исследования доказательств при расследовании преступлений. Харьков : ХИВД, 1994. С. 3; Шиканов В. И. Актуальные вопросы уголовного судопроизводства и криминалистики в условиях современного научно-технического прогресса. Иркутск : Восточ.-Сибир. кн. изд-во, 1978. 190 с.; Щербаковский М. Г., Кравченко А. А. Применение специальных знаний при раскрытии и расследовании преступлений. Харьков : Ун-т внутр. дел, 1999. С. 5–9.

[2] Шиканов В. И. Актуальные вопросы уголовного судопроизводства и криминалистики в условиях современного технического прогресса. Иркутск : Изд-во ИГУ, 1978. С. 25–26.

законодавства. Згідно з положеннями ч. 1 ст. 69, ч. 1 ст. 71 та ч. 6 ст. 95 КПК України, головним критерієм визначення процесуальних форм застосування спеціальних знань у кримінальному процесі є саме суб'єкти їх застосування, а саме:

– спеціаліст – у формах консультації і технічної допомоги під час досудового розслідування та судового розгляду;

– судовий експерт – у формі залучення до проведення судової експертизи.

Законодавець висвітлює значення поняття спеціальних знань у ст. 101 КПК України, яка регламентує право кожної сторони кримінального провадження надати суду висновок експерта, що ґрунтується на його наукових, технічних або інших спеціальних знаннях. Згідно з ч. 1 ст. 242 КПК України, заборонено проведення експертизи для з'ясування питань права, що унеможливлює віднесення юридичних знань у теорії використання спеціальних знань до категорії «спеціальних».

Отже, поняття «спеціальні знання» ми тлумачимо як наукові, технічні або інші з позицій кримінального процесуального закону неюридичні знання, отримані внаслідок спеціальної підготовки та практики суб'єктом, процесуальний статус якого визначається як експерт або прирівнюється до спеціаліста.

У дослідженнях з тематики класифікації форм використання спеціальних знань у кримінальному провадженні науковці дедалі частіше відходять від традиційного розподілу таких форм на процесуальні (залучення спеціалістів до участі в слідчих діях і проведення судових експертиз) та непроцесуальні (проведення доекспертних досліджень, ревізій, консультативно-довідкова допомога спеціаліста)[1]. Слід віддати перевагу розгляду лише прямо регламентованих КПК України форм, класифікація яких ґрунтується або на критеріях суб'єктного складу їхніх застосовувачів, або

[1] Грамович Г. И. Тактика использования специальных знаний в раскрытии и расследовании преступлений : учеб. пособие. Минск : Минск. высш. шк. МВД СССР, 1987. 66 с.; Коваленко Е. Г. Использование экспертных знаний в деятельности органов внутренних дел : учеб. пособие. Киев : Киев. высш. шк. МВД СССР им. Ф. Э. Дзержинского, 1990. 87 с.; Щербаковский М. Г., Кравченко А. А. Применение специальных знаний при раскрытии и расследовании преступлений. Харьков : Ун-т внутр. дел, 1999. 78 с.

процесуальних способів їхньої реалізації, або мети їх застосування[1]. Так, В. М. Ревака за способом реалізації спеціальних знань виокремлює п'ять форм:

1) дослідження (передекспертне, зокрема ревізія, й експертне);

2) техніко-прикладна форма (застосування спеціальних знань під час провадження процесуальних дій);

3) оперативно-розшукова форма;

4) знаково-лінгвістична форма (переклад);

5) консультаційна форма[2].

Дослідники В. К. Лисиченко та В. В. Циркаль аргументують недопустимість використання спеціальних знань у непроцесуальній формі[3]. Продовжуючи цю думку, Ю. В. Романюк стверджує, що консультування слідчого зі спеціалістом варто вважати одним зі способів набуття слідчим певних спеціальних знань, розглядаючи слідчого суб'єктом спеціальних знань, класифікує форми використання спеціальних знань за суб'єктами: слідчий, спеціаліст, експерт[4]. Нині ця позиція вже суперечить зазначеній вище нормі

[1] Бондар А. В. Форми використання спеціальних знань під час розслідування знищення або пошкодження майна. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 (104). С. 46–58; Воробей О. В. Використання спеціальних знань і призначення окремих видів судових експертиз під час розслідування кримінальних правопорушень, пов'язаних з діяльністю конвертаційних центрів. *Криміналістичний вісник.* 2017. № 1 (27). С. 154–160; Лазебний А. М. Використання спеціальних знань при розслідуванні кримінальних правопорушень проти громадського порядку : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2016. 20 с.; Лазебний А. М. Роль спеціальних знань у кримінальному судочинстві України. *Міжнародний юридичний вісник.* 2016. Вип. 2 (4). С. 23–29; Садчікова К. А. Використання спеціальних знань на стадії досудового розслідування (процесуальний аспект) : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017. 233 с.

[2] Ревака В. М. Форми використання спеціальних пізнань у досудовому провадженні : дис. … канд. юрид. наук : 12.00.09. Харків, 2006. 180 с.

[3] Лисиченко В. К. Использование данных естественных и технических наук в следственной и судебной практике : учеб. пособие. Киев : Вища шк., 1979. С. 20–24, 26.

[4] Романюк Ю. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : дис. … канд. юрид. наук : 12.00.09. Київ, 2002. 217 с.

кримінального процесуального закону.

Процесуалісти акцентують на меті використання спеціальних знань[1]. Так, В. М. Тертишник виокремлює чотири форми використання знань спеціалістом, серед них:

а) безпосередньо практична діяльність у:

– підготовці, організації та проведенні слідчих (розшукових) дій;

– виявленні, закріпленні, вилученні доказів, зразків об'єктів для експертного дослідження, а в разі необхідності – їх огляді й дослідженні;

б) методична – з питань науково-практичних прийомів і методів організації та проведення слідчих (розшукових) дій, виявлення й роботи з доказами;

в) технічна – у використанні науково-технічних засобів під час проведення слідчих (розшукових) дій, необхідних для виявлення, закріплення, вилучення, огляду й дослідження речових доказів;

г) консультативна – полягає в усних роз'ясненнях, довідках зі спеціальних питань, що можуть виникнути або виникають під час підготовки, проведення гласних і негласних слідчих (розшукових) дій, роботі з доказами та процесуальному оформленні їх результатів [2].

Науковець А. М. Лазебний, використовуючи категорію «мета використання спеціальних знань», характеризує в методиці розслідування кримінальних правопорушень проти громадської безпеки дві інші форми: пошук і фіксація та призначення й проведення експертиз[3]. На думку автора, кожна з них передбачає використання знань спеціалістів під час здійснення окремих слідчих (розшукових) дій.

Вивчення спеціальної криміналістичної літератури та сучасної слідчої практики дає підстави стверджувати, що нині неможливо проводити досудове розслідування, під час якого не було б

[1] Садчікова К. А. Використання спеціальних знань на стадії досудового розслідування (процесуальний аспект) : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017.С. 3; Тертишник В. М. Кримінально-процесуальне право України : підручник. 4-те вид., доповн. і переробл. Київ : А.С.К., 2003. С. 691

[2] Тертишник В. М. Кримінально-процесуальне право України : підручник. 4-те вид., доповн. і переробл. Київ : А.С.К., 2003. С. 691.

[3] Лазебний А. М. Використання спеціальних знань при розслідуванні кримінальних правопорушень проти громадського порядку : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2016. С. 10.

використано спеціальні знання хоча б в одній прямо передбаченій КПК України формі їх реалізації. У теорії кримінального процесу або криміналістики вони мають різні умовні назви, однак спосіб їх реалізації, передбачений процесуальним законодавством, від цього не змінюється.

Отже, враховуючи положення чинного КПК України, вважаємо, що можна виокремити три процесуальні форми використання спеціальних знань під час досудового розслідування:

1) залучення спеціаліста для надання письмової консультації;

2) залучення спеціаліста для надання безпосередньої технічної допомоги під час процесуальних дій;

3) залучення експерта для проведення судової експертизи й виконання обов'язків судового експерта.

Передчасною видається відмова деяких науковців від непроцесуальних форм використання спеціальних знань. Адже високим рівнем апробованості слідчою практикою доведена ефективність таких непроцесуальних форм використання спеціальних знань, як:

1) усне консультування слідчого зі спеціалістом (зазначають про необхідність використання 90 % анкетованих працівників правоохоронних органів);

2) залучення спеціаліста під час перевірки оперативної інформації про злочини, що вчинені або готуються (50 % анкетованих).

Повсякденна практика розслідування злочинів, вчинених у кіберпросторі, засвідчує наявність безлічі організаційних і тактичних питань використання таких форм спеціальних знань.

Залучення спеціаліста для надання письмової консультації (згідно зі ст. 71 КПК України). Консультації традиційно можуть бути письмовими й усними, однак процесуальною є лише письмова форма консультації (ч. 2 ст. 105 чинного КПК України регламентує процесуальний спосіб надавання консультації спеціаліста – це письмове пояснення спеціаліста, який брав участь у проведенні відповідної процесуальної дії, що є додатком до протоколу такої дії).

Нормою ч. 6 ст. 95 КПК України закріплено можливість визнання судом висновку або думки особи, яка дає показання, що ґрунтуються на її спеціальних знаннях, доказом. Однак ні письмові, ні усні показання спеціаліста, що були надані слідчому, не будуть

належати до показань як джерела доказів. Для оцінки їх як доказу вони мають відповідати вимогам ст. 101 КПК України – тобто ґрунтуватися на спеціальних знаннях експерта, що надав відповідний висновок. Тож, з огляду на зміст ч. 8 ст. 95 КПК України, слідчий, прокурор можуть отримати від спеціаліста за його згодою пояснення, що не будуть джерелом доказів. Метою їх отримання може бути консультування; такі пояснення будуть мати тактичне значення, їх братимуть до уваги під час формування версій, підтверджуватимуть або спростовуватимуть шляхом проведення судових експертиз та інших слідчих дій[1].

Вивчення матеріалів слідчої практики дає підстави для висновку, що у справах щодо злочинів, вчинених у кіберпросторі, письмові пояснення спеціаліста є додатковим способом підтвердження джерела формування такого доказу, як документ – електронний носій інформації. В абсолютній більшості проваджень пояснення надають штатні працівники кіберполіції, які є фахівцями з інформаційних технологій або електроніки й телекомунікацій, і в процесуальному статусі спеціаліста були залучені під час проведення огляду місця події. У письмовому поясненні такий спеціаліст описує методи так званого експрес-аналізу (процес встановлення фактичних даних, що мають значення для конкретного факту правопорушення); методи вилучення (копіювання) та збереження нетрадиційних (цифрових) слідів злочину.

Залучення спеціаліста для надання безпосередньої технічної допомоги. Відповідно до ст. 71 КПК України, спеціаліст залучається під час проведення процесуальної дії для фотографування, складення схем, планів, креслень, відбору зразків для проведення експертизи тощо. Специфіка цієї форми полягає в тому, що її реалізація слідчим фактично дає змогу оформити в процесуальне джерело доказів результат залучення в кримінальне провадження спеціаліста як суб'єкта спеціальних знань. Можливо, саме тому, визначаючи специфіку цієї форми використання спеціальних знань, експерти-

[1] Ківалов С. В., Міщенко С. М., Захарченко В. Ю. Кримінальний процесуальний кодекс : наук.-практ. комент. Харків : Одіссей, 2013. С. 205-206.

практики називають цей формат роботи «взаємодією слідчого та спеціаліста в кримінальних провадженнях»[1].

У документі як джерелі доказів у значенні ст. 99 КПК України спеціаліст утілює свої спеціальні знання, зокрема через:

1) створення матеріалів фотозйомки, звукозапису, відеозапису й інших носіїв інформації (стосовно досліджуваної категорії злочинів під час огляду чи обшуку спеціаліст найчастіше створює копії комп'ютерної інформації на спеціально підготовленому для цього електронному носії);

2) постановку з дозволу слідчого питань, що відображаються в протоколах слідчих (розшукових) дій (актуально з позицій психолога, педагога, лікаря, спеціаліста економічного фаху);

3) подання зауважень щодо протоколів процесуальних дій, чим акцентує увагу учасників процесу на обставинах й особливостях речей і документів, що стосуються відповідної сфери спеціальних знань.

Для надання технічної допомоги під час розслідування злочинів, вчинених у кіберпросторі, в абсолютній більшості обшуків і тимчасових доступів до речей та документів (99 %) залучають спеціаліста з інформаційних технологій та/або електроніки й телекомунікацій разом з інспектором/техніком-криміналістом; близько 20 % допитів і слідчих оглядів проходять із залученням спеціаліста економічного профілю («фінанси, банківська справа та страхування», «підприємництво, торгівля та біржова діяльність», які є співробітниками національних експертних установ МВС, СБ або Міністерства юстиції України). Специфіка основного злочину в злочинній сукупності зрідка є підставою для залучення спеціалістів вужчого профілю, зокрема:

– спеціаліста в роботі з банківським комп'ютерним обладнанням, системного адміністратора, системного оператора;

– спеціаліста у сфері мережевих технологій та систем зв'язку (за умови використання для дистанційного передання даних каналів електрозв'язку);

[1] Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. С. 78

– іншої категорії спеціалістів (бухгалтер, економіст, інженер-електрик, спеціаліст супутникових систем зв'язку, оператор стільникових, пейджингових, інтернет-мереж тощо).

До 2015 року функцією експертної служби МВС України було визнано участь спеціалістів в оперативно-розшукових заходах, слідчих та інших процесуальних діях, що знаходилися у сфері управління МВС України, зокрема й Національної поліції[1]. У підрозділах Експертної служби були чергові експерти при органі поліції, яких залучали як спеціалістів-криміналістів до проведення не тільки оглядів місця події, а й інших слідчих (розшукових) дій; експертів лабораторій комп'ютерно-технічної експертизи залучали також як спеціалістів за вимогою слідчого.

Після реорганізації Експертної служби в листопаді 2015 року, відповідно до оновленого Положення про Експертну службу МВС України[2], основною функцією служби стало проведення експертизи, забезпечення залучення працівників Експертної служби МВС у досудове розслідування та судовий розгляд стали другорядною функцією, а техніко-криміналістичне забезпечення проведення слідчих (розшукових) дій, згідно з Інструкцією про порядок залучення працівників органів досудового розслідування поліції та Експертної служби МВС України як спеціалістів для участі в проведенні огляду місця події[3], стали здійснювати тільки у форматі роботи спеціаліста Експертної служби в складі спеціалізованої пересувної лабораторії.

Тому задля належного техніко-криміналістичного супроводження кримінального провадження під час реорганізації

[1] Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 9 серп. 2012 р. № 691 (втратив чинність на підставі наказу МВС України від 3 листоп. 2015 р. № 1343). URL: https://zakon.rada.gov.ua/laws/show/z1541-12.

[2] Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 3 листоп. 2015 р. № 1343. URL: https://zakon.rada.gov.ua/laws/show/z1390-15.

[3] Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події : наказ МВС України від 3 листоп. 2015 р. № 1339. URL: https://zakon.rada.gov.ua/laws/show/z1392-15?find=1&text=%F1%E5%EA%F2%EE%F0#w11.

структури органів досудового розслідування 2017 року на рівні ГСУ було організовано діяльність слідчих-криміналістів, а на рівні слідчого відділу територіального органу поліції – інспекторів-криміналістів (техніків-криміналістів або, в окремих випадках, секторів техніко-криміналістичного забезпечення слідчих дій) (п. 4 Положення про органи досудового розслідування Національної поліції України)[1].

У справах щодо злочинів, вчинених у кіберпросторі, з метою техніко-криміналістичного забезпечення проведення слідчих оглядів, оглядів місця події, обшуків і тимчасових доступів до речей та документів переважно залучають інспекторів-криміналістів, старших інспекторів-криміналістів, техніків-криміналістів або керівника сектору техніко-криміналістичного забезпечення слідчого відділу. Будучи наділеними правами спеціаліста, вони технічно допомагають слідчому в збиранні (виявленні, фіксації та вилученні) традиційних слідів злочину, використовуючи техніко-криміналістичні, технічні, інженерно-технологічні й інші спеціальні знання, а також практичні навички застосування відповідних техніко-криміналістичних засобів і прийомів. Результати роботи спеціаліста, що не були занесені або не були додані як додаток до протоколу слідчої (розшукової) дії, не мають доказового значення (навіть за умови відображення їх у формі письмових пояснень до протоколів процесуальної дії). Працівники ж Експертної служби МВС у складі спеціалізованої пересувної лабораторії залучаються як спеціалісти до проведення оглядів та обшуків стосовно досліджуваної категорії злочинів зрідка. Результати аналізу матеріалів практики засвідчують, що лише за умови розслідування злочинів, що викликали значний суспільний резонанс, або якщо провадження процесуальних дій здійснюють у зв'язку із запитом про міжнародну правову допомогу.

Спеціаліст з інформаційних технологій та/або електроніки й телекомунікацій, що залучається під час проведення процесуальних дій, нині є штатним працівником кіберполіції (управління інформаційних технологій та програмування), а процесуальним

[1] Про організацію діяльності органів досудового розслідування Національної поліції України : наказ МВС України від 6 лип. 2017 р. № 570. URL: https://zakon.rada.gov.ua/laws/show/z0918-17?find=1&text=%EA%F0%E8%EC%B3%ED %E0%EB%B3%F1%F2#w136.

способом його залучення стало письмове доручення слідчого, прокурора згідно з процесуальним порядком, передбаченим для взаємодії слідчого зі співробітником оперативного підрозділу (ст. 41 КПК України). На жаль, на практиці слідчі (50 % аналізованого матеріалу) цілком передають свої повноваження щодо здійснення слідчої (розшукової) дії такому суб'єкту. Останній зобов'язаний на виконання письмового доручення слідчого про проведення слідчих (розшукових) і негласних слідчих (розшукових) дій (згідно наказу МВС України від 7 лип. 2017 р. № 575; п. 9 Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами НП України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні), тому фактично їх проводить, що не цілком відповідає процесуальному статусу спеціаліста.

КПК України прямо не містить заборон щодо процесуальних дій, у яких залучення спеціаліста є неможливим. Отже, застереження деяких учених щодо участі спеціаліста під час НС(Р)Д не мають жодного юридичного підґрунтя. Залучення спеціаліста є правом слідчого, прокурора, а не їхнім обов'язком. Тому з дотриманням режиму секретності (спеціаліст повинен мати допуск до державної таємниці відповідної форми) під час проведення НС(Р)Д та відповідно до специфіки питань її проведення, складності та її змісту, що потребують залучення спеціальних знань, слідчий і прокурор самостійно приймають рішення про можливість залучення до НС(Р)Д спеціаліста відповідного фаху та кваліфікації.

У цьому контексті слід з'ясувати питання про правомірність надання співробітнику оперативного підрозділу, якому доручено провести, наприклад, НС(Р)Д, процесуального статусу спеціаліста. Згідно з п. 4.13 Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні, як спеціаліст може бути запрошений співробітник (працівник) органу, якому слідчим доручено проведення негласної слідчої (розшукової) дії, що володіє спеціальними знаннями та навичками застосування технічних або інших засобів і може надавати консультації слідчому, прокурору в процесі дослідження матеріалів про результати проведення негласної слідчої (розшукової)

дії[1]. Однак, з огляду на структуру КПК України, спеціаліст входить до категорії «інші учасники кримінального провадження»; відповідно до принципу неупередженості процесуальної діяльності, спеціаліст не може належати до жодної зі сторін кримінального провадження. Співробітник оперативного підрозділу – це «сторона обвинувачення», тому процесуальний закон засвідчує хибність думки з приводу повного доручення спеціалісту – співробітнику оперативного підрозділу проведення НС(Р)Д. На нашу думку, доручаючи згідно зі ст. 41 КПК України проведення будь-якої слідчої (розшукової) дії, зокрема й негласної, оперативному підрозділу, слідчий чи прокурор за необхідності окремо мають приймати рішення про залучення іншого учасника кримінального провадження з процесуальним статусом спеціаліста.

Досліджуючи зміст діяльності з проведення НС(Р)Д, використання їхніх результатів у кримінальному провадженні, С. С. Кудінов виокремив такі напрями використання спеціалістами спеціальних знань у зв'язку з проведенням НС(Р)Д:

а) для їх підготовки (пов'язано з обранням найсприятливіших умов для проведення НС(Р)Д (час, місце), підготовкою або виготовленням технічних, імітаційних засобів, визначенням кола учасників, їх добором й інструктажем);

б) безпосередньо під час їх проведення (розглянуто як вчинення конкретних дій, застосування тактичних прийомів проведення; наприклад, розкриття та запечатування спеціалістом кореспонденції, участь у здійсненні візуального спостереження);

в) для фіксації, оформлення отриманих результатів та їх збереження (полягає у врахуванні та використанні рекомендацій щодо роботи з окремими предметами, речовинами, вилученні слідів, речових доказів, зокрема забезпечення належних умов їх зберігання до передання прокурору);

[1] Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації Державної прикордонної служби України, Міністерства фінансів України, Міністерства юстиції України від 16 листоп. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

г) проведення досліджень отриманих матеріалів (полягає в їх використанні або врахуванні безпосередньо під час дії, наприклад, виявлення та фіксація позначок предмета контрольованої поставки; виявлення, фіксація та збереження негласно отриманих зразків хімічних речовин)[1].

Спеціалістами в класичному значенні їхнього статусу як типових учасників НС(Р)Д, що проводять у справах щодо злочинів, вчинених у кіберпросторі, ми вважаємо співробітників і працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України (ІСТЕ СБ України). Відповідно до відомчої інструкції[2], їх залучають для технічної допомоги слідчі СБ України, переважно під час розслідування злочинів, вчинених у кіберпросторі з антидержавно-політичних мотивів.

Залучення спеціаліста для надання усної консультації. У процесуальному законі немає згадок про отримання усних консультацій спеціаліста під час досудового розслідування; усні консультації та роз'яснення спеціаліста законодавець регламентує лише стосовно стадії судового розгляду (у ст. 360 КПК України). Ефективність цієї непроцесуальної форми використання спеціальних знань з метою подальшого залучення експерта для проведення судової експертизи не викликає сумніву в жодного практика. Такі усні консультації проводять здебільшого з керівниками й експертами (за погодженням із керівником) лабораторій експертних служб, зокрема:

– лабораторій комп'ютерно-технічних і телекомунікаційних досліджень;
– лабораторій досліджень у сфері інформаційних технологій;
– лабораторій економічних досліджень.

Залучення спеціаліста під час перевірки оперативної інформації про злочини, що вчинені або готуються. Процесуальні

[1] Кудінов С. С. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України.* 2014. Т. 11. № 3 (31). С. 154–161.

[2] Про затвердження Інструкції про участь співробітників та працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України як спеціалістів в кримінальному провадженні : наказ СБ України від 19 берез. 2016 р. № 138. URL: https://zakon.rada.gov.ua/laws/show/z0564-16?lang=ru.

підстави для залучення оперативними співробітниками до участі в проведенні ОРЗ спеціалістів не виокремлено. Лише в деяких законах є згадки про можливість на договірних засадах використовувати допомогу кваліфікованих спеціалістів й експертів, зокрема іноземців, з будь-яких установ, організацій, контрольних і фінансових органів для забезпечення оперативно-розшукової діяльності (ч. 1 ст. 17 Закону України «Про Національне антикорупційне бюро України», ст. 13 Закону України «Про боротьбу з тероризмом»). У зв'язку із регламентованою в КПК України можливістю використання результатів оперативно-розшукової діяльності як джерел доказів, вважаємо залучення спеціалістів під час перевірки оперативної інформації про злочини, що вчинені або готуються, непроцесуальною формою використання спеціальних знань.

Практика перевірки оперативної інформації про досліджувану категорію злочинів засвідчує, що залучення осіб, які володіють спеціальними технічними знаннями, для підготовки ОРЗ та їх проведення в низці випадків є обов'язковою передумовою ефективності проведення їх оперативними підрозділами. Напрями використання допомоги спеціаліста є аналогічними з проведенням слідчих (розшукових) дій, зокрема й негласних.

Отже, специфіка залучення спеціаліста під час розслідування злочинів, вчинених у кіберпросторі, визначається через нормативно окреслене коло повноважень останнього та спосіб його залучення.

5.2. Специфіка залучення експерта для проведення судової експертизи під час розслідування злочинів, вчинених у кіберпросторі

Сутність експертизи полягає в тому, що експерт самостійно на підставі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо досліджує надані йому об'єкти, явища й процеси з метою надання висновку з питань, що є або будуть предметом судового розгляду[1]. У спеціальній літературі експертним дослідженням вважають «вивчення обізнаною особою наданих їй об'єктів і

[1] Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. *Відомості Верховної Ради України.* 1994. № 28. Ст. 232.

матеріалів справи, виявлення, аналіз або порівняння притаманних їм властивостей та ознак із застосуванням відповідних способів, методик і технічних засобів, оцінка й формулювання на підставі спеціальних знань висновків у вигляді відповідей на поставлені питання»[1].

Законодавець 2017 року шляхом внесення змін до КПК України змінив традиційну процедуру призначення експертизи слідчим: для залучення в кримінальне провадження судового експерта необхідно було звернення слідчого до слідчого судді, а підставою її проведення стала ухвала про доручення проведення судової експертизи. У цій процедурі невизначеними лишилися чимало організаційних аспектів її виконання.

По-перше, не всі ухвали слідчих суддів містили роз'яснення для експерта з приводу звернення в подальшому за всіма організаційними питаннями щодо її виконання до слідчого чи прокурора. Організація комунікації слідчого з експертом через слідчого суддю необґрунтовано подовжувала часові межі для проведення експертизи.

По-друге, ініціювання проведення судової експертизи одночасно слідчим і стороною захисту могло призвести до неможливості отримання доступу одним з експертів до об'єктів, що підлягають дослідженню. Адже останні вже на підставі іншої ухвали або договору були передані стороною процесу на інше дослідження. Водночас не завжди стороною, яка перша звернулася до слідчого судді з клопотання про проведення експертизи, була сторона обвинувачення.

По-третє, виключення слідчим суддею з ухвали питань, поставлених слідчим у клопотанні, фактично позбавляло можливості отримати на них відповіді від суб'єкта спеціальних знань, адже не було механізму оскарження такої ухвали; причиною цієї ситуації могла бути некомпетентність слідчого судді в означеній сфері.

По-четверте, слідчий суддя як суб'єкт прийняття рішення про проведення будь-якої експертизи не мав можливості перевірити на стадії розгляду клопотання факт, який був основною причиною відповідних процесуальних змін – чи не спрямовано відповідне клопотання на затягування досудового розслідування або зловживання своїми процесуальними правами.

[1] Лисиченко В. К., Циркаль В. В. Использование специальных знаний в следственной и судебной практике : учеб. пособие. Киев : КГУ, 1987. С. 19–20.

По-п'яте, за умови, якщо судова експертиза знаходиться на виконанні в експерта, а вповноважена особа приймала рішення про закриття кримінального провадження, поставала проблема необхідності доведення дослідження до кінця. Фактично виконання такої ухвали необґрунтовано збільшувало завантаженість експертної установи, адже ухвала залишалася обов'язковою для виконання експертом.

Тож в умовах браку часу та механізмів оскарження такої ухвали слідчого судді правове оформлення процесу призначення судової експертизи було формальною процедурою, що призводила до численних упущень і недоліків у процесі проведення експертизи, негативного впливу на перебіг розслідування. Низький рівень взаємодії експертних установ з органами досудового розслідування та суду своїм наслідком має низьку ефективність експертних установ[1] та заважає слідчому вчасно отримати інформацію доказового значення. Зазначене стало причиною повернення в жовтні 2019 року до традиційної для практиків процедури призначення експертизи: її знову можуть проводити експертна установа, експерт або експерти, яких залучають сторони кримінального провадження або слідчий суддя за клопотанням сторони захисту у випадках та порядку, передбачених ст. 244 цього Кодексу, якщо для з'ясування обставин, що мають значення для кримінального провадження, необхідні спеціальні знання (ч. 1 ст. 242 КПК України)[2].

Однак навіть ці зміни не забезпечать розв'язання всіх проблем, пов'язаних із залученням експерта слідчим. Адже монополія державних спеціалізованих установ (ст. 7 Закону України «Про судову експертизу») у питанні проведення експертиз у кримінальному провадженні теж затягує процес проведення окремих видів судових експертиз. Експерти в деяких галузях знань перевантажені обсягом доручених їм експертиз, що унеможливлює своєчасне виконання

[1] Цимбал П. В., Омельчук Л. В. Перспективи удосконалення інституту судової експертизи у кримінальному процесуальному законодавстві України. *Юридичний часопис Національної академії внутрішніх справ* 2013. № 1. С. 75-81

[2] Про внесення змін до деяких законодавчих актів України щодо вдосконалення окремих положень кримінального процесуального законодавства : Закон України від 4 жовт. 2019 р. № 187-IX. URL: https://zakon.rada.gov.ua/laws/show/187-20#n6.

ухвали суду. Єдиним шляхом подолання цієї проблеми для слідчого стає обрання перспективи направлення кримінального провадження для судового розгляду без отримання висновку експерта або пошук експертної установи, яка в умовах меншої завантаженості буде згодна порушити принцип дотримання закріплених нормативно регіональних зон обслуговування та провести експертизу, постанова або ухвала про яку надійшла з іншого регіону. Водночас залучення іноземних експертів досі є неможливим, адже формалізм призначення експертизи передбачає визначення в постанові слідчого тільки державної експертної установи, експерту якої доручають провести експертизу.

Окреслені аспекти залучення експерта в кримінальне провадження обґрунтовують необхідність порушення питань тактики призначення судової експертизи. Це система розроблених наукою та практикою прийомів і способів, застосовуваних на підставі процесуального закону під час підготовки, призначення та проведення експертизи з метою найефективнішого використання спеціальних знань під час вирішення питань, які мають значення для встановлення істини в розслідуваній справі[1].

Отже, питання залучення експерта для проведення судових експертиз під час розслідування злочинів, вчинених у кіберпросторі, доцільно висвітлювати в контексті тактичних рекомендацій, спрямованих на оптимізацію процесу призначення та проведення поширених видів експертиз.

Унаслідок вчинення злочинів у кіберпросторі утворюються як традиційні в криміналістичному сенсі, так і нетрадиційні або «цифрові» сліди, що потребує проведення в таких справах широкого спектру судових експертиз, а саме:

– експертизи комп'ютерної техніки і програмних продуктів;

– експертизи телекомунікаційних систем (обладнання) та засобів;

– технічної експертизи документів;

[1] Крышов И. Ф. Пути развития тактики экспертизы / И. Ф. Крышов // Сборник научных работ. – Вид. 3. – Вильнюс, 1968. – С. 7; Стецик Б.В. Особливості тактичних, процесуальних та організаційних засад підготовки, призначення та проведення судовов-подчеркознавчої експертизи. Науковий вісник Львівської комерційної академії. Серія : Юридична. 2015. Вип. 1. С. 246-260.

– експертизи відеозвукозапису;

– експертизи у сфері інтелектуальної власності;

– інших видів експертиз, без проведення яких неможливо отримати необхідні відомості, що свідчать про ознаки складу одного зі злочинів злочинної сукупності (наприклад, економічних експертиз під час розслідування злочинів, пов'язаних із фінансово-економічною сферою відносин у кіберпросторі; психологічної, мистецтвознавчої експертизи або відповідної комплексної експертизи[1] – злочинів, пов'язаних із соціальною сферою відносин суб'єктів у кіберпросторі; трасологічних експертиз – злочинів, що вчинені з антидержавно-політичних або корисливих мотивів, лінгвістичної експертизи мовлення (семантико-текстуальний аналіз писемного й усного мовлення) – злочинів, що вчинені з антидержавно-політичних мотивів; судово-балістичних, судово-хімічних експертиз тощо – злочинів, що порушують встановлений порядок обігу певних речей).

Під час розслідування всіх класифікаційних груп і підгруп злочинів, вчинених у кіберпросторі, типово (99 % аналізованого матеріалу) призначається ***експертиза комп'ютерної техніки і програмних продуктів.***

Науковці та слідчі в практиці для позначення цієї експертизи використовують термін «комп'ютерно-технічна експертиза» (КТЕ). Залежно від завдання, специфіки дослідження та видів об'єктів, які досліджують, у теорії виокремлюють різні її види, а саме: апаратно-комп'ютерну експертизу, програмно-комп'ютерну експертизу; експертизу даних (інформаційно-комп'ютерну); комп'ютерно-мережеву експертизу; комплекс цих експертиз[2].

Цей поділ має значення в теоретичному аспекті, проте сутність КТЕ лишається незмінною. Фактично в слідчій діяльності немає

[1] Шендрик В. В., Сафронов С. О., Крєпаков І. О., Жилін Є. В. Боротьба з порнографією: криміналістичні та оперативно-розшукові аспекти : науково-практичний посібник. Харків, 2010. 216 с. С. 211.

[2] Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. 250 с.; Настільна книга слідчого : наук.-практ. вид. / [М. І. Панов, В. Ю. Шепітько, В. О. Коновалова та ін.]. Київ : Ін Юре, 2003. 715 с.; Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 411 с.; Хатунцев Н. А. О специальных знаниях, необходимых при исследовании компьютерных средств и систем. *Актуальные проблемы российского права.* 2010. № 1. С. 332–339.

чіткого розподілу об'єктів дослідження КТЕ, цифрова природа інформації в кіберпросторі зумовлює неможливість відмежування дослідження змісту інформації від матеріального об'єкта, що є її носієм. За статистичними даними Державного науково-дослідного експертно-криміналістичного центру (ДНДЕКЦ) МВС України, здійснено єдине облікування об'єктів і кількості КТЕ: станом на 25 липня 2019 року загалом у структурах Експертної служби МВС проведено 1652 КТЕ, на дослідженні знаходилося 6239 об'єктів КТЕ. Тому ми будемо розглядати саме цей вид експертизи.

Аналіз спеціальної літератури й нормативних джерел дає змогу визначити, що КТЕ – це дослідження технічних властивостей комп'ютерного (цифрового) обладнання, програмного забезпечення, інформації, що містяться на цифрових носіях, з метою встановлення фактичних даних, які мають значення для провадження та пов'язані із застосуванням комп'ютерної техніки, а також виявляються на підставі спеціальних знань у галузях комп'ютерної техніки та програмування.

Об'єктами судової експертизи є комп'ютери з носіями інформації (будь-які накопичувачі інформації – дискети, жорсткі диски, CD-диски, флеш-карти тощо), програмні продукти й інша комп'ютерна техніка (наприклад, мобільні телефони, банкомати, гральні автомати, карт-ридери, електронні записні книжки, пейджери, принтери тощо), а також документація до обладнання.

Базовим документом з питань визначення орієнтовного переліку питань для проведення КТЕ є Інструкція про призначення та проведення судових експертиз та експертних досліджень та Науково-методичні рекомендації з питань підготовки та призначення судових експертиз та експертних досліджень (п. 13 розділу ІІ Рекомендацій)[1]. Типові переліки таких питань містяться також у наукових і методичних публікаціях з тематики розслідування різних видів кіберзлочинів та злочинів, пов'язаних з обстановкою кіберпростору[2].

[1] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

[2] Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних

Проте, на наше переконання, важливіше значення мають вимоги щодо формулювання таких переліків. Нещодавно колектив практиків ДНДКЦ МВС України запропонував чіткі вимоги до питань, що ставлять на вирішення КТЕ[1]. Розглянемо їх із власним аргументуванням.

1. Під час формулювання питання потрібно користуватися усталеним понятійним апаратом, уникати напівпрофесійних чи жаргонних термінів (наприклад, вінчестер, флешка, комп тощо). Слід застосовувати термінологію, визначену законами України, державними стандартами й іншими нормативно-правовими актами. Лише в разі відсутності термінів, визначених законодавчими або нормативними актами, допустимо використовувати терміни, які запропоновані безпосередньо розробниками самих технічних засобів, програмних продуктів у супровідній документації.

2. Питання має бути максимально чітким і передбачати можливість надання судовим експертом однозначної відповіді. Часто для проведення КТЕ надають об'єкти, які потенційно не містять і не можуть містити інформацію, що має значення для доказування. Так, наприклад, відповідно до вимог щодо повноти розслідування злочину, слідчий направляє для дослідження експерту всі комп'ютери, що були тимчасово вилучені під час обшуку в офісі, IP адресу якого було використано для вчинення злочину, уникаючи в такий спосіб проведення їх попереднього огляду та виконання вибіркової роботи з метою визначення конкретного комп'ютера.

технологій / за ред. Я. Ю. Кондратьєва. Київ : Паливода А. В., 2004. 144 с.; Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рек. / [О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.; Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 411 с.; Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. 168 с.

[1] Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. С. 89-90.

3. Формулювання питання не має стосуватися етапів дослідження інформації (опис характеристик носіїв інформації та особливостей розміщення інформації на них, відновлення і дослідження інформації серед знищених файлів є обов'язковим етапом дослідження).

4. Питання не повинні мати правовий (наприклад, щодо правомірності дій користувача, контрафактності, ліцензійності чи вартості програмного продукту) або довідковий зміст, коли вони не несуть змістовного навантаження (наприклад, які інформація, файли та папки містяться на носії; який зміст інформації, що міститься на носії; яке цільове призначення інформації на носії; чи міститься на конкретному електронному носії інформація щодо фінансово-господарської діяльності; чи містить носій інформації відомості про втручання до автоматизованої системи).

5. Питання мають бути спрямовані на встановлення конкретних обставин події, що належать до предмета доказування. Максимально повно сформульоване питання дає змогу отримати вичерпну відповідь. У питаннях чітко називають певний проміжок часу встановлюваної дії, суть дії (друк, редагування, створення), конкретні програми, їх призначення, файли з форматами, сайти тощо.

6. Питання не повинні виходити за межі компетенції судового експерта певної/их експертної/их спеціальності/ей. У цьому сенсі зауважимо, що поширеною помилкою є призначення однією ухвалою КТЕ щодо декількох об'єктів, для дослідження яких потенційно потрібно залучати спеціалістів різного фаху або різних експертних спеціальностей (наприклад, одночасно за комп'ютером і засобом мобільного зв'язку, який був засобом комунікації, що становить інтерес для досудового розслідування злочину).

7. Питання мають відповідати наявній нині методичній та технічній базі, доступній судовому експерту. Слідчий повинен розуміти, що не всі територіальні підрозділи Експертної служби МВС України або інститути судових експертиз Міністерства юстиції України мають у своєму розпорядженні однакові програмно-апаратні засоби для проведення досліджень. Програмно-апаратні комплекси для виготовлення побітних копій носіїв цифрової інформації, що надають змогу експертам провести повне або часткове відновлення інформації, утраченої випадково або знищеної з метою приховування злочину, наявна в експертних підрозділах МВС. Однак, якщо є потреба в дослідженні надто великих

обсягів інформації, то необхідно ще на етапі призначення експертизи обирати той експертний підрозділ (із сучаснішими комп'ютерними аналітичними системи), що здатний на відповідному технічному рівні провести дослідження. На жаль, в експертних службах не ведуть статистики таких випадків. Лише з обліковуваних даних продуктивності експертних підрозділів можна дійти висновку, що в територіальних підрозділах під час оновлення матеріально-технічної бази для проведення КТЕ одразу збільшується навантаження на експертів у середньому на 100 %.

8. Питання мають бути поставлені так, щоб під час виконання конкретних завдань розслідування витрати (фінансові, технічні, часові тощо) на проведення досліджень були мінімальними. На жаль, зауважують експерти, часто однією ухвалою слідчого судді призначають експертизу за доволі значною кількістю об'єктів КТЕ, що фактично унеможливлює своєчасне та належне її проведення. Терміни проведення судових експертиз безпосередньо залежать від складності дослідження, кількості об'єктів, кількості поставлених питань і завантаженості фахівців, які проводять КТЕ. Наприклад, відповідно до п. 14, 15 Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби МВС України, до 30 днів проводять експертизу щодо матеріалів, які належать до категорії досліджень середньої складності (за умови дослідження від 10 до 20 однорідних і/або не більше ніж 10 різноманітних об'єктів, вирішення не більше ніж 5 запитань і застосування від трьох до п'яти загальнонаукових і/або спеціальних методів дослідження)[1]. Аналіз матеріалів кримінальних проваджень стосовно досліджуваного виду злочинів засвідчує, що орієнтовний термін проведення КТЕ часто перевищує 30 днів, адже на розв'язання експерту ставлять завжди понад п'ять питань, а наявність на дослідженні одного об'єкта не є показником невеликого обсягу роботи, обсяг інформації на конкретному об'єкті дослідження може переважати сумарний обсяг інформації на десяти таких об'єктах. Тому на практиці призначення КТЕ за окреслених

[1] Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : наказ МВС України від 17 лип. 2017 р. № 591. URL: https://zakon.rada.gov.ua/laws/show/z1024-17?find=1&text=%F1%F2%F0%EE%EA#w12.

обставин може діяти таке правило: «один об'єкт – одна експертиза». Хоча, відповідно до статистичних даних ДНДЕКЦ МВС України, середня пропорція становить одну експертизу для п'яти–шести об'єктів.

З метою оптимізації процесу проведення КТЕ експерти розробили такий алгоритм підготовчих заходів для слідчого (прокурора):

1) провести процесуальний огляд об'єктів із залученням фахівців (наприклад, Експертної служби МВС України) з метою встановлення наявності даних, що можуть мати доказове значення в кримінальному провадженні, і для вирішення питання про доцільність подальшого призначення експертизи;

2) попередньо узгодити перелік питань за конкретними об'єктами із фахівцями (судовими експертами) й оптимізувати кількість питань;

3) визначити першочерговість і пріоритети дослідження наданих для експертизи об'єктів;

4) за об'єктивної потреби дослідження значного обсягу різноманітної комп'ютерної техніки (понад 10 одиниць) призначати експертизи з розмежуванням за групами об'єктів дослідження, а іноді – окремі експертизи за кожним об'єктом дослідження[1].

На підставі аналізу судово-слідчої практики ми вважаємо можливим доповнити цей алгоритм дій слідчого (прокурора) під час залучення експерта для проведення КТЕ такими заходами:

1) оцінити фактичну й документальну інформацію про те, що у справі могли вже бути проведені інші експертизи (або знаходяться на виконанні в експерта), пов'язані з дослідженням цифрової інформації; отримані з цього приводу клопотання експерта;

2) оцінити терміновість ініціювання проведення експертизи (чи має фактичну можливість інша сторона процесу залучити за договором експерта раніше, ніж це буде здійснено в межах досудового розслідування);

3) конкретизувати кількість, якість і перелік об'єктів, що надаватимуть для дослідження судовому експерту (це допоможе оцінити реальну можливість проведення експертизи з позицій витрачання на неї

[1] Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. С. 91-92.

часу, її складність і значення майбутніх висновків для конкретного кримінального провадження).

Для розслідування злочинів, вчинених у кіберпросторі, притаманне призначення КТЕ в комплексі з іншими видами експертиз. Поширеними в цьому сенсі можна вважати комплексні КТЕ й технічну експертизу документів (ТЕД) або експертизу відеозвукозапису.

Комплексна КТЕ і ТЕД – це дослідження, що проводять для вирішення спільних (інтеграційних) питань стосовно документів, виготовлених за допомогою комп'ютерної техніки. У сучасних умовах злочинці мають доступ до різноманітних принтерів, витратних матеріалів та багатофункціонального поліграфічного обладнання, які через порівняно невисоку ціну та можливість анонімного придбання (стосовно поліграфічного обладнання для підроблення банківських карт) надають можливість виготовити високої якості підроблені документи як знаряддя для вчинення злочинів надалі.

Документи на пластиковій основі науковці класифікують за різними критеріями та розглядають стосовно них ознаки підробки. Наприклад, С. М. Науменко досліджував ознаки підробки та класифікацію пластикових документів за розміром, зокрема: стосовно документів формату банківської картки або документів розміру ID 1 – свідоцтва про реєстрацію транспортного засобу[1]. До підробки першого виду належать випадки, коли реквізити бланка друкують на папері або полімерному матеріалі з використанням струменевого або лазерного кольорових принтерів, персональні дані можуть наносити термосублімаційним способом друку. Документ виглядає неякісно, виявити підробку уважному патрульному поліцейському нескладно. До підробки другого виду належать випадки, коли використовують справжній бланк; для цього верхні захисні плівки знімають, первинний текст частково або цілком видаляють. Згодом наносять вторинні персональні дані з використанням (у цьому разі) монохромного лазерного принтера. Документ виглядає якісніше, виявити підробку може експерт. Водночас науковець зазначає, що в експертній практиці дедалі частіше трапляються випадки, коли первинний текст цілком видаляють, потім на оригінальний бланк наносять вторинні персональні дані з використанням термосублімаційного принтера, тоді вже наносять

[1] Науменко С. М. Стосовно питання щодо підробки ідентифікаційних документів. *Криміналістика і судова експертиза.* 2019. Вип. 64. С. 457.

оригінальні захисні плівки. У такому випадку підроблений документ майже не відрізняється від оригінального, тому в процесі його дослідження навіть експертам складно формулювати висновок щодо встановлення факту внесення змін. Наявність для експертного дослідження комп'ютерної техніки, яку ймовірно використовували для виготовлення документів, стає передумовою належного рівня проведення судової експертизи. Таким чином, комплексну КТЕ і ТЕД проводять для:

– встановлення типу й ідентифікації комп'ютерної та копіювально-розмножувальної техніки за виготовленими за їх допомогою матеріальними документами;

– пошуку даних з наданого на експертизу документа (фактів і способів створення та внесення змін до документів, виявлення їх первинного змісту);

– ідентифікації знайденої комп'ютерної інформації з даними на паперовому носієві.

Об'єктами такої експертизи є одночасно:

– об'єкти КТЕ, а саме техніка, що могла бути використана для виготовлення документа (комп'ютер, принтер, багатофункціональний пристрій, інсталяційні диски до них, з'єднувальні та мережеві кабелі);

– об'єкти ТЕД, а саме переважно документи, що обслуговують грошовий обіг (платіжні картки, чеки, банківські документи), цінні папери, посвідчення, приватні листи); матеріали, які використовують для створення документа (барвники, поліграфічні фарби в штрихах, тонери, картриджі розмножувальної техніки, клейні матеріали).

У Науково-методичних рекомендаціях з питань підготовки та призначення судових експертиз та експертних досліджень (п. 3 розділу II)[1] визначено такі обов'язкові вимоги до об'єктів, що надають експерту:

1) для виконання ідентифікаційних завдань експертизи обов'язковим є наявність електронного оригіналу документа (файлу);

[1] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

2) електронний оригінал документа встановлюють під час огляду комп'ютерної техніки, проведеного за обов'язковою участю спеціаліста в галузі комп'ютерно-технічних досліджень;

3) принтери (передусім струменеві) слід направляти на експертизу в найстисліший термін, оскільки застигання барвника може призвести до змін у вигляді та характері нанесення барвника на папір;

4) до призначення експертизи слідчому необхідно з'ясувати, чи змінювали знімні частини (картриджі), чи піддавали ремонту які-небудь вузли принтерів;

5) якщо картриджі лазерних принтерів змінювали, необхідно вжити заходів щодо розшуку відпрацьованих картриджів і подати їх на дослідження;

6) для проведення експертизи слід також вилучити вільні зразки, які були виготовлені на вилученому принтері в період, що відповідає періоду виготовлення досліджуваних документів.

Комплекс КТЕ й експертизи відеозвукозапису є також типовим під час розслідування злочинів, вчинених у кіберпросторі, адже злочинці активно використовують мультимедійні технології, що ґрунтуються на представлених даних у цифровому форматі відеозображення із застосуванням анімації та звукового супроводу. У цій експертизі спільні (інтеграційні) питання пов'язані зі встановленням їх оригінальності та незмінності (відсутністю монтажу) запису за допомогою комп'ютерної техніки.

Основним об'єктом дослідження є файли зі звуковими, відеоформатами. Їх носіями, що відправляють на дослідження, переважно є мобільні телефони, смартфони. Ця техніка становить різновид терміналу стільникового зв'язку, SIM-карти до неї є необхідним компонентом для функціонування такого терміналу як телекомунікаційного засобу[1]. Тому дослідження їх є завданням експертизи телекомунікаційних систем (обладнання) та засобів. Проте, виконуючи функції цифрового органайзера або персонального комп'ютера (спеціалізованого комп'ютера з відповідним програмним забезпеченням для роботи з електронною поштою, перегляду

[1] Харабуга Ю. С. Комп'ютерно-технічне дослідження мобільних телефонів, смартфонів та SIM-карт. *Криміналістика та судова експертиза.* 2014. Вип. 59. С. 335–342.

текстових або мультимедійних файлів тощо), ця техніка одночасно є об'єктом КТЕ[1]. Мобільні телефони оснащені слотом для карти пам'яті, та/або їх можна підключити до комп'ютера як звичайний зовнішній накопичувач інформації з файловою системою.

За межі компетенції експерта з КТЕ будуть виходити питання походження інформації в пам'яті мобільного терміналу (унаслідок мобільного зв'язку, відеозапису, звукозапису або фотозйомки). Це потребує комплексного дослідження за участю експертів інших видів судової експертизи[2]. Аналогічно комплексного дослідження потребує встановлення походження інформації в пам'яті SIM-карти. Дослідження відео- та звукової інформації, утвореної за допомогою мікрофону та відеокамери комп'ютера, мають проводити за участю експерта з технічного дослідження матеріалів і засобів відеозвукозапису за умови, що поставлене завдання передбачає вирішення питань про здійснення запису представленим терміналом й установлення відсутності в записі змін. Дослідження інформації, яка могла утворитися внаслідок мобільного або іншого зв'язку, слід проводити також за участю експерта з експертизи телекомунікаційних систем (обладнання) та засобів за умови, що поставлене завдання передбачає вирішення питань про походження інформації внаслідок мобільного або іншого зв'язку[3].

У переліку питань до КТЕ, запропонованому С. В. Самойловим під час розроблення методики розслідування шахрайства в мережі Інтернет, на нашу думку, містяться також спільні з дослідженням відеозвукозапису питання, зокрема[4]:

---

[1] Харабуга Ю. С., Білий С. Б. Дослідження мобільних телефонів і смарт-карт до них у межах комп'ютерно-технічної експертизи. *Теорія та практика судової експертизи і криміналістики.* 2009. Вип. 9. С. 454–458.

[2] Харабуга Ю. С. Комп'ютерно-технічне дослідження мобільних телефонів, смартфонів та SIM-карт. *Криміналістика та судова експертиза.* 2014. Вип. 59. С. 337

[3] Дослідження інформації в пам'яті терміналів стільникового зв'язку : звіт НДР (заключ.) / ЛНДІСЕ ; наук. кер. Ю. С. Харабуга. Львів : ЛНДІСЕ, 2011. 65 с. № держ. реєстрації 0110U002599.

[4] Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. С. 162-164

1) чи зберігаються на представлених на дослідження накопичувачах графічні файли із зображенням (описують смисловий аспект зображення, наприклад, зображення цифрового фотоапарата, мобільного телефона тощо);

2) якщо зберігається, де саме, яка кількість та обсяг файлів, яка дата створення й останніх змін, у який спосіб було отримано зображення (чи створено за допомогою графічних редакторів на комп'ютерній системі (пристрої), завантажено з мережі Інтернет, відскановано, сфотографовано тощо);

3) чи зберігаються на представлених на дослідження накопичувачах відеофайли, які містять інформацію про (описують смисловий аспект відеофайлу, наприклад, реклама або можливості цифрового фотоапарата, мобільного телефона тощо);

4) якщо зберігається, де саме, яка кількість та обсяг файлів, яка дата створення й останніх змін, у який спосіб було створено такі файли (чи створено (змонтовано) за допомогою відеоредакторів на комп'ютерній системі (пристрої), завантажено з мережі Інтернет, знято відеокамерою тощо).

Експертизу телекомунікаційних систем (обладнання) та засобів фактично проводили лише в 10 % аналізованих проваджень щодо злочинів, вчинених у кіберпросторі. Проте такий показник міг бути значно вищим, основні причини цього – висока вартість такої експертизи, потреба в постійному оновленні матеріально-технічного забезпечення експертних служб для її проведення та нестача відповідних експертних кадрів у системі Експертної служби МВС України.

Право на проведення судових експертиз законодавчо надано судовим експертам, яких внесено до державного Реєстру атестованих судових експертів за відповідною експертною спеціальністю. У Реєстрі станом на 1 жовтня 2019 року за експертною спеціальністю «10.17. Дослідження телекомунікаційних систем (обладнання) та засобів» значиться 48 судових експертів, які є співробітниками державних спеціалізованих установ. У більше ніж половини експертів свідоцтво вже недійсне для проведення таких експертиз, деяких експертів звільнено з експертних установ МВС України. Згідно з даними ДНДКЦ МВС України, станом на 25 липня 2019 року в експертних службах МВС за відповідною експертною спеціальністю більше половини посад є вакантними, відповідні експерти є тільки в

ДНДЕКЦ, Вінницькому та Чернівецькому НДЕКЦ. Тенденція до збільшення кількості об'єктів, що спрямовують на такі дослідження (за даними ДНДКЦ за 2017 рік, досліджено 69 об'єктів, за 2018 рік – 224), засвідчує нагальну необхідність розв'язання кадрових проблем у цьому напрямі проведення експертиз.

Експертиза телекомунікаційних систем (обладнання) та засобів – це дослідження телекомунікаційних систем і засобів, мереж, їхніх складових та інформації, яку вони передають, приймають та обробляють, з метою встановлення технічних параметрів і стану об'єкта, визначення їх функціонального призначення. Цей вид досліджень потребує окремих знань, пов'язаних із розумінням інформаційних процесів у комп'ютерних мережах, мережах зв'язку, спеціалізованих телекомунікаційних пристроях[1], чим і зумовлене виокремлення відповідної експертної спеціальності.

Під час розслідування злочинів, вчинених у кіберпросторі, об'єктами цієї експертизи часто є: Інтернет IP вузли, веб-сторінки, приймачі радіосигналів, вузли комутації; первинні мережі зв'язку, наземні станції супутникового зв'язку, обставини (адресації в мережі Інтернет; передачі радіосигналів; використання доменних імен у мережі Інтернет тощо). Таку експертизу призначають здебільшого під час розслідування злочинів, вчинених у кіберпросторі, за умови, якщо способом вчинення (приховування або підготовки) злочину є:

– втручання в роботу мереж операторів зв'язку,

– заміна, спотворення, витікання, втрата трафіку і спотворення процесу його обробки;

– порушення встановленого порядку маршрутизації трафіку.

Слідчий формулює питання для експертного дослідження на підставі того матеріалу, який наявний у кримінальному провадженні, та з дотриманням вимог до питань, аналогічних розглянутим вище для проведення КТЕ. Користуючись загальновизнаним у теорії судової експертизи поділом питань на ідентифікаційні та діагностичні, вважаємо всі питання, які вирішує експертиза телекомунікаційних

[1] Бобрицький С. М. Методичні аспекти дослідження телекомунікаційних систем (обладнання) та засобів. *Теорія та практика судової експертизи і криміналістики.* 2008. Вип. 8. С. 445–449.

систем (обладнання) та засобів, діагностичного спрямування, зокрема таким є типовий їх перелік[1]:

1) які тип, марка, модель телекомунікаційного засобу (системи);

2) чи в робочому стані знаходиться телекомунікаційний засіб (об'єкт);

3) які технічні характеристики (параметри) має телекомунікаційний засіб;

4) які характеристики підключень до мережі має телекомунікаційний засіб;

5) чи наявний факт доступу до телекомунікаційної системи та в який спосіб;

6) чи здійснено використання ресурсів та інформації в телекомунікаційній системі та в який спосіб;

7) чи наявний факт передання (отримання) інформації в телекомунікаційній системі та в який спосіб;

8) чи є ознаки втручання в роботу телекомунікаційної системи та в який спосіб;

9) чи змінював користувач телекомунікаційної системи (мережі) налаштування окремих пристроїв, як саме і в який час;

10) яка причина виходу з ладу телекомунікаційного засобу (системи);

11) який загальний характер підключень до телекомунікаційної мережі виконував об'єкт (телекомунікаційна система, засіб);

12) за допомогою яких програмних засобів здійснювали підключення до телекомунікаційної мережі;

13) яка топологія апаратних засобів, об'єднаних у телекомунікаційну систему;

14) чи відповідає телекомунікаційна система (засіб) технічній документації;

[1] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

15) чи можливе використання телекомунікаційного засобу (обладнання) для зазначених цілей;

16) які шляхи маршрутизації даних у телекомунікаційній системі;

17) за яким алгоритмом обробляють чи оброблено інформацію телекомунікаційним засобом (системою);

18) чи могли апаратні засоби об'єднуватися в телекомунікаційну мережу та за якими ознаками;

19) чи наявний факт передання (отримання) інформації в телекомунікаційній системі та в який спосіб.

Експертиза у сфері інтелектуальної власності. Сучасне науково-методичне забезпечення проведення таких експертиз стосується різних за походженням об'єктів інтелектуальної творчості[1]. У межах розслідування злочинів, вчинених у кіберпросторі, традиційно здійснюють два види таких досліджень: дослідження, пов'язані з комп'ютерними програмами й компіляціями даних (базами даних), та/або дослідження, пов'язані з виконанням, фонограмами, відеограмами, програмами (передачами) організацій мовлення. Експерти використовують і відповідні методики та методичні рекомендації щодо: проведення судових експертиз оптичних носіїв, які містять об'єкти авторського права й суміжних прав; дослідження ознак контрафактності лазерних компакт-дисків, аудіо- і відеокасет; проведення судово-експертних досліджень веб-сайту як об'єкта інтелектуальної власності[2].

Орієнтовний перелік питань, які ставлять перед експертом, міститься в Науково-методичних рекомендаціях з питань підготовки та призначення судових експертиз та експертних досліджень (розділ V)[3].

---

[1] Реєстр методик проведення судових експертиз. *Міністерство юстиції України :* [сайт]. URL: http://rmpse.minjust.gov.ua/search.

[2] Біленчук П. Д., Колонюк В. П., Шульга О. О. Криміналістичне забезпечення досліджень у сфері інтелектуальної власності: історія, сьогодення, перспективи. *Криміналістика і судова експертиза.* 2016. Вип. 61. С. 467–477.

[3] Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL:https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

Використовуючи загальновизнаний у теорії судової експертизи поділ питань на ідентифікаційні й діагностичні, зауважимо, що типові діагностичні питання стосуються аналізу:

– відповідності досліджуваних об'єктів певним умовам, необхідним для надання їм правової охорони;

– виявлення ознак об'єктів права інтелектуальної власності;

– виявлення ознак неліцензійності використання комп'ютерної програми;

– встановлення факту відтворення (використання) цих об'єктів тощо. Встановлюючи факт повного або часткового відтворення об'єкта під час створення іншого об'єкта, можливо вирішити й ідентифікаційне питання щодо встановлення наявності відображення цих ознак у конкретному індивідуально визначеному об'єкті. Зокрема, експерт відповідатиме на питання:

– чи є вихідні тексти (вихідні коди) або їх частина певної комп'ютерної програми переробкою вихідних текстів (вихідних кодів) іншої комп'ютерної програми;

– чи є певна комп'ютерна програма самостійним, оригінальним твором, що відрізняється від комп'ютерної програми.

Зважаючи на специфіку досліджуваних об'єктів щодо експертизи комп'ютерних програм і компіляцій даних та/або програм (передач) організацій мовлення, слід визнати, що до їх проведення залучають експертів, які здебільшого мають спеціалізацію в галузі інформаційних технологій та/або електроніки й телекомунікацій, більшість з них є експертами спеціалізації КТЕ. Можливо, саме тому для слідчого чи прокурора доволі проблемним стає питання доцільності призначення експертизи у сфері інтелектуальної власності. Слідчі та прокурори можуть затягувати призначення останньої в умовах, коли першою в справі вже призначена та/або проведена КТЕ, а проведення експертизи у сфері інтелектуальної власності потребує значних витрат з позицій бюджетної політики. На нашу думку, якщо наслідком проведення експертизи буде встановлення ознак складу конкретного злочину, то без експертизи процес розслідування не має сенсу. Тому стосовно досліджуваної категорії злочинів експертиза у сфері інтелектуальної власності є обов'язковою під час розслідування інтелектуального піратства.

Отже, окремі складнощі залучення експертів для проведення судових експертиз не можуть бути причиною відмови слідчого та/або

прокурора від застосовування КТЕ, експертизи телекомунікаційних систем (обладнання) та широкого спектру інших експертиз. Адже судові експертизи є одним з найефективніших засобів формування доказів вчинення злочинів у кіберпросторі.

ПІСЛЯМОВА

Сформульовано ряд висновків.

1. Кіберпростір як середовище злочинної діяльності та об'єкт криміналістичних дослідженнях розглядається у двох значеннях: а) середовище (обстановка), окремі елементи (телекомунікаційна мережа, комп'ютерна інформація, інформаційні технології тощо) якого можуть використовуватись як знаряддя злочину; б) специфічна обстановка для слідоутворення (сліди злочинів).

Використана для досягнення злочинного результату обстановка кіберпростору має притаманні лише їй подвійні чинники технічної та соціальної природи, зокрема: 1) віддаленість (дистанційність) доступу до предмета посягання з використанням кіберпростору, що забезпечує транскордонну складову такої злочинної діяльності; 2) оперативність створення, поширення, модифікації або знищення інформації в кіберпросторі, що є предметом злочинного посягання або слідом злочину – це сприяє значному прискоренню та якісному приховуванню злочинної діяльності; 3) віртуальність, що забезпечує відносну конфіденційність інформації про особу злочинця та можливість упливати на свідомість певної категорії осіб; 4) комунікативність, яка уможливлює створення злочинних груп та ефективну діяльність уже наявної організованої злочинності; 5) недосконалість забезпечення інформаційної безпеки та правової охорони відносин у кіберпросторі, що надає злочинцю можливість уникати кримінальної відповідальності за вчинені злочини.

2. Сучасний стан правового регулювання боротьби зі злочинами, вчиненими у кіберпросторі, характеризується дезорганізованістю системи нормативно-правових актів у цьому напрямку на міжнародному рівні регулювання та відносною цілісністю системи актів на національнальному рівні.

Центральне місце на національному рівні в механізмі правового регулювання боротьби з такими злочинами займають норми Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року, Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15 листопада 2000 року, загальні та спеціальні норми КК України, які передбачають численні конвенційні та альтернативні Конвенціям склади кримінальних правопорушень, що вчиняються в обстановці кіберпростору. Іншими складовими

національної системи правового регулювання боротьби з такими злочинами виступають норми галузевого законодавства, зокрема у сфері забезпечення національної, економічної та кібернетичної безпеки, захисту суспільства, дітей, інформації, авторських та суміжних прав.

Запропоновано доповнити окремі статті КК України кваліфікаційною ознакою стосовно використання обстановки кіберпростору для вчинення відповідних видів злочинів, зокрема проти основ національної безпеки України (ст. 109–114 КК України), у сфері охорони державної таємниці (ст. 328, 330); проти виборчих прав і свобод (ст. 157, 158, 159, 159-1); проти власності (ст. 185, 189, 191); у сфері господарської діяльності (ст. 206, 209, 231, 232); пов'язаних з тероризмом (ст. 258, 258-2, 258-3, 258-5); у сфері незаконного обігу наркотичних засобів (ст. 307, 311); придбання чи збут зброї, бойових припасів або вибухових речовин, аналогічних дій та використання спеціальних технічних засобів отримання інформації (ст. 263, 359).

3. Криміналістична класифікація злочинів, вчинених у кіберпросторі, є дворівневою системою, яка утворюється з чотирьох груп злочинів, виділених за мотивом на першому рівні та в межах цих груп з підгруп – за технологіями злочинної діяльності.

I. Злочини, вчинені з корисливих мотивів, що пов'язані з фінансово-економічними відносинами у кіберпросторі: 1.1. злочини, що порушують встановлений порядок обігу певних речей (наркотичних засобів, психотропних речовин, прекурсорів, зброї, бойових припасів та вибухових речовин, технічних засобів отримання інформації); 1.2. злочини, що спрямовані на заволодіння чужим майном, та пов'язані із ними злочини у сфері функціонування електронних розрахунків; 1.3. злочини, що порушують механізми захисту від монополізму та недобросовісної конкуренції;

II. Злочини, вчинені з соціально-економічних мотивів, що пов'язані з соціальною сферою відносин суб'єктів у кіберпросторі: 2.1. злочини, пов'язані із насильницько-егоїстичними діями; 2.2. інтелектуальне піратство та злочини, пов'язані із комунікаційними діями;

III. Злочини, вчинені з політичних мотивів суб'єктів у кіберпросторі: 3.1. злочини, що пов'язані з антидержавницькими діями; 3.2. злочини політико-ідеологічного спрямування;

IV. Злочини, вчинені з ідейних мотивів (пов'язані зі світоглядом) суб'єктів у кіберпросторі: 4.1. злочини, пов'язані із насильницько-дискримінаційними діями; 4.2. злочини, пов'язані із анархістськими діями у кіберпросторі.

4. Структурними елементами криміналістичної характеристики злочинів, вчинених у кіберпросторі, є: 1) предмет посягання (матеріальні цінності, грошові кошти, інформація тощо); 2) особа злочинця, у тому числі у складі організованої групи чи злочинної організації; 3) способи вчинення злочинів у кіберпросторі (підготовки, безпосереднього вчинення та приховування) / технології вчинення злочинів (сукупність способів, що забезпечують досягнення кінцевої злочинної мети при вчиненні сукупності різних за кримінально-правовими ознаками злочинів); 4) сліди злочинів (в матеріальному та електронному середовищах).

Взаємозв'язки між особою злочинця (його мотивом) та предметом посяганння, типовими слідами та особою злочинця, технологією злочинної діяльності та особою злочинця (організованою групою), способом вчинення злочинів та інформаційно-комунікаційними технологіями, як знаряддями вчинення злочину, мають обов'язковий взаємозумовлений характер та високий ступінь інтенсивності такого зв'язку.

5. Предмети злочинного посягання у кіберпросторі розподілено на дві групи, які знаходяться у взаємозв'язку та не існують відокремлено як предмети злочину. В основі їх зв'язку знаходиться полімотивованість злочинної діяльності у кіберпросторі.

Первинними предметами посягання у кіберпросторі є: 1) інформаційний продукт (проявляється у вигляді «інформації з обмеженим доступом» (персональні дані, банківська, державна та комерційна таємниця) або об'єктів авторського права або суміжних прав (аудіовізуальні твори (традиційно фільми, що вийшли у прокатний показ), бази даних (компіляції даних), комп'ютерні програми фонограми та передачі організацій мовлення); 2) інформаційний ресурс як сукупність інформаційних продуктів, що організована за допомогою певної інформаційної технології (це попередньо створений злочинцем файл; веб-сайт; автоматизовані (електронно-інформаційні) системи різного призначення).

Вторинними предметами посягання виступають майно, комп'ютери, комп'ютерні мережі, мережі електрозв'язку та

документи. Вторинні предмети посягання розподілено на два види матеріальних цінностей: 1) такі, що мають позитивні властивості (грошові готівкові або безготівкові кошти, товари, цілісні майнові комплекси критично важливого об'єкта інфраструктури; комп'ютери, комп'ютерні мережі, мережі електрозв'язку документи, які виконують функцію захисту інформації від несанкціонованого втручання в роботу з останньою); 2) такі, що мають негативні властивості (наркотичні засоби, психотропні речовини, прекурсори, технічні засоби отримання інформації, зброя, бойові припаси та вибухові речовини).

6. За критерієм професійності виділено п'ять типів особи злочинця, зокрема: 1) злочинець-користувач початкового рівня; 2) злочинець-звичайний користувач; 3) злочинець-упевнений користувач; 4) злочинець-досвідчений користувач; 5) злочинець-користувач професіонал.

Критеріями визначення професійності (кваліфікації) злочинця вбачається наступна сукупність ознак: 1) здатність злочинця використовувати технології анонімізації доступу до ресурсів мережі Інтернет (проксі-сервісів (комплексів програм), віртуальних приватних мереж, інших засобів-анонімайзерів); 2) мобільність злочинця (індивідуальна професійна, соціальна або географічна); 3) психологічні характеристики (ознаки) злочинця, що впливають на формування й реалізацію злочинної мети; 4) роль у складі організованої злочинної групи.

7. Типові способи вчинення злочинів у кіберпросторі класифікуються за ознакою кібертехнологій на вісім груп. Про характерні технології вчинення злочинів у кіберпросторі висновується в разі вчинення сукупності злочинів у межах однієї або декількох класифікаційних підгруп злочинів у кіберпросторі, зокрема: 1) технології незаконного збагачення, засновані на попередньому заволодінні персональними даними/комерційною таємницею фізичної/юридичної особи шляхом несанкціонованого втручання в роботу комп'ютерної техніки; 2) технології заволодіння безготівковими коштами шляхом застосування електронних платіжних систем, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки; 3) технології «шпигунства», засновані на попередньому отриманні доступу до державної/комерційної таємниці шляхом несанкціонованого

втручання в роботу комп'ютерної техніки; 4) технології службових розкрадань шляхом застосування електронних платіжних систем, засновані на несанкціонованих діях з інформацією, вчинені особою, яка має право доступу до неї; 5) технології приховування незаконного походження безготівкових коштів, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки; 6) технології незаконного збагачення, засновані на попередньому несанкціонованому втручанні в роботу комп'ютера, комп'ютерної системи, мережі з метою нейтралізації засобів інтелектуального захисту.

8. Визначено чотири організаційні форми початку кримінального провадження щодо злочинів, вчинених у кіберпросторі, а саме: 1) за заявою потерпілого/повідомлення особи про кримінальне правопорушення (безальтернативна форма); 2) за матеріалами оперативних підрозділів, отриманими в результаті перевірки оперативної інформації (альтернативна форма); 3) у межах реалізації матеріалів ОРС (безініціативна форма); 4) унаслідок виявлення слідчим злочину, вчиненого у кіберпросторі, під час розслідування іншого кримінального провадження (ініціативна форма). Три перші форми охарактеризовані як типові щодо злочинів, вчинених у кіберпросторі.

9. Взаємодія слідчого із оперативними підрозділами, власниками (розпорядниками) систем, володільцями інформації в системах та іншими суб'єктами на ринку телекомунікаційних послуг є невід'ємною складовою процесу виявлення та розслідування злочинів, вчинених у кіберпросторі. Особливості організації протидії кіберзагрозам в Україні та організації національного сегменту кіберпростору зумовлюють суб'єктів та форми їх взаємодії зі слідчим в процесі розслідування злочинів, вчинених у кіберпросторі.

10. Початковий етап розслідування злочинів триває з моменту внесення інформації про злочин у ЄРДР до моменту висунення принаймні одній особі законної й обґрунтованої підозри у вчиненні кримінального правопорушення (одного або декількох); наступний етап – до закриття кримінального провадження або направлення до суду обвинувального акта, клопотання про застосування примусових заходів медичного або виховного характеру, клопотання про звільнення особи від кримінальної відповідальності. Початковому етапу як більш навантаженому основними та тактичними завданнями

розслідування надається особливе значення в методиці розслідування злочинів, вчинених у кіберпросторі. Основними завданнями початкового етапу розслідування таких злочинів є: 1) встановлення відсутності/наявності події кримінального правопорушення (час, місце, спосіб та інші обставини вчинення кримінального правопорушення); 2) встановлення складу визначеного кримінального правопорушення (час, місце, спосіб, мета/мотив, повторність, вчинення групою осіб/організованою групою, наслідки й інші обставини вчинення кримінального правопорушення); 3) встановлення фактичних даних, які вказують на конкретну особу, що могла вчинити кримінальне правопорушення (форма вини, мотив і мета вчинення кримінального правопорушення особою, стосовно якої вирішують питання щодо вручення їй повідомлення про підозру); 4) забезпечення здійснення кримінального провадження; 5) встановлення злочинної діяльності в повному обсязі; 6) встановлення характеру й тяжкості обвинувачення щодо кожного суб'єкта злочину.

11.Виокремлено три групи типових слідчих ситуацій початкового етапу розслідування злочинів вказаної категорії: 1) ситуації, що характеризуються наявністю персоналізованих відомостей про користувача як імовірного злочинця; 2) ситуації, що характеризується наявністю неперсоналізованих відомостей про користувача як імовірного злочинця; 3) ситуації, яким властива відсутність будь-яких відомостей про особу злочинця. У межах кожної з груп таких слідчих ситуацій схарактеризовано три різновиди: 1) ситуація, коли кримінальне провадження розпочато на підставі отримання заяви/повідомлення особи про кримінальне правопорушення; 2) ситуація, коли кримінальне провадження розпочато внаслідок перевірки оперативної інформації; 3) ситуація, коли кримінальне провадження розпочато в межах реалізації матеріалів ОРС. Розгляд ситуацій у комплексі з основними тактичними завданнями та комплексом слідчих (розшукових) дій та інших заходів пізнання визначає специфіку розслідування класифікаційних груп/підгруп злочинів, вчинених у кіберпросторі.

12. Оптимізація розслідування вказаних злочинів потребує:

а) впровадження таких нових тактичних операцій як «Персоналізація відомостей про особу/осіб злочинця/ів», «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»; внутрішня їх структура та особливості тактики провадження їхніх компонентів визначається в контексті поєднання слідчих та негласних слідчих (розшукових) дій задля досягнення однойменних тактичних завдань розслідування;

б) вдосконалення розроблених тактичних операцій у частині оновлення структурування таких тактичних операцій: «Збирання електронних (цифрових) носіїв інформації», «Організація затримання та/або отримання свідчень злочинця, що діє в кіберпросторі» та «Матеріалізація ідеальних слідів вчинення злочинів у кіберпросторі». Взаємозв'язок усіх тактичних операцій зумовлений характером інформації про особу злочинця, відповідно слідчою ситуацією.

13. Спеціальні знання під час розслідування злочинів, вчинених у кіберпросторі, використовуються у процесуальних та непроцесуальних формах. До процесуальних форм відносимо: залучення спеціаліста для надання письмової консультації; залучення спеціаліста для безпосередньої технічної допомоги під час процесуальних дій; залучення експерта для проведення судової експертизи й виконання обов'язків судового експерта. До непроцесуальних – усне консультування слідчого зі спеціалістом; залучення спеціаліста під час перевірки оперативної інформації про злочини, що вчинені або готуються. Специфіка залучення спеціаліста визначається через нормативно окреслене коло повноважень останнього та спосіб його залучення.

Надання доручення працівнику спеціальних підрозділів кіберполіції в порядку ст. 41 КПК України для проведення слідчої (розшукової) дії не визнається формою залучення спеціаліста. Спеціаліст з інформаційних технологій, електроніки й телекомунікацій може залучатися для технічної допомоги, слідчий при цьому залишається основним виконавцем слідчої (розшукової) дії. Типово спеціалістами в справах щодо досліджуваних злочинів вважаємо співробітників і працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз СБ України (ІСТЕ СБ України), інспектора-криміналіста (технік-криміналіста або керівника сектору техніко-криміналістичного забезпечення) слідчого відділу, працівників Експертної служби МВС України в складі спеціалізованої пересувної лабораторії.

14. Призначення та проведення судових експертиз є найефективнішим засобом формування доказів вчинення злочинів у кіберпросторі. Специфіка залучення експерта для проведення судової експертизи під час розслідування злочинів, вчинених у кіберпросторі, визначається потребою у одночасному призначенні та проведенні широкого спектра судових експертиз, зокрема: КТЕ; експертизи телекомунікаційних систем (обладнання); технічної експертизи документів; експертизи відеозвукозапису; відповідних комплекних експертиз.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аверина Н. А., Скрыпников А. И. Раскрытие серийных преступлений против личности и убийств, совершенных по найму : учеб.-метод. пособие. М. : ВНИИ МВД России, 1998. 56 с.

2. Аверьянов А. Н. Системное познание мира. М. : Политиздат, 1985. 263 с.

3. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : автореф. дис. ... канд. юрид. наук : 12.00.08. Київ, 2002. 18 с.

4. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. … канд. юрид. наук : 12.00.08. Київ, 2002. 231 с.

5. Азаров Д. С. Особливості механізму вчинення злочинів у сфері комп'ютерної інформації. *Юридична Україна.* 2004. № 7 (19). С. 64–68.

6. Айков Д., Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М. : Мир, 1999. 351 с.

7. Алексеев А. И. Криминология : курс лекций. М. : Щит-М, 1999. 340 с.

8. Аленін Ю. П. Початок досудового розслідування за КПК України 2012 року. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 198–203.

9. Аляєв Г. Теорія інформації на тлі історії філософії. *Науковий вісник Чернівецького університету.* 2015. Вип. 754–755. С. 3–8. (Серія «Філософія»).

10. 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.

11. Анапольська А. І. Розслідування шахрайств, пов'язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків : дис. ... канд. юрид. наук : 12.00.09. Луганськ, 2008. 225 с.

12. Андреев Б. В., Вагонова Е. А. Право и Интернет : учеб. пособие. М., 2001. 26 с.

13. Аніщенко В. М. Соціальна мобільність. *Енциклопедія освіти* / за ред. В. Г. Кременя. Київ : Юрінком Інтер, 2008. 1040 с.

14. Антонов В. М. Інтернет: енциклопедичне видання : навч.-метод. посіб. Київ : Комп'ютер, 2008. 128 с.

15. Аркуша Л. І. Основи виявлення та розслідування легалізації доходів, одержаних в результаті організованої злочинної діяльності: Интернет : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2011. 496 с.

16. Арсеньев В. Д., Заблоцкий В. Г. Использование специальных знаний при установлении фактических обстоятельств уголовного дела. Красноярск : Краснояр. ун-т, 1986. 152 с.

17. Аубакирова А. А. Ошибки допускаемые в ходе следственного осмотра при расследовании преступлений, связанных с компьютерным тероризмом. *Роль науки в повышении ефективности деятельности правоохранительных органов :* материалы Междунар. наук.-практ. конф. (Алмата, 24 июня 2011 р.). Алмата, 2011. С. 266–272. 606 с.

18. Ахмедшин Р. Л. Криминалистическая характеристика личности преступника. Томск : Томск. ун-т, 2005. 210 с.

19. Багрій М. В. Іметування обстановки злочину: поняття, зміст, місце у системі негласних слідчих розшукових дій. *Порівняльно-аналітичне право.* 2015. № 4. С. 371–374.

20. Баев О. Я. Криминалистика. Лекционный курс : учеб. пособие. 4-е изд., перераб. и доп. М. : ЮСТИЦИЯ, 2017. 372 с.

21. Баев О. Я. О методических основах расследования насильственных преступлений. *Актуальные вопросы уголовного права, процесса и криминалистики* : сб. науч. тр. Калининград, 1998. 86 с.

22. Бажанов М. И. Уголовное право Украины. Общая часть. Днепропетровск : Пороги, 1992. 168 с.

23. Бангкокська декларація про взаємодію і відповідні заходи: стратегічні союзи в галузі попередження злочинності і кримінального правосуддя : резолюція Генеральної Асамблеї ООН № 60/177, Додаток 1. URL: https://zakon3.rada.gov.ua/laws/show/995_785.

24. Бантишев О. Ф. Кримінальна відповідальність за злочини проти основ національної безпеки України (проблеми кваліфікації) : монографія. Київ : Нац. акад. СБ України, 2001. 122 с.

25. Барцицька А. А. Криміналістичні технології: сутність та місце в системі криміналістичної науки : дис. … канд. юрид. наук : 12.00.09. Одеса, 2011. 262 с.

26. Баскаков В. Інформація з обмеженим доступом: поняття та ознаки. *Актуальні проблеми державотворення :* матеріали наук.-практ. конф. (Київ, 28 черв. 2011 р.). Київ : Ліпкан О. С., 2011. С. 47–49.

27. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. М., 1991. 157 с.

28. Батурин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991. 272 с.

29. Бауэр Ф. Л., Гооз Г. Информатика : в 2 ч. М., 1990. Ч. 1 : Вводный курс. 336 с.

30. Бахін В., Лук'янчиков Б. Склад і призначення криміналістичної характеристики злочинів. *Часопис Донецького університету.* 2000. Вип. 1 (4). С. 39–44.

31. Бачило И. Л. Информационное право: основы практической информатики : учеб. пособие. М. : Юринформцентр, 2001. 352 с.

32. Безготівкові розрахунки в Україні зростають: найчастіше українці розраховуються безготівково у торговельних мережах. *Національний банк України :* [сайт]. URL: https://bank.gov.ua/control/uk/publish/article?art_id=58370337.

33. Бекетов М. Ю. Следователь органов внутренних дел и милиция: взаимодействие при расследовании преступлений : учеб. пособие. М. : Щит-М, 2004. 96 с.

34. Белкин Р. С. Криминалистика и проблемы сегодняшнего дня. *Злободневные вопросы российской криминалистики.* М. : НОРМА, 2001. 237 с.

35. Белкин Р. С. Криминалистическая энциклопедия. 2-е изд., доп. М. : Мегатрон XXI, 2000. 334 с.

36. Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 2 : Частные криминалистические теории. 464 с.

37. Белкин Р. С. Курс криминалистики : в 3 т. М. : Юристъ, 1997. Т. 3 : Криминалистические средства, приёмы и рекомендации. 480 с.

38. Белкин Р. С. Курс криминалистики : учеб. пособие. 3-е изд., доп. М. : ЮНИТИ-ДАНА ; Закон и право, 2001. 837 с.

39. Берназ В. П. Правовое и криминалистические проблемы двойственных полномочий детективов НАБУ. *Криминалист первопечатный.* 2015. № 11. С. 55–69.

40. Бернська Конвенція про захист літературних та художніх творів (Паризький акт від 24 лип. 1971 р., змінений 2 жовт. 1979 р.) : міжнар. док. від 24 лип. 1971 р. URL: http://zakon3.rada.gov.ua/laws/show/995_051/page

41. Биленчук П. Д., Еркенов С. Е., Кофанов А. В. Транснациональная преступность: состояние и трансформация : учеб. пособие / под ред. П. Д. Биленчука. Киев : Атика, 1999. 272 с.

42. Бізнес расследование «Угроза с востока». URL: http://project.liga.net/projects/eastern_threat.

43. Біленький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великої Британії та України (порівняльно-правове дослідження) : автореф. дис. … юрид. наук : 12.00.08. Київ, 2016. 20 с.

44. Біленький В. П. Відповідальність за кіберзлочини за кримінальним правом США, Великобританії та України (порівняльно-правове дослідження) : дис. ... канд. юрид. наук : 12.00.08. Одеса, 2015. 230 с.

45. Біленчук П. Д., Гель А. П., Салтевський М. В., Семаков Г. С. Криміналістика (криміналістична техніка) : курс лекцій. Київ : МАУП, 2001. 216 с.

46. Біленчук П. Д., Зубань М. А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навч. посіб. Київ : Укр. акад. внутр. справ, 1994. 72 с.

47. Біленчук П. Д., Колонюк В. П., Шульга О. О. Криміналістичне забезпечення досліджень у сфері інтелектуальної власності: історія, сьогодення, перспективи. *Криміналістика і судова експертиза.* 2016. Вип. 61. С. 467–477.

48. Біленчук П. Д., Кравчук В. В., Кравчук О. В., Кулик В. М. Комп'ютерний тероризм: практика запобігання, протидії, розслідування : навч. посіб. / за заг. ред. П. Д. Біленчука. Хмельницький : Хмельн. ЦНТЕІ, 2008. 258 с.

49. Біленчук П. Д. Криміналістичне дослідження обвинуваченого. Київ : УАВС, 1995. 128 с.

50. Білоусов А. С. Криміналістичний аналіз об'єктів комп'ютерних злочинів : дис... канд. юрид. наук : 12.00.09. Запоріжжя, 2008. 245 с.

51. Бобрицький С. М. Методичні аспекти дослідження телекомунікаційних систем (обладнання) та засобів. *Теорія та*

практика судової експертизи і криміналістики. 2008. Вип. 8. С. 445–449.

52. Богомолов М. В. Уголовная ответственность за неправомерный доступ к охраняемой законом компьютерной информации : дис. … канд. юрид. наук : 12.00.08. Красноярск, 2002. URL: https://legalns.com/download/books/lib/criminalistics/book-001.pdf.

53. Бондар А. В. Форми використання спеціальних знань під час розслідування знищення або пошкодження майна. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 3 (104). С. 46–58.

54. Бондаренко Д. А. Злочини, пов'язані з використанням владних та інших повноважень: особа злочинця як елемент криміналістичної характеристики. *Вісник Запорізького юридичного інституту.* 2000. № 2. С. 214–218.

55. Борисова Л. В. Транснаціональні комп'ютерні злочини як об'єкт криміналістичного дослідження : дис. … канд. юрид. наук : 12.00.09. Київ, 2007. 217 с.

56. Бранислав Трентовский и возникновеник кибернетики: из наследия Н. Н. Моисеева. *Экология и Жизнь*. 2007. № 8 (69). С. 15-19.

57. 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. / за ред. І. В. Бондаренко. Київ, 2009. 182 с.

58. Валуйська М. Ю. Кримінологічна характеристика особистості злочинців, що вчинили умисні вбивства при обтяжуючих обставинах : дис. ... канд. юрид. наук : 12.00.08. Харків : ХНУВС, 2002. 248 с.

59. Вапнярчук В. В. Досудове провадження. Глава 14. *Кримінальний процес* : підручник / [Ю. М. Грошевий, В. Я. Тацій, А. Р. Туманянц та ін.] ; за ред. В. Я. Тація, Ю. М. Грошевого, О. В. Капліної, О. Г. Шило. Харків : Право, 2013. 824 с.

60. Варий М. Й. Психологія : навч. посіб. 2-ге вид. Київ : Центр учб. літ., 2009. 288 с.

61. Васильев В. Л. Юридическая психология : учеб. пособие. 5-е изд., доп. и перераб. СПб. : Питер, 2005. 655 с.

62. Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2003. 1440 с.

63. Великий тлумачний словник сучасної української мови / гол. ред. В. Т. Бусел. Київ ; Ірпінь : Перун, 2005. 1728 с.

64. Великородна Д. В. Зміст і структура ринку інформаційних продуктів і послуг. *Вісник економіки транспорту і промисловості.* 2010. № 29. С. 72–76.

65. Вербець В. В., Субот О. А., Христюк Т. А. Соціологія : навч. посіб. Київ, 2009. 550 с.

66. Вертузаєв М. С., Голубєв В. О., Котляревський О. І., Юрченко О. М. Безпека комп'ютерних систем. Комп'ютерна злочинність та її попередження / за ред. О. П. Снігерьова. Запоріжжя, 1998. 316 с.

67. Вехов В. Б., Голубев В. А. Расследование компьютерных преступлений в странах СНГ : монография / под ред. Б. С. Смагоринского. Волгоград : ВА МВД России, 2004. 304 с.

68. Вехов В. Б. Компьютерные преступления: способы совершения и раскрытия / под ред. Б. П. Смагоринского. М. : Право и Закон, 1996. 182 с.

69. Вехов В. Б., Попова В. В., Илюшин Д. А. Тактические особенности расследования преступлений в сфере компьютерной информации : науч.-практ. пособие. 2-е изд., доп. и испр. М. : ЛексЭст, 2004. 160 с.

70. Взаємодія при розслідуванні економічних злочинів : монографія / [кол. авт.: А. Ф. Волобуєв, І. М. Осика, Р. Л. Степанюк та ін.] ; за заг. ред. А. Ф. Волобуєва. Харків : Курсор, 2009. 320 с.

71. Викрито хакера, який зламував облікові записи користувачів соціальних мереж. *Департамент кіберполіції :* [сайт]. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-oblikovyx-zapysiv-korystuvachiv-soczialnyx-merezh-6339.

72. Винер Н. Кибернетика. М., 1983. 352 с.

73. Використання електронних (цифрових) доказів у кримінальних провадженнях : метод. рек. / [М. В. Гребенюк, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за заг. ред. М. В. Гребенюка. Київ : МНДЦ при РНБО України, 2017. 77 с.

74. Вирок Бабушкінського районного суду м. Дніпропетровська від 24 черв. 2015 р. Справа № 1-кс/200/4990/15. Архівна справа. URL: http://reyestr.court.gov.ua/Review/45932252.

75. Вирок Бердянського міськрайонного суду Запорізької області від 5 квіт. 2016 р. Справа № 310/7032/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56953260.

76. Вирок Білоцерківського міськрайонного суду Київської області від 5 жовт. 2010 р. Справа № 1-7/2010. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/63156830.

77. Вирок Вижницького районного суду Чернівецької області від 12 груд. 2013 р. Справа № 713/2307/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/36016798.

78. Вирок Дарницького районного суду м. Києва від 28 груд. 2015 р. Справа № 753/23764/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/54799070.

79. Вирок Дарницького районного суду м. Києва від 25 жовт. 2016 р. Справа № 753/15944/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/62224792.

80. Вирок Дніпровського районного суду м. Дніпродзержинська Дніпропетровської області від 4 жовт. 2017 р. Справа № 209/3720/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/69294676.

81. Вирок Дружківського міського суду Донецької області від 11 жовт. 2016 р. ЄУН 229/2951/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/62206468.

82. Вирок Жовтневого районного суду м. Дніпропетровська від 11 серп. 2016 р. Справа № 1-кп/201/169/2016. Архівна справа. URL: http://reyestr.court.gov.ua/Review/59701953.

83. Вирок Івано-Франківського міського суду від 11 берез. 2013 р. Справа № 0907/17660/2012. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/29872888.

84. Вирок Київського районного суду м. Одеси від 12 черв. 2015 р. Справа № 520/3455/15-к. *Єдиний державний реєстр судових рішень* : [сайт]. URL: http://reyestr.court.gov.ua/Review/45059214

85. Вирок Київського районного суду м. Одеси від 24 січ. 2018 р. Справа № 520/316/18. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/71757839.

86. Вирок Кіровського районного суду м. Кіровограда від 15 лип. 2016 р. Справа № 404/3962/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/59029350.

87. Вирок Ковпаківського районного суду м. Суми від 1 черв. 2017 р. Справа № 592/4835/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/66841350.

88. Вирок Колегії суддів Печерського районного суду м. Києва від 24 берез. 2016 р. Справа № 757/27385/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56716129.

89. Вирок Колегії суддів Приморського районного суду м. Одеси від 6 черв. 2016 р. Справа № 522/6835/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/58207973.

90. Вирок Ленінського районного суду м. Полтави від 30 серп. 2016 р. Справа № 553/2825/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/60132327.

91. Вирок Луцького міськрайонного суду Волинської області від 21 жовт. 2013 р. Справа № 161/10410/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/34405754.

92. Вирок Луцького міськрайонного суду Волинської області від 12 трав. 2014 р. Справа № 161/20739/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/38642120.

93. Вирок Луцького міськрайонного суду Волинської області від 1 берез. 2018 р. Справа № 161/1345/18. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/72886703.

94. Вирок Ніжинського міськрайонного суду Чернігівської області від 6 трав. 2016 р. Справа № 740/432/15. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/57559283.

95. Вирок Нікопольського міськрайонного суду Дніпропетровської області від 2 груд. 2015 р. Справа № 182/3014/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/54012641.

96. Вирок Нікопольського міськрайонного суду Дніпропетровської області від 30 серп. 2018 р. Справа № 182/4213/18. *Єдиний державний реєстр судових рішень* : [сайт]. URL: http://reyestr.court.gov.ua/Review/76270022

97. Вирок Орджонікідзевського районного суду м. Запоріжжя від 14 січ. 2016 р. Справа № 335/859/15-к 1-кп/335/18/2016. Архівна справа. URL: http://reyestr.court.gov.ua/Review/54962947.

98. Вирок Переяслав-Хмельницького міськрайонного суду Київської області від 30 серп. 2013 р. Справа № 373/2151/13-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/33209010.

99. Вирок Придніпровського районного суду м. Черкаси від 29 січ. 2018 р. Справа № 711/9946/17 URL: http://www.reyestr.court.gov.ua/Review/71848933.

100. Вирок Рівненського міського суду Рівненської області від 15 липня 2015 року. Справі № 569/10370/14-к *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/ Review/49017035.

101. Вирок Рівненського міського суду Рівненської області від 27 лип. 2017 р. Справа № 569/10782/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/67942562

102. Вирок Соснівського районного суду м. Черкаси від 19 листоп. 2012 р. Справа № 1-443/12. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/27536021.

103. Вирок Солом'янського районного суду м. Києва від 28 листоп. 2014 р. Справа № 1-кп/760/715/14. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/41620960.

104. Вирок Соснівського районного суду м. Черкаси від 19 листоп. 2012 р. Справа № 1-443/12. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/27536021.

105. Вирок Старокостянтинівського районного суду Хмельницької області від 21 берез. 2017 р. Справа № 683/444/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/65809534.

106. Вирок Тернопільського міськрайонного суду Тернопільської області від 19 лют. 2016 р. Справа № 607/16616/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/55977478.

107. Вирок Франківського районного суду м. Львова від 23 черв. 2017 р. Справа № 465/2887/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/Review/67455018.

108. Вирок Херсонського міського суду Херсонської області 09 серп. 2018 р. Справа № 766/9634/18. *Єдиний державний реєстр судових рішень* : [сайт]. URL URL: http://reyestr.court.gov.ua/Review/75817657.

109. Вирок Шевченківського районного суду м. Запоріжжя від 26 лют. 2013 р. Справа № 1-кп/336/67/2013. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/29608881.

110. Вирок Шевченківського районного суду м. Києва від 23 квіт. 2014 р. Справа № 761/10994/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/38502750.

111. Вирок Шевченківського районного суду м. Києва від 30 листоп. 2016 р. Справа № 761/39282/16-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://www.reyestr.court.gov.ua/ Review/63392350.

112. Вирок Шевченківського районного суду м. Києва від 24 трав. 2017 р. Справа № 761/12994/17. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/ Review/66711667.

113. Вирок Шевченківського районного суду м. Чернівці від 5 трав. 2014 р. Справа № 727/11024/13-к. Архівна справа. URL: http://www.reyestr.court.gov.ua/ Review/46270509.

114. Виявлення та розлідування злочинів, пов'язаних з використанням засобів доступу до банківських рахунків : метод. рек. / [В. О. Фінагеєв, С. С. Сернявський, О. Ю. Татаров та ін.]. Київ : Нац. акад. внутр. справ, 2013. 79 с.

115. Владения ПК и список программ для резюме Александра Грак, карьерный консультант. URL: https://www.im-konsalting.ru/blog/uroven-vladeniya-kompyuterom-dlya-rezyume.

116. Власова Г. П. Співвідношення кримінальних процесуальних проваджень та диференціації кримінальних процесуальних форм. *Науково-інформаційний вісни*к. 2015. № 11. С. 153-157.

117. В Луганской области полиция разоблачили хакера, который создал и распространил вредоносный вирус-майнер. URL:

https://www.ukrinform.ru/rubric-regions/2498815-policia-razoblacila-hakera-kotoryj-sozdal-vredonosnyj-virus-dla-majninga.html.

118. Возгрин И. А., Вандышев В. В., Дербенев А. П. Криминалистическая методика расследования преступлений. Минск : Вышэйш. шк., 1983. 214 с.

119. Возгрин И. А. Введение в криминалистику: история, основы теории, библиография. СПб., 2003. 475 с.

120. Возгрин И. А. Научные основы криминалистической методики расследования преступлении : в 4 ч. СПб. : С.-петерб. юрид. ин-т МВД России, 1992. Ч. 2. 48 с.

121. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М., 2001. 496 с.

122. Волинець В. О. Віртуальна реальність: поняття та сутність. *Питання культурології*. 2014. Вип. 30. С. 35-41.

123. Волков Б. С. Проблема воли и уголовная ответственность. Казань, 1965. 136 с.

124. Волобуєв А. Ф. Економічні злочини: поняття та проблеми розробки методик розслідування. *Актуальні проблеми держави і права.* 2003. Вип. 21. С. 35–39.

125. Волобуєв А. Ф. Етапи розслідування в криміналістичній методиці. *Вісник Університету внутрішніх справ.* 1999. Вип. 5. С. 28–37.

126. Волобуєв А. Ф. Загальні положення криміналістичної методики : лекція. Харків : Ун-т внутр. справ, 1996. 36 с.

127. Волобуєв А. Ф. Комплексна методика розслідування економічних злочинів. *Вісник прокуратури.* 2003. № 6 (24). С. 53–56.

128. Волобуєв А.Ф. Механізм злочину та його зв'язок з концептуальними положеннями криміналістики: монографія. Кривий Ріг: Вид. Р. А. Козлов, 2019. 122 с.

129. Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : автореф. дис. … д-ра юрид. наук : 12.00.09. Харків, 2002. 22 с.

130. Волобуєв А. Ф. Наукові основи комплексної методики розслідування корисливих злочинів у сфері підприємництва : дис. … д-ра юрид. наук : 12.00.09. Харків, 2001. 426 с.

131. Волобуєв А. Ф. Проблемні питання початку досудового розслідування. *Актуальні проблеми кримінального права, процесу та*

криміналістики : матеріали V Міжнар. наук.-практ. конф. (Одеса, 1 листоп. 2013 р.). Одеса : Фенікс, 2013. С. 237–240.

132. Волобуєв А. Ф. Технології злочинної діяльності як об'єкт криміналістичного дослідження. *Теорія та практика судової експертизи і криміналістики :* зб. наук.-практ. матеріалів. Харків : Право, 2003. Вип. 3. С. 148–152.

133. Волчецкая Т. С. Криминалистическая ситуалогия : монография / под ред. Н. П. Яблокова. М. ; Калининград : Калинингр. ун-т, 1997. 248 с.

134. Воробей О. В. Використання спеціальних знань і призначення окремих видів судових експертиз під час розслідування кримінальних правопорушень, пов'язаних з діяльністю конвертаційних центрів. *Криміналістичний вісник.* 2017. № 1 (27). С. 154–160.

135. Воробієнко П. П., Нікітюк Л. А., Резніченко П. І. Телекомунікаційні та інформаційні мережі : підручник. Київ : Саммит-Книга, 2010. 708 с.

136. Гаврилин Ю. В. Расследование неправомерного доступа к компьютерной информации : учеб. пособие / под ред. Н. Г. Шурухнова. М. : ЮИ МВД РФ, Кн. мир, 2001. 88 с.

137. Гавло В. К. К вопросу о разработке психолого-криминалистической характеристики преступления. *Актуальные проблемы правоведения в современный период.* Томск : ТГУ, 1996. С. 185–186.

138. Гавло В. К. О следственной ситуации и методике расследования хищений, совершаемых с участием должностных лиц. *Вопросы криминалистической методологии, тактики и методики расследования*. М., 1973. С. 90–94.

139. Гавло В. К. Теоретические проблемы и практика применения методики расследования отдельных видов преступлений. Томск : Томск. ун-т, 1985. 333 с.

140. Гавловський В. Інформаційна безпека: захист інформації в автоматизованих системах (організаційно-правовий аспект). *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні*. Київ, 2000. С. 50-53.

141. Галаган В. І. Проблеми вдосконалення кримінальнопроцесуальної діяльності органів внутрішніх справ

України : монографія. К. : Нац. академія внутр. справ України, 2002. 300 с.

142. Галкин В. М. Средства доказывания в советском уголовном процессе. М. : ВНИИСЭ, 1968. Ч. 2.: Заключение эксперта. 68 с.

143. Гармаев Ю. П. Теоретические основы формирования криминалистических методик расследования преступлений : автореф. дис. … д-ра юрид. наук : 12.00.09. М., 2003. 39 с.

144. Герасимов И. Ф. Этапы раскрытия преступлений. *Следственные ситуации и раскрытие преступлений*. Свердловск, 1975. С. 10–16.

145. Герасимчук А. А., Палеха Ю. І., Шиян О. М. Соціологія : навч. посіб. 4-те вид., випр. і доповн. Київ, 2004. 246 с.

146. Герцензон А. А. Уголовное право. Общая часть. М. : РИО ВЮА, 1948. 496 с.

147. Глазычев В. Игры цивилизаций. *Век XX и мир.* 1994. № 11–12. С. 102-118.

148. Головин А. Ю., Берестнев М. А. Современные подходы к пониманию криминалистической характеристики преступлений. *Криміналістика XXI століття :* матеріали Міжнар. наук.-практ. конф. (25–26 листоп. 2010 р.). Харків : Право, 2010. С. 250–254.

149. Голубєв В. А. Аналіз кіберзлочинності у сфері економічної безпеки. *Information Technology and Security.* 2013. № 1. С. 26–32.

150. Голубєв В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій : навч посіб. / за ред. Р. А. Калюжного. Запоріжжя : ГУ ЗІДМУ, 2002. 292 с.

151. Голубєв В. О. Інформаційна безпека: проблеми боротьби з кіберзлочинністю. Запоріжжя : ЗІДМУ, 2003. 250 с.

152. Голубєв В. О., Юрченко О. М. Злочини у сфері комп'ютерної інформації: способи скоєння та засоби захисту / за ред. О. П. Снігерьова, М. С. Вертузаєва. Запоріжжя, 1998. 140 с.

153. Гончаренко В. И. Использование данных естественных и технических наук в уголовном судопроизводстве. Киев : Вища шк., 1980. 160 с.

154. Гончаренко В. И., Кушнир Г. А., Подпалый В. Л. Понятие криминалистической характеристики преступлений. *Криминалистика и судебная экспертиза :* респ. межведом. науч.-метод. сб. Киев : Вища шк., 1986. Вып. 33. С. 4–8.

155. 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.

156. Горбаньов І. М. Особливості проведення допитів окремих категорій свідків при розслідуванні незаконного розповсюдження комп'ютерних програм. *Вісник Академії адвокатури України*. 2005. Вип. 2. С. 114–118.

157. Горбачевський В. Я. Теоретико-прикладні засади розкриття умисних вбивств з кваліфікуючими ознаками : автореф. дис. … д-ра юрид. наук : 12.00.09. Київ, 2009. 34 с.

158. Городенко Л. Правові взаємини електронних видань та держави. *Наукові записки Інституту журналістики*. 2005. Т. 20. С. 11–17.

159. Грамович Г. И. Тактика использования специальных знаний в раскрытии и расследовании преступлений : учеб. пособие. Минск : Минск. высш. шк. МВД СССР, 1987. 66 с

160. Грібов М. Л. Розмежування спеціального слідчого експерименту й іметування обстановки злочину. *Науковий вісник Національної академії внутрішніх спр*ав. 2016. № 4 (101). С. 64–73.

161. Гуцалюк М. В. Проблеми протидії комп'ютерній злочинності в глобальній інформаційній мережі Internet. *Вісник Центру дослідження комп'ютерної злочинності.* 2005. № 4. URL: http://www.crime-research.org/library/Gucal.htm.

162. Дагель П. С. Классификация мотивов преступления и ее криминологическое значение. *Некоторые вопросы социологии и права* : материалы науч.-теорет. конф. Иркутск, 1967. С. 265–274.

163. Денісова О. О. Інформаційні системи і технології в юридичній діяльності : навч. посіб. Київ: КНЕУ, 2003. 315 с.

164. Дивак М. П. Системний аналіз : метод. посіб. Тернопіль, 2004. 136 с.

165. Динту В. А. Місце кіберпростору в системі обстановки злочину. *Науковий вісник Херсонського державного університету*. 2016. Вип. 2. Т. 3. С. 72-75.

166. Динту В. А. Обстановка злочину як елемент криміналістичної характеристики злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Одеса, 2014. 18 с.

167. Динту В. А. Спеціальний слідчий експеримент як форма контролю за вчиненням злочину. *Порівняльно-аналітичне право*. 2014. № 4. С. 184–186.

168. Добровольский Д. В. Актуальные проблемы борьбы с компьютерной преступностью: уголовно-правовые и криминологические проблемы : дис. ... канд. юрид. наук : 12.00.08. М., 2005. 218 с.

169. Доброродній О. А. Оперативно-розшукове забезпечення розслідування вбивств на замовлення, вчинених з корисливих мотивів у сфері підприємництва : автореф. дис. … канд. юрид. наук : 12.00.09. Дніпропетровськ : ДДУВС, 2011. 20 с.

170. Довгий С. О., Воробієнко П. П., Гуляєв К. Д. Сучасні телекомунікації: мережі, технології, безпека, економіка, регулювання / за ред. С. О. Довгого. Київ : Азимут-Україна, 2013. 608 с.

171. Договір між Кабінетом Міністрів України та Федеральним Урядом Республіки Австрія про співробітництво у сфері боротьби зі злочинністю : постанова Кабінету Міністрів від 17 лип. 2014 р. № 270. URL: http://zakon3.rada.gov.ua/laws/show/040_040

172. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : Закон України від 21 лип. 2006 р. № 23-V. URL: http://zakon1.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=994_687.

173. Додатковий протокол № 2 до Європейської Конвенції про взаємодопомогу у кримінальних справах від 20 квітня 1959 р. : міжнар. док. від 8 листоп. 2001 р. URL: http://zakon5.rada.gov.ua/laws/show/994_518/page?text=%F2%E5%EB%E5%EA%EE%EC.

174. Документування злочинів у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку при проведенні дослідчої перевірки : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за заг. ред. Л. П. Скалозуба, І. В. Бондаренко. Київ, 2010. 245 с.

175. Долженков С. О. Оперативно-розшукове забезпечення кримінального судочинства підрозділами боротьби з економічною злочинністю : автореф. дис. … канд. юрид. наук : 12.00.09. Львів : ЛьвДУВС, 2011. 20 с.

176. Дослідження інформації в пам'яті терміналів стільникового зв'язку : звіт НДР (заключ.) / ЛНДІСЕ ; наук. кер. Ю. С. Харабуга. Львів : ЛНДІСЕ, 2011. 65 с. № держ. реєстрації 0110U002599.

177. Драпкин Л. Я. Общая характеристика следственных ситуаций. *Следственная ситуация :* сб. науч. тр. М. : Всесоюз. ин-т по изучению причин и разраб. мер предупреждения преступности, 1985. 80 с.

178. Драпкин Л. Я. Предмет доказывания и криминалистические характеристики преступлений. *Криминалистические характеристики в методике расследования преступлений.* 1978. Вып. 69. С. 17–18.

179. Дримлюга Р. И. Интернет-преступность : автореф. дис. ... канд. юрид. наук : 12.00.08. Владивосток, 2007. 23 с.

180. Дубов Д. В. Кіберпростір як новий вимір геополітичного суперництва : монографія. Київ : НІСД, 2014. 328 с.

181. Дудник Л. І. Становлення і розвиток оперативно-розшукової діяльності. *Національний вісник державної податкової служби України.* 2005. № 3 (30). С. 231–238. (Серія «Економіка і право»).

182. Дюжев Д. В. Інформаційне суспільство: соціально-правова парадигма суспільного розвитку : автореф. дис. … канд. філос. наук : 09.00.03. Донецьк, 2004. 18 с.

183. Дулов А. В. Права и обязанности участников судебной экспертизы. Минск : МВССПО БССР, 1962. 408 с.

184. Эйсман А. А. Заключение эксперта. Структура и научное обоснование. М. Юрид. лит., 1967. 147 с.

185. Європейської Конвенції про видачу правопорушників: міжнар. док. від 13 груд. 1957 р. URL: http://zakon3.rada.gov.ua/laws/show/995_033.

186. Європейська Конвенція про захист прав людей та основоположних свобод : міжнар. док. від 4 листоп. 1950 р. URL: http://zakon5.rada.gov.ua/laws/show/995_004?nreg=995_004&find=1&text=%F1%EA%E0%F0&x=12&y=7#n150

187. Жаров В. О. Інтелектуальна власність в Україні: правові аспекти набуття, здійснення та захисту прав : монографія. Київ : Ін Юре, 2000. 188 с.

188. Жирний Г. Ю. До питання про класифікацію окремих криміналістичних методик. *Актуальні проблеми криміналістики :*

матер. Міжнар. наук.-практ. конф. (Харків, 25–26 верес. 2003 р.). Харків, 2003. С. 105.

189. Журавель В. А. Криміналістичні методики: сучасні наукові концепції : монографія. Харків : Апостиль, 2012. 304 с.

190. Журавель В. А. Криміналістична класифікація злочинів: засади формування та механізм застосування. *Вісник Академії правових наук*. 2002. № 3 (30). С. 160–166.

191. Журавель В. Криміналістична характеристика злочинів: проблеми формування та застосування. *Вісник Національної академії правових наук.* 2008. № 4. С. 198–209.

192. Журавель В. Проблеми періодизації досудового розслідування. *Вісник Національної академії правових наук України*. 2014. № 2 (77). С. 136–143.

193. Журавель В. Системи слідчих дій та тактичні операції в структурі окремої криміналістичної методики розслідування злочинів. *Вісник АПрН України*. 2009. № 2 (57). С. 197–208.

194. Журавель В. А. Специфика предмета допроса потерпевшего при расследовании отдельных видов преступлений. *Проблемы социалистической законности :* респ. межведом. науч. сб. Харьков : Высшая шк., 1983. Вып. 12. С. 122–125.

195. Журавель В. А. Тактичні завдання розслідування та механізм їх вирішення. *Теорія та практика судової експертизи і криміналістики.* 2017. Вип. 17. С. 11–18.

196. Журавель В. А. Технології побудови окремих криміналістичних методик розслідування злочинів. *Науковий вісник Львівської комерційної академії.* 2015. Вип. 2. С. 305–315. (Серія «Юридична»).

197. Журба А. І. Особливості предмета доказування у справах про комп'ютерні злочини : дис. ... канд. юрид. наук : 12.00.09. Харків, 2008. 191 с.

198. Зав'ялов С. М. Способи вчинення злочину: сучасні проблеми вивчення та використання у боротьбі зі злочинністю : дис. ... канд. юрид. наук : 12.00.09. Київ, 2007. 230 с.

199. Зайцев А. П., Голубятников И. В., Мешеряков Р. В., Шелупанов А. А. Програмно-апаратные средства обеспечения информационной безопасности : учеб. пособие. М. : Машиностроение-1, 2001. 260 с.

200. Затенацький Д. В. Ідеальні сліди в криміналістиці (технікокриміналістичні та тактичні прийоми їх актуалізації) : монографія / за ред. В. Ю. Шепітька. Харків : Право, 2010. 160 с.

201. Захарова І. В., Філіпова Л. Я. Основи інформаційно-аналітичної діяльності : навч. посіб. Київ : Центр учб. літ., 2013. 335 с.

202. Збірник міжнародних договорів України про правову допомогу у кримінальних справах. Багатосторонні договори. Київ : Фенікс, 2006. 800 с.

203. Звіт про результати роботи за 2016 рік Управління ООН з наркотиків та злочинності щодо кіберзлочинності. URL: http://www.unodc.org/documents/rpanc/RP_Annual_Report_RU_31.05.17_low.pdf.

204. Зейкан Я. П. Про недопустимі докази. Харків : Фактор, 2019. 128 с.

205. Зелінська Н. А. Міжнародно-правова концепція міжнародного злочину : автореф. дис. … д-ра юрид. наук : 12.00.11. Київ, 2007. 37 с.

206. Зелинский А. Ф. Осознаваемое и неосознаваемое в преступном поведении. Харьков : Вища шк., 1986. 168 с.

207. Зуев Е. И. О понятии специальных познаний в уголовном процессе. *Вопросы теории криминалистики и судебной экспертизы :* материалы науч. конф. (Москва, декабрь 1969 г.). М., 1969. Вып. 1. С. 73–76.

208. Иванов В. В. Методические рекомендации по совершенствованию взаимодействия следователя с оперативными подразделениями органов внутренних дел при раскрытии и расследовании преступлений. Чернигов, 1997. 34 с.

209. Илюшин Д. А. Особенности расследования преступлений, совершаемых в сфере предоставления услуг Интернет : дис. … канд. юрид. наук : 12.00.09. Волгоград, 2008. 237 с.

210. Информатика для гуманитариев : учебник / [Г. Е. Кедрова и др.]. М. : Юрайт, 2018. 439 с.

211. Информационная и кибербезопасность в современном мире: опыт СБУ. *Ліга: виступ А. Климчик:* [сайт]. URL: https://www.liga.net/politics/ opinion/informatsionnaya-i-kiberbezopasnost-v-sovremennom-mire-opyt-sbu.

212. Ищенко Е. П. Расследование преступлений, связанных с профессиональной деятельностью. М., 2009. 352 с.

213. Інформаційне право та правова інформатика : курс лекцій / [В. Г. Хахановський, І. В. Мартиненко, В. М. Смаглюк та ін.] ; за заг. ред. Є. М. Моісеєва. Київ : Київ. нац. ун-т внутр. справ, 2007. 253 с.

214. Как работает технология Torrent? URL: https://itproger.com/news/63.

215. Калюжный Р. А. Теоретические и практические проблемы использования вычислительной техники в системе органов внутренних дел (организационно-правовой аспект) : автореф. дис. ... д-ра юр. наук : 12.00.02. Киев, 1992. 23 с.

216. Кант И. Трактаты и письма / пер. с нем. М. : Наука, 1980. 709 с.

217. Капинус О. С. Убийства: мотивы и цели. М. : ИМПЭ-ПАБЛИШ 2003. 312 с.

218. Карпов Н. С. Злочинна діяльність : монографія. Київ : Семенко Сергій, 2004. 310 с.

219. Карчевський М. В. Відповідальність за незаконне втручання в роботу ЕОМ (комп'ютерів), систем та комп'ютерних мереж: аналіз складу злочину : дис. ... канд. юрид. наук : 12.00.08. Луганськ, 2003. 175 с.

220. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки : навч. посіб. Київ : Атіка, 2010. 168 с.

221. Кастельс М. Информационная эпоха: экономика, общество, культура / пер. с англ. ; под науч. ред. О. И. Шкаратана. М., 2000. 606 с.

222. Кіберполіція викрила шахраїв, що за допомогою СМС-розсилки ошукували громадян. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-shaxrayiv-shho-za-dopomogoyu-sms-rozsylky-oshukuvaly-gromadyan-foto-2963.

223. Ківалов С. В., Міщенко С. М., Захарченко В. Ю. Кримінальний процесуальний кодекс : наук.-практ. комент. Харків : Одіссей, 2013. 1104 с.

224. Кіпа О. Правопорушення в мережі Інтернет. *Часопис Київського університету права*. 2010. № 4. С. 346-349.

225. Клименко Н. И. Криминалистика как наука : монография. Киев : Правник, 1997. 83 с.

226. Ковалев Д. И. Криминологическая характеристика личности преступника, совершившего преступление в сфере компьютерной информации. *Вестник Академии.* 2011. № 3. С. 90–94.

227. Коваленко Є. Г. Наукові засади кримінально-процесуального доказування : монографія. Київ : Юрінком Інтер, 2011. 448 с.

228. Коваленко Е. Г. Использование экспертных знаний в деятельности органов внутренних дел : учеб. пособие. Киев : Киев. высш. шк. МВД СССР им. Ф. Э. Дзержинского, 1990. 87 с.

229. Ковальчук С. О. Вчення про речові докази у кримінальному процесі: теоретико-правові та практичні основи : монографія. Івано-Франківськ : Супрун В. П., 2017. 618 с.

230. Когутич І. І. Про перспективи «комп'ютерізації» та сутність технології в криміналістиці. *Часопис Київського університет права*. 2015. № 4. С. 255-259.

231. Козьяков Д. Масова інформація в мережі Інтернет: правові аспекти. *Вісник Національної Академії прокуратури України*. 2010. № 1. С. 120-123.

232. Колесниченко А. Н., Коновалова В. Е. Криминалистическая характеристика преступлений : учеб. пособие. Харьков : Юрид. ин-т, 1985. 92 с.

233. Колесниченко А. Н. Научные и правовые основы расследования отдельных видов преступлений : автореф. дис. ... д-ра юрид. наук : 12.00.09. Харьков, 1967. 42 с.

234. Колмогоров А. Н. Теория информации и теория алгоритмов. М. : Наука, 1987. 304 с.

235. Комп'ютерна злочинність : навч. посіб. / [П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін.]. Київ : Атіка, 2002. 240 с.

236. Конвенції ООН проти транснаціональної організованої злочинності : міжнар. док. від 15 листоп. 2000 р. URL: http://zakon3.rada.gov.ua/ laws/show/995_789.

237. Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних : міжнар. док. від 28 січ. 1981 р. URL: http://zakon5.rada.gov.ua/laws/show/994_326.

238. Конвенція про кіберзлочинність : міжнар. док. від 23 листоп. 2001 р. URL: http://zakon3.rada.gov.ua/laws/show/994_575?nreg=994_575&find=1&text=%F7%E0%F1&x=0&y=4#w11.

239. Конвенція про права дитини : міжнар. док. від 20 листоп. 1989 р. (зі змінами, схваленими резолюцією 50/155 Генеральної Асамблеї ООН від 21 груд. 1995 р., Факультативні протоколи від 1 січ. 2000 р. та 2 листоп. 2014 р.). URL: http://zakon5.rada.gov.ua/ laws/show/995_021.

240. Коновалова В. Е. Версия: концепция и функции в судопроизводстве : монография. Харьков : Консум, 2000. 176 с.

241. Коновалова В. Е. Концепция криминалистической тактики: прогнозы развития. *Актуальні проблеми криміналістики :* матеріали Міжнар. практ. конф. Харків, 2003. С. 68–72.

242. Коновалова В. О., Шепітько В. Ю. Юридична психологія : підручник. 2-ге вид., переробл. і доповн. Харків : Право, 2008. 240 с.

243. Копнин П. В. Диалектика, логика, наука. М. : Наука, 1973. 311 с.

244. Коржанський М. Й. Кримінальне право і законодавство України. Загальна частина : курс лекцій. Київ : Атіка, 2001. 432 с.

245. Корж В. П. Методика расследования экономических преступлений, совершаемых организованными группами, преступными организациями. *Руководство для следователей :* науч.-практ. пособие. Харьков, 2002. 280 с.

246. Корж В. П. Теоретические основы методики расследования преступлений, совершаемых организованными преступными образованиями в сфере экономической деятельности : монография. Харьков, 2002. 412 с.

247. Кормич Б. А. Інформаційне право : підручник. Харків, 2011. 334 с.

248. Корнилов Г. А. Расследование преступлений, совершаемых в финансово-кредитной сфере. М. ; Якутск, 2002. 252 с.

249. 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.

250. Кравцов М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків, 2016. 16 с.

251. Кривоченко Л. М. Класифікація злочинів за ступенем тяжкості у Кримінальному кодексі України : монографія. Київ, 2010. 120 с.

252. Криминалистика / под ред. Н. П. Яблокова, В. Я. Колдина. М. : МГУ, 1990. 464 с.

253. Криминалистика: расследование преступлений в сфере экономики : учебник / под ред. В. Д. Грабовского, А. Ф. Лубина. Н. Новгород : Нижегор. ВШ МВД России, 1995. 400 с.

254. Криминалистика / [Т. В. Аверьянова, Р. С. Белкин, И. А. Возгрин и др.] ; под ред. Р. С. Белкина. Москва : Акад. МВД РФ, 1995. Т. 1 : История, общая и частные теории. 279 с.

255. Криминалистика : учебник / [Т. В. Аверьянова, Р. С. Белкин и др.]. М. : НОРМА-ИНФРА, 1999. 971 с.

256. Криминалистика : учебник / [под ред. И. Ф. Пантелеева, Н. А. Селиванова]. М. : Юрид. лит., 1988. 672 с.

257. Криминалистика: Техника и тактика расследования преступлений / под ред. А. Я. Вышинского. М. : Юрид. изд-во, 1938. 540 с.

258. Криминология / под ред. А. И. Долговой. М., 1997. 784 с.

259. Криміналістика : підручник / [А. Ф. Волобуєв, О. О. Волобуєва, О. А. Самойленко та ін.] ; за ред. А. Ф. Волобуєва. Київ : КНТ, 2011. 504 с.

260. Криміналістика: підручник / [В. В. Пясковський, Ю. М. Чорноус, А. В. Іщенко та ін.]. Київ : Центр учб. літ., 2015. 544 с.

261. Криміналістика : підручник / [П. Д. Біленчук, В. К. Лисиченко, Н. І. Клименко та ін.] ; за ред. П. Д. Біленчука. 2-ге вид., випр. і доповн. Київ : Атіка, 2001. 544 с.

262. Криміналістика : підручник : у 2 т. / [В. Ю. Шепітько, В. А. Журавель, В. О. Коновалова та ін.] ; за ред. В. Ю. Шепітька. Харків : Право, 2019. Т. 1. 456 с.

263. Криминалистика : учебник / [Б. Е. Богданов и др.] ; отв ред. А. Н. Васильєв. М., 1971. 564 с.

264. Криміналістичне забезпечення виявлення і розслідування злочинів : монографія / [Л. І. Аркуша, О. Ю. Нетудихатка, О. О. Подобний та ін.] ; за ред. В. В. Тіщенка. Одеса : Гельветика, 2018. 412 с.

265. Кримінальне право України. Загальна частина : підручник / [М. І. Бажанов, Ю. В. Баулін, В. І. Борисов та ін.] ; за ред. М. І. Бажанова, В. В. Сташиса, В. Я. Тація. Київ : Юрінком Інтер ; Харків : Право, 2001. 416 с.

266. Кримінальне процесуальне право України : навч. посіб. / [К. В. Бєляєва, А. М. Бірюкова, В. І. Бояров та ін.] ; за заг. ред. В. Г. Гончаренка, В. А. Колесника. Київ : Юстиніан, 2014. 573 с.

267. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14.

268. Кримінальний процесуальний кодекс України : Закон України від 13 квіт. 2012 р. № 4651-VI. URL: https://zakon.rada.gov.ua/laws/show/4651-17.

269. Крыгин С. В. Расследование преступлений, совершаемых в сфере компьютерной информации : дис. … канд. юрид. наук : 12.00.09. Н. Новгород, 2002. 200 с.

270. Крылов В. В. Информационные компьютерные преступления : учеб. и практ. пособие. М. : Инфра-М, 1997. 285 с.

271. Крылов В. В. Расследование преступлений в сфере информации. М. : Городець, 1998. 264 с.

272. Крышов И. Ф. Пути развития тактики экспертизы. Сборник научных работ. Вид. 3. Вильнюс, 1968. С. 7–11.

273. Кудінов С. С. Використання спеціальних знань під час проведення негласних слідчих (розшукових) дій. *Вісник Академії адвокатури України.* 2014. Т. 11. № 3 (31). С. 154–161.

274. Кудінов С.С., Шехавцов Р. М., Дроздов О. М., Гриненко С. О. Негласні слідчі (розшукові) дії та використання результатів оперативно-розшуової діяльності у кримінальному провадженні: навч.-практ. посіб. 3-е вид., розш. та допов. Х. : Оберіг, 2018. 540 с.

275. Кузьмін С. А. Комп'ютерна (кібернетична) інформація як предмет вчинення злочину (кримінально-правовий аспект). *Інформація і право.* 2012. № 3 (6). С. 159–163.

276. Кузьмічов В. С., Чорноус Ю. М. Розслідування злочинів: міжнародне і національне законодавство. *Теорія і практика :* навч. посіб. Київ : КНТ, 2008. 448 с.

277. Куликов В. И. Основы криминалистической теории организованной преступной деятельности. Ульяновск : Филиал МГУ, 1994. 256 с.

278. Кулініч О. О. Доменне ім'я як похідний засіб індивідуалізації інформаційних ресурсів фізичних та юридичних осіб у мережі Інтернет. *Актуальні проблеми держави та права.* 2009. № 51. С. 195–200.

279. Курушин В. Д., Минаев В. А. Компьютерные преступления и информационная безопасность. М., 1998. 256 с.

280. Кустов А. М. Криминалистика и механизм преступления : цикл лекций. М. ; Воронеж : МОДЭК, 2002. 304 с.

281. Лавриненко В. Н., Кафтан В. В., Чернышова Л. И. Философия : учеб. и практикум / под ред. В. Н. Лавриненко. 7-е изд., перераб. и доп. М., 2015. 711 с.

282. Лазебний А. М. Використання спеціальних знань при розслідуванні кримінальних правопорушень проти громадського порядку : автореф. дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2016. 20 с.

283. Лазебний А. М. Роль спеціальних знань у кримінальному судочинстві України. *Міжнародний юридичний вісник.* 2016. Вип. 2 (4). С. 23–29.

284. Ларичев В. Д., Трунцевский Ю. В. Защита авторского и смежных прав в аудиовизуальной сфере: уголовно-правовой и криминологический аспекты. М. : Дело, 2004. 351 с.

285. Лащук Є. В. Предмет злочину в кримінальному праві : дис. … канд. юрид. наук : 12.00.08. Київ, 2005. 262 с.

286. Леонтьев А. Н. Деятельность. Сознание. Личность. М. : Политиздат, 1975. 304 с.

287. Лисенко В. В. Використання у доказовому процесі інформації, що міститься в електронному вигляді. Організація протидії злочинам у сфері інтелектуальної власності та комп'ютерних технологій: доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвідомчому семінарі-нараді / відп. ред. Л. П. Скалозуб, В. І. Василинчук, С. А. Лебідь. Київ, 2009. 114 с.

288. Лисенко В. В. Особливості допиту головного бухгалтера (керівника підприємства) у справах про ухилення від сплати податків. *Вісник прокуратури.* 2007. № 10. С. 109–114.

289. Лисиченко В. К. Использование данных естественных и технических наук в следственной и судебной практике : учеб. пособие. Киев : Вища шк., 1979. 89 с.

290. Лисиченко В. К., Циркаль В. В. Использование специальных знаний в следственной и судебной практике : учеб. пособие. Киев : КГУ, 1987. 100 с.

291. Ліпкан В. А., Капінус Л. І. Доступ до інформації з обмеженим доступом: проблеми вироблення уніфікованих дефініцій. *Публічне право*. 2013. № 4. С. 45–53.

292. Літвінов М. Ю. Світова та українська практика боротьби з кіберзлочинністю. *Право і безпека.* 2014. № 1. С. 85–89.

293. Лобойко Л. М., Банчук О. А. Кримінальний процес : навч. посіб. Київ : Ваіте, 2014. 280 с.

294. Лобойко Л. М. Кримінальний процес : підручник. Київ : Істина, 2014. 432 с.

295. Лубин А. Ф. Методология криминалистического исследования механизма преступной деятельности : дис. … д-ра юрид. наук : 12.00.09. Н. Новгород, 1997. 337 с.

296. Лубин А. Ф. Механизм преступной деятельности: развитие концепции. *Белкинские чтения «Памяти Учителя».* Н. Новгород, 2001. С. 13–22.

297. Лужецька О. Р. Предмет посягання в системі криміналістичної характеристики вимагання. *Науковий вісник Національного університету державної податкової служби України.* 2014. № 2 (65). С. 202–207. (Серія «Економіка, право»).

298. Лузгин И. М. Моделирование при расследовании преступлений. М., 1981. 152 с.

299. Лузгин И. М. Методологические проблемы расследования. М. : Юрид. лит., 1973. 216 с.

300. Лукашевич В. Г. Криминалистическая теория общения: постановка проблемы, методика исследования, перспективы использования: монографія. К. : Издательство Украинской академии внутренних дел, 1993. 194 с.

301. Лук'янчиков Є. Д. Інформаційне забезпечення розслідування злочинів (правові і тактико-криміналістичні аспекти) : дис. … д-ра юрид. наук : 12.00.09. Київ, 2005. 430 с.

302. Лук'янчиков Є. Д., Лук'янчиков Б. Є. Формування доказів у кримінальному провадженні. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2016. № 2. С. 118–129.

303. Лук'янчиков Є. Д. Методологічні засади інформаційного забезпечення розслідування злочинів : монографія. Київ : Нац. акад. внутр. справ України, 2005. 360 с.

304. Лунев В. В. Преступное поведение: мотивация, прогнозирование, профилактика. М., 1980. 263 с.

305. Мазуров В. А. Компьютерные преступления: классификация и способы противодействия : учеб.-практ. пособие. М. : Палеотип, 2002. 148 с.

306. Майданик Н. Web-сайт в мережі Інтернет як особливий об'єкт авторського права. *Юридична Україна.* 2008. № 12. С. 73–80.

307. Маклаков А. Г. Общая психология. СПб. : Питер, 2000. 592 с.

308. Марков В. В. Про механізм скоєння злочинів у кіберпросторі та особливості їх кваліфікації. *Південноукраїнський правничий часопис.* 2013. № 1. С. 112–115.

309. Марущак А. І. Інформаційне право: доступ до інформації : навч. посіб. Київ, 2007. 531 с.

310. Марущак А. І. Правові основи захисту інформації з обмеженим доступом. Київ, 2007. 208 с.

311. Масол Д. І. Мотиви расової, національної чи релігійної нетерпимості у кримінальному праві України : автореф. дис. … канд. юрид. наук : 12.00.08. Київ, 2014. 20 с.

312. Матусовський Г. А. Загальні положення методики розслідування злочинів. *Криміналістика :* підручник / за ред. В. Ю. Шепітька. Київ : Ін Юре, 2001. 684 с.

313. Матусовский Г. А. Экономические преступления: криминалистический анализ. Харьков : Консум, 1999. 480 с.

314. Мащенко П. Л., Пилипенко М. О. Технология Блокчейн и ее практическое применение. *Наука, техника, образование.* 2017. № 32. С. 61-64.

315. Мешков В. М., Попов В. Л. Оперативно-розыскная тактика и особенности легализации полученной информации в ходе предварительного следствия : учеб.-практ. пособие. М. : Щит-М, 1999. 80 с.

316. Митричев С. П. Методика расследования отдельных видов преступлений : лекции. М., 1973. 38 с.

317. Мещеряков В. А. Преступления в сфере компьютерной информации: основы теории и практики расследования. Воронеж : Воронеж. гос. ун-т, 2002. 407 с.

318. Михальчук Т. В. Використання інформації, отриманої телекомунікаційним шляхом, у розслідуванні злочинів : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 222 с.

319. Міжнародна конвенція про ліквідацію всіх форм расової дискримінації : міжнар. док. від 4 січ. 1969 р. URL: куhttp://zakon3.rada.gov.ua/laws/show/995_105

320. Міжнародний пакт про громадянські й політичні права : міжнар. док. від 16 груд. 1966 р. URL: http://zakon3.rada.gov.ua/laws/show/995_043.

321. Міненерговугілля має намір утворити групу за участю представників усіх енергетичних компаній, що входять до сфери управління Міністерства, для вивчення можливостей щодо запобігання несанкціонованому втручанню в роботу енергомереж. *Міністерство енергетики та вугільної промисловості України :* [сайт]. URL: http://mpe.kmu.gov.ua/minugol/control/uk/publish/article?art_id=245086886&cat_id=35109.

322. Морозов В. Д. Проблема развития в философии и естествознании: историко-философский очерк. Минск : Вышейшая шк., 1969. 447 с.

323. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.

324. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис. ... канд. юрид. наук : 12.00.09. Київ, 2005. 218 с.

325. Моторина Е. В. Первоначальный этап расследования нарушений авторских и смежных прав в аудиовизуальной сфере : дис. … канд. юрид. наук : 12.00.09. Ростов н/Д, 2005. 193 с.

326. Музюкин А. П. Мотив преступления и его уголовно-правовое значение : автореф. дис. … канд. юрид. наук : 12.00.08. Рязань, 2010. 23 с.

327. Надгорный Г. М. Гносеологические аспекты понятия «специальные знания». *Криминалистика и судебная экспертиза.* 1980. Вып. 21. С. 41–42

328. На Одещині кіберполіція виявила фіктивний сайт земельного кадастрового бюро. URL: https://cyberpolice.gov.ua/news/na-odeshhyni-kiberpolicziya-vyyavyla-fiktyvnyj-sajt-zemelnogo-kadastrovogo-byuro-7030.

329. Настільна книга слідчого / редкол.: В. Я Тацій, М. Г. Панов, В. Ю. Шепітько. Київ : Ін Юре, 2003. 716 с.

330. Науменко С. М. Стосовно питання щодо підробки ідентифікаційних документів. *Криміналістика і судова експертиза.* 2019. Вип. 64. С. 456–464

331. Небава М. І. Теорія корпоративного управління: вузлові питання : навч. посіб. Київ : Центр інновацій та розвитку, 2004. 295 с.

332. Негласні слідчі (розшукові) дії та особливості їх проведення оперативними підрозділами органів внутрішніх справ : навч.-практ. посіб. /[Б. І. Бараненко, О. В. Бочковий, М. Г. Вербенський та ін.] ; за ред. М. Г. Вербенського, Б. І. Бараненка. Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2014. 416 с.

333. Незалежна Асоціація банків України «Антикібер»: Кіберзлочинність: проблеми боротьби і прогнози. URL: http://anticyber.com.ua/article_detail.php?id=140.

334. Немов Р. С. Психология : учебник : в 3 кн. 4-е изд. М. : ВЛАДОС, 2003. Кн. 1 : Общие основы психологии. 688 с.

335. Никифорчук Д. Й. До питання використання результатів оперативно-розшукової діяльності у кримінальному судочинстві. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2010. Вип. 22. С. 61–66.

336. Ніколаюк С. І., Никифорчук Д. Й., Томма Р. П., Барко В. І. Протидія злочинам у сфері інтелектуальної власності (ст. 176, 177, 227, 229 КК України) : наук.-практ. посіб. Київ : КНТ, 2006. 192 с.

337. Новий тлумачний словник української мови : в 3 т. / уклад.: В. Яременко, О. Сліпушко. Київ : Аконіт, 2006. Т. 3. 926 с.

338. Нор В. Т., Бобечко Н. Р. Кримінально-процесуальне законодавство України: досягнення, загрози, очікування. *Право України*. 2016. № 12. С. 9–18.

339. Носов Н. А. Словарь виртуальных терминов. Труды лаборатории виртуалистики. *Труды Центра профориентации*. М., 2000. Вып. 7. 69 с.

340. Образцов В. А. Выявление и изобличение преступника. М. : Юристъ, 1997. 336 с.

341. Общая психология : курс лекций / сост. Е. И. Рогов. М. : ВЛАДОС, 1995. 448 с.

342. Овчинский С. С. Оперативно-розыскная информация. М. : Спарк, 2000. 220 с.

343. Одерій О. В. Криміналістична характеристика злочинів проти довкілля: проблеми побудови та використання. *Теорія та практика судової експертизи і криміналістики.* 2012. № 3. С. 51–60.

344. Одерій О. В. Предмет посягання як елемент криміналістичної характеристики злочинів проти довкілля: окремі

питання. *Ученые записки Таврического национального университета им. В. И. Вернадского.* 2013. № 1. Т. 26 (65). С. 255–259. (Серия «Юридические науки»).

345. Одерій О. В. Теорія і практика розслідування злочинів проти довкілля : монографія. Харків, 2015. 528 с.

346. Ожегов С. И., Шведова Н. Ю. Толковый словарь русского языка: 80 000 слов и фразеологических выражений. 4-е изд., доп. М. : Азбуковник, 1999. 944 с. URL: http://slovariki.org/tolkovyj-clovar-ozegova/11579.

347. Озерський І. В. Взаємодія слідчого з органом дізнання (організаційно-правовий та психологічний аналіз) : монографія. Київ, 2004. 217 с.

348. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навч. посіб. / [В. М. Бутузов, В. Д. Павловський, Л. П. Скалозуб та ін.] ; за ред. Б. В. Романюка, Є. Д. Скулиша. Київ, 2011. 404 с.

349. Орлов Ю. Ю. Застосування оперативної техніки в оперативно-розшуковій діяльності міліції (теорія і практика) : монографія. Київ : КНУВС, 2007. 559 с.

350. Орлов Ю. Ю. Організація і тактика отримання оперативно-розшукової інформації : дис. … канд.. юрид. наук : 27.07.04. Київ, 2001. 220 с.

351. Осипенко А. Л. Информационное пространство глобальных сетей как объект криминологичского изучения. *Современное право*. 2009. № 5. С. 110-114.

352. Осипенко А. Л., Кушниренко С. И. Правовые и организационные основы международного сотрудничества в противодействии трансграничным преступлениям, совершаемым с использованием Интернета. *Современное право.* 2008. № 8. С. 38–42.

353. Осипенко А. Л. Организованная преступность в сети Интернет. *Вестник Воронежского Института МВД России.* 2012. № 3. С. 10–15.

354. Особливості виявлення та розслідування злочинів у сфері використання комп'ютерних технологій : наук.-практ. посіб. / [В. М. Бутузов, В. Д. Гавловський, М. В. Гуцалюк та ін.] ; за ред. І. Є. Лазарєва, Б. В. Романюка. Київ, 2001. 90 с.

355. Остапенко Г. Комунікація та комунікативна активність суспільства в добу Інтернет-технологій: соціальний аспект. *Вісник Книжкової палати*. 2013. № 9. С. 47-49.

356. Пазиніч В. І. Правові та організаційні засади розслідування злочинів у сфері мобільних телекомунікацій України : дис. … канд. юрид. наук : 12.00.09. Київ, 2009. 217 с.

357. 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. Київ, 2004. 214 с.

358. Паляничко Д. Г. Методика розслідування злочинів, пов'язаних із дитячою порнографією : дис. ... канд. юрид. наук : 12.00.09. Одеса, 2013. 210 с.

359. Панов Н. Н. Средства совершения преступления: понятие и виды. *Проблеми законності :* респ. міжвідом. наук. зб. / відп. ред. В. Я. Тацій. Харків, 2003. С. 127–133.

360. Пастухов О. М. Авторське право в Інтернеті. Київ : Школа, 2004. 144 с.

361. Петренко-Лисак А. О. Соціальний простір у міждисциплінарному вимірі : навч. посіб. Київ : Вадекс, 2013. 400 с.

362. Петрушенко В. Л. Філософія. Курс лекцій : навч. посіб. 2-ге вид., випр. і доповн. Київ : Каравела ; Львів : Новий світ-2000, 2002. 544 с.

363. Пивоваров В. В., Щербина Л. І. Взаємодія органів досудового слідства та дізнання при розслідуванні кримінальних справ : монографія. Харків : Право, 2006. 176 с.

364. Письмо Постоянного представителя Швейцарии при ООН от 7 окт. 2004 года на имя Генерального секретаря с Приложением Отчета о Женевском этапе всемирной встречи на высшем уровне по вопросам информационного общества, Женева Palexpo, 10–12 дек. 2003 г. URL: http://www.un.org/ru/documents/ ods.asp?m=%20A/C.2/59/3.

365. Поваров Г. Н. Ампер и кибернетика. М., 1977. 95 с.

366. Погорецький М. А., Кумичко А. С. Фактичні дані та їх значення для документування оперативними підрозділами злочинів у сфері рефінансування Національним банком України вітчизняних банків. *Вісник кримінального судочинства*. 2015. № 4. С. 54–62.

367. Погорецький М. А. Оперативно-розшукова діяльність: правове визначення поняття. *Право України.* 2001. № 11. С. 122.

368. Поджаренко К. Є. Криміналістичне забезпечення розкриття і розслідування злочинних порушень прав інтелектуальної власності : автореф. дис. ... канд. юрид. наук : 12.00.09. Київ, 2009. 18 с.

369. Подільчак О. М. Мотив і мотивація злочинів учинених жінками : автореф. дис. … канд. юрид. наук : 12.00.08. Харків, 2004. 20 с.

370. Поливанюк В. Д. Тактичні особливості проведення допиту при розслідуванні злочинів, скоєних у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Теоретичні та практичні проблеми організації досудового слідства* : матеріали Всеукр. наук.-практ. конф. (Запоріжжя, 20–21 трав. 2005 р.) : у 2 ч. Запоріжжя : Юрид. ін-т МВС України, 2005. Ч. 1. С. 79–81.

371. Поліція оголосила підозру організаторам кількох онлайн-казино. URL:https://cyberpolice.gov.ua/news/policziya-ogolosyla-pidozru-organizatoram-kilkox-onlajn-kazyno-5427.

372. Положення про порядок ведення Єдиного реєстру досудових розслідувань : наказ Генеральної прокуратури України від 6 квіт. 2016 р. № 139. URL: https://www.gp.gov.ua/ua/pd.html?_m=publications&_t=rec&id=110522.

373. Проблема связей и отношений в материалистической диалектике / отв. ред. В. С. Тюхтин. М. : Наука, 1990. 288 с.

374. Пособие для следователей: расследование преступлений повышенной общественной опасности / под ред. Н. А. Селиванова, А. М. Дворядкина. М. : Лига разума, 1998. 444 с.

375. Презентація звіту Про роботу Національної комісії що здійснює державне регулювання у сфері зв'язку та інформатизації за 2017 рік. URL: https://nkrzi.gov.ua/images/upload/ 142/7598/ Presentation_2017.pdf/

376. Про авторські та суміжні права : Закон України від 23 груд. 1993 р. № 3792-XII. URL: https://zakon.rada.gov.ua/laws/show/3792-12.

377. Про банки і банківську діяльність : Закон України від 7 груд. 2000 р. № 2121-III. URL: https://zakon.rada.gov.ua/laws/show/2121-14

378. Проблемы регулирования Интернета вещей: 15-й Глобальный симпозиум для регуляторных органов (Либревиль, 8–10 июня 2015 г.)/ *Itunews*. 2015. № 4. URL: https://itunews.itu.int/Ru/Note.aspx?Note=6060.

379. Про внесення змін до деяких законодавчих актів України щодо вдосконалення окремих положень кримінального процесуального законодавства : Закон України від 4 жовт. 2019 р. № 187-IX. URL: https://zakon.rada.gov.ua/laws/show/187-20#n6.

380. Про внесення змін до деяких законодавчих актів щодо забезпечення дотримання прав учасників кримінального провадження та інших осіб правоохоронними органами під час здійснення досудового розслідування : Закон України від 16 листоп. 2017 р. № 2213-VIII. URL: https://zakon.rada.gov.ua/laws/show/2213-viii.

381. Про внесення змін до Кримінального та Кримінального процесуального кодексів України щодо невідворотності покарання за окремі злочини проти основ національної безпеки, громадської безпеки та корупційні злочини : Закон України від 7 жовт. 2014 р. № 1689-VII. URL: https://zakon.rada.gov.ua/go/1689-18.

382. Про внесення змін до Закону України «Про звернення громадян» щодо електронного звернення та електронної петиції : Закон України від 2 лип. 2015 р. № 577-VIII. URL: http://zakon.rada.gov.ua/laws/show/577-19#n2.

383. Про державну підтримку кінематографії в Україні : Закон України від 23 берез. 2017 р. № 1977-VIII. URL: https://zakon.rada.gov.ua/laws/show/1977-19.

384. Про Державну службу спеціального зв'язку та захисту інформації України : Закон України від 23 лют. 2006 р. № 3475-IV. URL: https://zakon.rada.gov.ua/laws/show/3475-15.

385. Про державну таємницю : Закон України від 21 січ. 1994 р. № 3855-XII. URL: https://zakon.rada.gov.ua/laws/show/3855-12.

386. Про доступ до публічної інформації : Закон України від 13 січ. 2011 р. № 2939-VI. URL: https://zakon.rada.gov.ua/ laws/show/2939-17.

387. Про Єдиний реєстр досудових розслідувань : наказ Генеральної прокуратури України від 17 серп. 2012 р. № 69. URL: https://zakon.rada.gov.ua/rada/card/v0069900-12.

388. Про затвердження Інструкції з організації взаємодії органів досудового розслідування з іншими органами та підрозділами Національної поліції України в запобіганні кримінальним правопорушенням, їх виявленні та розслідуванні: Наказ МВС України від 07 лип. 2017 р. № 575. URL : https://zakon.rada.gov.ua/laws/show/z0937-17.

389. Про затвердження Інструкції з організації проведення та оформлення експертних проваджень у підрозділах Експертної служби Міністерства внутрішніх справ України : наказ МВС України від 17 лип. 2017 р. № 591. URL: https://zakon.rada.gov.ua/laws/show/z1024-17?find=1&text=%F1%F2%F0%EE%EA#w12.

390. Про затвердження Інструкції про організацію проведення негласних слідчих (розшукових) дій та використання їх результатів у кримінальному провадженні : наказ ГП України, МВС України, СБ України, Адміністрації державної прикордонної служби України, Міністерства Фінансів України, Міністерства юстиції України від 16 лист. 2012 р. № 114/1042/516/1199/936/1687/5. URL: https://zakon2.rada.gov.ua/laws/show/v0114900-12.

391. Про затвердження Інструкції про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі в проведенні огляду місця події : наказ МВС України від 3 листоп. 2015 р. № 1339. URL: https://zakon.rada.gov.ua/laws/show/z1392-15?find=1&text=%F1%E5%EA%F2%EE%F0#w11.

392. Про затвердження Інструкції про призначення та проведення судових експертиз та експертних досліджень та Науково-методичних рекомендацій з питань підготовки та призначення судових експертиз та експертних досліджень : наказ Міністерства юстиції України від 8 жовт. 1998 р. № 53/5. URL: https://zakon.rada.gov.ua/laws/show/z0705-98?find=1&text=%EA%EE%EC%EF%27%FE%F2%E5%F0#w110.

393. Про затвердження Інструкції про участь співробітників та працівників Українського науково-дослідного інституту спеціальної техніки та судових експертиз Служби безпеки України як спеціалістів в кримінальному провадженні : наказ СБ України від 19 берез. 2016 р. № 138. URL: https://zakon.rada.gov.ua/laws/show/z0564-16?lang=ru.

394. Про затвердження переліку об’єктів державної власності, що мають стратегічне значення для економіки і безпеки держави : постанова Кабінету Міністрів України від 4 берез. 2015 р. № 83. URL: http://zakon5.rada.gov.ua/laws/show/83-2015-%D0%BF.

395. Про затвердження Положення про Департамент кіберполіції НП України : наказ Національної поліції України від

10 листоп. 2015 р. № 85. *Офіційний матеріал Департаменту Документального забезпечення Національної поліції України.*

396. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 9 серп. 2012 р. № 691 (втратив чинність на підставі наказу МВС України від 3 листоп. 2015 р. № 1343). URL: https://zakon.rada.gov.ua/laws/show/z1541-12.

397. Про затвердження Положення про Експертну службу Міністерства внутрішніх справ України : наказ МВС України від 3 листоп. 2015 р. № 1343. URL: https://zakon.rada.gov.ua/laws/show/z1390-15

398. Про завтвердження Порядку ведення єдиного обліку в органах (підрозділах) поліції заяв і повідомлень про кримінальні правопорушення та інші події : наказ МВС України від 8 лют. 2019 р. № 100. URL: https://zakon.rada.gov.ua/laws/show/z0223-19#n7.

399. Про затвердження Порядку розгляду звернень та організації проведення особистого прийому громадян в органах та підрозділах Національної поліції України : наказ МВС України від 15 листоп. 2017 р. № 93. URL: http://zakon.rada.gov.ua/laws/show/z1493-17.

400. Про затвердження Правил надання та отримання телекомунікаційних послуг : постанова Кабінету Міністрів від 11 квіт. 2012 р № 295. URL: http://zakon2.rada.gov.ua/laws/show/295-2012-%D0%BF/page?text=%F1%EF%E0%EC#w11

401. Про захист інформації в інформаційно-телекомунікаційних системах : Закон України від 5 лип. 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.

402. Про захист персональних даних : Закон України від 1 черв. 2010 р. № 2297-VI. URL: http://zakon2.rada.gov.ua/laws/show/2297-17.

403. Про заходи протидії незаконному обігу наркотичних засобів, психотропних речовин і прекурсорів та зловживанню ними : Закон України від 15 лют. 1995 р. № 62/95-ВР URL: https://zakon.rada.gov.ua/laws/show/62/95-%D0%B2%D1%80.

404. Про звернення громадян : Закон України від 2 жовт. 1996 р. № 393/96-ВР. *Відомості Верховної Ради України.* 1996. № 47. Ст. 256.

405. Про інформацію: Закон України від 2 жовт. 1992 р. № 2657-XII URL: https://zakon.rada.gov.ua/laws/show/2657-12

406. Про Національну комісію, що здійснює державне регулювання у сфері зв`язку та інформатизації : Указ Президента України від 23 листоп. 2011 р. № 1067/2011. URL: https://zakon.rada.gov.ua/laws/show/1067/2011.

407. Про Національну поліцію України : Закон України від 2 лип. 2015 р. № 580-VIII. URL : https://zakon.rada.gov.ua/ laws/show/580-19.

408. Про національну програму інформатизації : Закон України від 4 лют. 1998 р. № 74/98-ВР. URL: https://zakon.rada.gov.ua/ laws/show/74/98-%D0%B2%D1%80.

409. Про оперативно-розшукову діяльність: Закон України від 18 лют. 1992 р. № 2135-XII URL: https://zakon.rada.gov.ua/laws/show/2135-12.

410. Про організацію діяльності органів досудового розслідування Національної поліції України : наказ МВС України від 6 лип. 2017 р. № 570. URL:https://zakon.rada.gov.ua/laws/show/z0918-17?find=1&text=%EA%F0%E8%EC%B3%ED %E0%EB%B3%F1%F2#w136.

411. Про основи національної безпеки України : Закон України від 19 черв. 2003 р. № 964-IV. URL: http://zakon2.rada.gov.ua/ laws/show/964-15.

412. Про основні засади забезпечення кібербезпеки України : Закон України від 5 жовт. 2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19.

413. Про платіжні системи та переказ коштів в Україні : Закон України 5 квіт. 2001 р. №2346-III-ВР. URL: https://zakon.rada.gov.ua/ laws/show/2346-14.

414. Про приєднання України до Бернської конвенції про охорону літературних і художніх творів (Паризького акта від 24 лип. 1971 р., зміненого 2 жовт. 1979 р.) : Закон України від 31 трав. 1995 р. № 189/95-ВР. URL: http://zakon3.rada.gov.ua/laws/show/189/95-D0%B2%D1%80.

415. Про приєднання України до міжнародної конвенції про охорону інтересів виконавців, виробників фонограм і організацій мовлення : Закон України від 20 верес. 2001 р. № 2730-III-ВР. URL: http://zakon3.rada.gov.ua/laws/show/2730-14

416. Про прийняття Протоколу про внесення змін до Угоди ТРІПС : Закон України 3 лют. 2016 р. № 981-VIII. URL: http://zakon5.rada.gov.ua/laws/show/981-19/paran2#n2.

417. Про ратифікацію Другого додаткового протоколу до Європейської конвенції про взаємну допомогу у кримінальних справах : Закон України від 1 черв. 2011 р. № 3449-VI. URL: http://zakon5.rada.gov.ua/laws/show/3449-17

418. Про ратифікацію Європейської конвенції про видачу правопорушників 1957 р., Додаткового протоколу 1975 р. та Другого додаткового протоколу 1978 р. до Конвенції : Закон України від 16 січ. 1998 р. № 43/98. URL: http://zakon3.rada.gov.ua/laws/show/43/98-%D0%B2%D1%80.

419. Про ратифікацію Конвенції Міжнародної організації праці № 182 про заборону та негайні заходи щодо ліквідації найгірших форм дитячої праці : Закон України від 5 жовт. 2000 р. № 2022-III. URL: http://zakon3.rada.gov.ua/laws/show/2022-14.

420. Про ратифікацію Конвенції ООН проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів суходолом, морем і повітрям) : Закон України від 4 лют. 2004 р. № 1433-IV. *Відомості Верховної Ради України.* 2004. № 19. Ст. 263.

421. Про ратифікацію Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додаткового протоколу до Конвенції про захист осіб у зв'язку з автоматизованою обробкою персональних даних стосовно органів нагляду та транскордонних потоків даних : Закон України від 6 лип. 2010 р. № 2438-VI. URL: http://zakon5.rada.gov.ua/laws/show/2438-17.

422. Про ратифікацію Конвенції про захист прав людини і основоположних свобод 1950 р., Першого протоколу та протоколів № 2, 4, 7 та 11 до Конвенції : Закон України від 17 лип. 1997 р. № 475/97-ВР. URL: http://zakon3.rada.gov.ua/laws/show/ru/475/97-%D0%B2%D1%80.

423. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 7 верес. 2005 р. № 2824-IV-ВР. URL: http://zakon3.rada.gov.ua/laws/show/2824-15.

424. Про ратифікацію Конвенції про права дитини : постанова ВР УССР від 27 лют. 1991 р. № 789-XII. URL: http://zakon5.rada.gov.ua/laws/show/789-12.

425. Про ратифікацію Міжнародного пакту про економічні, соціальні і культурні права та Міжнародного пакту про громадянські й політичні права : Указ Президії ВР УСРС від 19 жовт. 1973 р. № 2148-VIII. URL: http://zakon3.rada.gov.ua/laws/show/2148-08.

426. Про рішення Ради національної безпеки і оборони України від 27 січ. 2016 р. «Про Стратегію кібербезпеки України» : Указ Президента України від 15 берез. 2016 р. № 96/2016. URL: http://zakon.rada.gov.ua/laws/show/96/2016#n11.

427. Про Службу безпеки України : Закон України від 25 берез. 1992 р. № 2229-XII. URL: https://zakon.rada.gov.ua/laws/show/2229-12.

428. Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. *Відомості Верховної Ради України.* 1994. № 28. Ст. 232

429. Про схвалення Стратегії розвитку інформаційного суспільства в Україні : розпорядження Кабінету Міністрів України від 15 трав. 2013 р. № 386-р. URL: https://zakon.rada.gov.ua/laws/show/386-2013-%D1%80.

430. Протасевич А. А., Зверянская Л. П. Особенности осмотра места происшествия по делам о киберпреступлениях. *Известия Иркутской государственной экономической академии (Байкальский госуниверситет экономики и права).* 2013. № 2. С. 23–26.

431. Про телекомунікації : Закон України від 18 листоп. 2003 р. № 1280-IV-ВР. URL: https://zakon.rada.gov.ua/laws/show/1280-15.

432. Протидія економічній злочинності / [П. І. Орлов, А. Ф. Волобуєв, І. М. Осика та ін.]. Харків : Нац. ун-т внутр. справ, 2004. 568 с.

433. Протидія кіберзлочинності : бібліограф. покажчик літ. / уклад.: Н. А. Косенкова, Т. О. Сіродан. 2-е вид., доповн. Київ, 2014. 48 с.

434. Путренко А. М. Мережа Інтернет як об’єкт дослідження при здійсненні оперативно-розшукової діяльності. *Актуальні проблеми управління інформаційною безпекою держави* : зб. матеріалів наук.-практ. конф. (17 берез. 2010 р.). Київ : Наук.-вид. відділ НА СБ України. 2010. 279 с.

435. Пчеліна О. В. Криміналістична класифікація злочинів. *Право і суспільство.* 2014. № 6-1. Ч. 2. С. 304–309.

436. Пчеліна О. В. Теоретичні засади формування та реалізації методики розслідування злочинів у сфері службової діяльності : автореф. … дис. д-ра юрид. наук : 12.00.09. Харків, 2017. 40 с.

437. Радецька В. Я. Мова науки криміналістики : дис. ... канд. юрид. наук : 12.00.09. Київ, 2002. 173 с.

438. Ревака В. М. Форми використання спеціальних пізнань у досудовому провадженні : дис. … канд. юрид. наук : 12.00.09. Харків, 2006. 180 с.

439. Регистрация оператором, провайдером в НКРСИ. URL: https://ogp.ua/ru/razresheniya-na-deyatelnost/registratsiya-operatorom-provajderom.

440. Реєстр методик проведення судових експертиз. *Міністерство юстиції України :* [сайт]. URL: http://rmpse.minjust.gov.ua/search

441. Реєстр операторів, провайдерів телекомунікацій. URL: https://nkrzi.gov.ua/index.php?r=site/index&pg=55&language=uk.

442. Реєстр щодо платіжних організацій, систем та операторів послуг платіжної інфраструктури. URL: https://bank.gov.ua/control/uk/publish/article?art_id=8436153.

443. Реуцький А. В. Методика розслідування злочинів у сфері виготовлення та обігу платіжних карток : автореф. дис. ... канд. юрид. наук : 12.00.09. Харків, 2009. 22 с.

444. Рішення Конституційного суду України у справі за конституційним поданням Жашківської районної ради Черкаської області щодо офіційного тлумачення положень частин першої, другої статті 32, частин другої, третьої статті 34 Конституції України : рішення Конституційного суду України від 20 січ. 2012 р. № 2-рп/2012. URL: http://zakon2.rada.gov.ua/laws/show/v002p710-12.

445. Рогозин В. Ю. Особенности расследования и предупреждения преступлений в сфере компьютерной информации : автореф. дис. … канд. юрид. наук : 12.00.09. Волгоград, 1998. 20 с.

446. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис. ... канд. юрид. наук : 12.00.08. Київ, 2003. 222 с.

447. Розова С. С. Методологические основы психологии : учеб. пособие. Новосибирск, 2013. Ч. 1 : Теория познания. 132 с.

448. Розова С. С. Научная классификация и ее виды. *Вопросы философии.* 1964. № 8. С. 68–79.

449. Розслідування злочинів, вчинених з використанням шкідливих програмних чи технічних засобів : метод. рек. /

[О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко та ін.]. Київ, 2016. 56 с.

450. Розслідування злочинів, пов'язаних з незаконним розповсюдженням у мережі Інтернет недійного контенту провайдерами програмних послуг та Інтернет-провайдерами : метод. рек. / [О. М. Стрільців, О. С. Тарасенко, І. Р. Курилін та ін.]. Київ, 2017. 44 с.

451. Романов С. Ю. Обман як спосіб злочинної діяльності : автореф. дис. ... канд. юрид. наук : 12.00.08. Харків, 1998. 16 с.

452. Романюк Б. В., Гавловський В. Д., Гуцалюк М. В., Бутузов В. М. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій / за ред. Я. Ю. Кондратьєва. Київ : Паливода А. В., 2004. 144 с.

453. Романюк Ю. В. Сучасні теоретичні та правові проблеми використання спеціальних знань у досудовому слідстві : дис. … канд. юрид. наук : 12.00.09. Київ, 2002. 217 с.

454. Россинская Е. Р., Усов А. И. Судебная компьютерно-техническая экспертиза. М. : Право и закон, 2001. 411 с.

455. Рудік В. М. Оперативно-розшукове забезпечення кримінального судочинства у справах про корисливо-насильницькі злочини : дис. … канд. юрид. наук : 21.07.04. Дніпропетровськ, 2006. 210 с.

456. Савченко А. В. Мотив і мотивація злочину : монографія. Київ : Атіка, 2002. 144 с.

457. Садчікова К. А. Використання спеціальних знань на стадії досудового розслідування (процесуальний аспект) : дис. … канд. юрид. наук : 12.00.09. Одеса, 2017. 233 с.

458. Салтевский М. В Криминалистическая характеристика: структура, элементы. *Специализированный курс криминалистики :* учебник. Киев, 1987. 520 с.

459. Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навч. посіб. Харків, 2000. 35 с.

460. Салтевский М. В. Проблема соотношения специальных и профессиональных знаний, используемых при производстве следственных действий. *Становление и развитие органов внутренних дел Украинской ССР.* Киев : КВШ МВД СССР, 1973. С. 134–135

461. Самойленко О. А. Інформаційний продукт як предмет посягання при вчиненні злочинів із використанням обстановки кіберпростору. *Вчені записки Таврійського національного університету імені В. І. Вернадського.* 2018. Т. 29 (68). № 4. С. 165–169. (Серія «Юридичні науки»).

462. Самойленко О. А. Криміналістичний та правовий аналіз злочинної діяльності в мережі Інтернет. *Порівняльно-аналітичне право.* 2015. № 4. С. 408–411.

463. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 250 с.

464. Самойленко О. А. Особливості розслідування викрадень майна, вчинених із використанням комп'ютерних технологій : монографія. Київ : КНТ, 2009. 328 с.

465. Самойлов С. В. Розслідування шахрайств, учинених із використанням мережі «Інтернет» : дис. … канд. юрид. наук : 12.00.09. Донецьк, 2014. 226 с.

466. Сатуев Р. С., Шраер Д. А., Яськова Н. Ю. Экономическая преступность в финансово-кредитной системе. М. : Центр экономики и маркетинга, 2000. 272 с.

467. Селиванов Н. А. Математические методы в собирании и исследовании доказательств. М. : Юрид. лит., 1974. 120 с.

468. Семинар-практикум 3: Укрепление мер реагирования систем предупреждения преступности и уголовного правосудия на появляющиеся формы преступности, такие как киберпреступность и незаконный оборот культурных ценностей, в том числе извлеченные уроки и международное сотрудничеств : справочный док. 13 Конгресс ООН по предупреждению преступности и уголовному правосудию (Доха, 12–19 апр. 2015 г. (A/CONF.222/12). URL: http://www.unodc.org/documents/congress/Documentation/A-CONF.222-12_Workshop3/ACONF222_12_r_V1500665.pdf.

469. Сергєєнкова О. П., Столярчук О. А., Коханова О. П., Пасєка О. В. Загальна психологія : навч. посіб. Київ : Центр учб. літ., 2012. 296 с.

470. Симонян Е. А. Единство теории и практики: философский анализ. М. : Наука, 1980. 240 с.

471. Скулиш Є. Д., Петрик В. М. Сутність інформаційно-психологічного впливу. *Актуальні проблеми управління*

інформаційною безпекою : зб. матеріалів наук.-практ. конф. (Київ, 17 берез. 2010 р.). Київ : Наук.-вид. відділ НА СБ України, 2010. 279 с.

472. Слепухина А. С. Компьютерные информационные технологии : курс лекций. Витебск : МИТСО, 2009. 201 с.

473. Словник української мови : в 11 т. / за ред. І. К. Білодіда. Київ : Наук. думка, 1970–1980. Т. 4. URL: http://sum.in.ua/.

474. Словник української мови : в 11 т. / [редкол.: І. К. Білодід (гол.) та ін.]. Київ : Ін-т мовознавства НАН УРСР, 1975. Т. 6 : П-Поїти. 832 с.

475. Смелік В. Б. Кореляційні зв'язки між окремими видами злочинів у сфері підприємництва (проблеми методики розслідування) : автореф. дис. … канд. юрид. наук : 12.00.09. Харків, 2006. 20 с.

476. Смоков С. М. Окремі проблемні питання, які виникають при застосуванні норм нового КПК України. *Юридичний часопис Національної академії внутрішніх справ.* 2013. № 1. С. 110–115.

477. Снігерьов О. П., Голубєв В. О. Проблеми класифікації злочинів у сфері комп'ютерної інформації. *Вісник Університету внутрішніх справ МВС України.* 1999. № 5. С. 25–28.

478. Создание эффективной программы ООН в области предупреждения преступности и уголовного правосудия : Резолюция Генеральной Ассамблеи ООН от 18 дек. 1991 г. № 46/152. URL: http://base.garant.ru/2565318/#ixzz4xKtuj3dP.

479. Сокал Р. Р. Кластер-анализ и классификация: предпосылки и основные направления. *Классификация и кластер*. М., 1980. 389 с.

480. Соколовский З. М. Понятия специальных знаний. К вопросу об основаниях назначения экспертизы. *Криминалистика и судебная экспертиза.* 1969. Вып. 6. С. 202–204.

481. Соснін О. В. Державна політика в галузі управління інформаційним ресурсом України : автореф. дис. ... д-ра політ. наук : 23.00.02. Одеса, 2005. 36 с.

482. Старушкевич А. В. Криміналістична характеристика злочинів : навч. посіб. Київ : Правник, 1997. 44 с.

483. Степанов Ю. В. Використання комп'ютерних засобів під час проведеення оперативно-розшукових заходів. *Ученые записки Таврического национального университета им. В. И. Вернадского.* 2013. № 2-1. Ч. 2. С. 342–348.

484. Стецик Б.В. Особливості тактичних, процесуальних та організаційних засад підготовки, призначення та проведення судово-подчеркознавчої експертизи. *Науковий вісник Львівської комерційної академії. Серія : Юридична*. 2015. Вип. 1. С. 246-260.

485. Столяр О. Міжнародно-правові проблеми визначення та класифікації кіберзлочинів. *Национальный юридический журнал* (науч.-практ. правов. изд. Респ. Молдова). 2017. IULIE. С. 185-188.

486. Строгович М. С. Уголовный процесс : учеб. пособие. М., 1938. 248 с.

487. Стрюк М. І., Семеріков С. О., Стрюк А. М. Мобільність: системний підхід. *Інформаційні технології і засоби навчання.* 2015. № 5. Т. 49. С. 37–70.

488. Сферы жизни общества: энциклопедия экономиста. URL: http://www.grandars.ru/college/sociologiya/sfera-obshchestva.html.

489. Таблица подписей и ратификации договора Совета Европы № 185 «Convention on Cybercrime». URL: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=dfS8PM6Z.

490. Танасевич В. Г. Проблемы раскрытия и расследования преступлений. *Советская криминалистика. Теоретические проблемы.* М., 1978. 245 с.

491. Таран О. В. Криміналістичне забезпечення розслідування злочинної діяльності у сфері порушення авторських прав : автореф. дис. … канд. юрид. наук : 12.00.09. Київ, 2005. 20 с.

492. Тарарухин С. А. Установление мотива и квалификация преступления. Київ : Вища шк., 1977. 152 с.

493. Тарасюк А. В. Доказування у справах про несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку у стадії досудового розслідування : монографія. Харків : ФІНН, 2011. 192 с.

494. Татаров О. Ю. Досудове провадження в кримінальному процесі України: теоретико-правові та організаційні засади (за матеріалами МВС) : монографія. Донецьк : Промінь, 2012. 640 с.

495. Теплицький Б. В., Шарай Л. Г., Ковальов К. М., Кузьмін С. А. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку : наук.-практ. посіб. Київ : Паливода А. В., 2019. 168 с.

496. Тертишник В. М. Кримінально-процесуальне право України : підручник. 4-те вид., доповн. і переробл. Київ : А.С.К., 2003. 1120 с.

497. Тертышник В. М. Нетрадиционные способы и формы собирания и исследования доказательств при расследовании преступлений. Харьков : ХИВД, 1994. 56 с.

498. Тимошенко П. Ю., Салтевский М. В., Жариков Ю. Ф. Теория и практика использования следов памяти (идеальных отображений) в расследовании преступлений / отв. ред. Р. С. Белкин. Киев : Укр. акад. внутр. дел, 1991. 88 с.

499. Тіщенко В. В. Концептуальні основи розслідування корисливо-насильницьких злочинів : дис. … д-ра юрид. наук : 12.00.09. Одеса, 2003. 445 с.

500. Тіщенко В. В. Теоретичні і практичні основи методики розслідування злочинів : монографія. Одеса : Фенікс, 2007. 260 с.

501. Тіщенко В. В. Технологічний підхід як новаційний напрямок у розвитку криміналістичної науки. *Науковий вісник Львівської комерційної академії*. 2015. Вип. 2. С. 322–323. (Серія «Юридична»).

502. Ткач О. В. Предмет злочинного посягання як елемент криміналістичної характеристики порушень недоторканності приватного життя. *Юрист України.* 2014. № 4 (29). С. 136–141.

503. Толковый словарь русского языка С. И. Ожегова. URL: http://slovariki.org/tolkovyj-clovar-ozegova/11579.

504. Транснациональная организованная преступность: дефиниции и реальность : монография / отв. ред. В. А. Номоконов. Владивосток : Дальневост. ун-т, 2001. 375 с.

505. Трунцевский Ю. В. Интеллектуальное пиратство: гражданско-правовые и уголовно-правовые меры противодействия. М. : Юрист, 2002. 148 с.

506. Угоди ВОІВ про авторське право за Міжнародною Конвенцією про захист виконавців, виробників фонограм і організацій мовлення (Римська конвенція): вчинено в Римі 26 жовт. 1961 р. URL: http://zakon3.rada.gov.ua/laws/show/995_763.

507. Угоди про торговельні аспекти прав інтелектуальної власності : міжнар. док. від 15 квіт. 1994 р. URL: http://zakon5.rada.gov.ua/laws/show/981_018.

508. Узагальнення Вищого спеціалізованого суду України з розгляду цивільних і кримінальних справ «Про практику розгляду скарг на рішення, дії чи бездіяльність органів досудового розслідування чи прокурора під час досудового розслідування» (станом на 12.01.2017). URL: http://protokol.com.ua/ua/vssu_uzagalnennya_pro_praktiku_rozglyadu_skarg_na_rishennya_dii_chi_bezdiyalnist_organiv_dosudovogo_rozsliduvannya.

509. У Києві відпустили адміністраторів груп смерті. URL: https://tsn.ua/kyiv/u-kiyevi-vidpustili-administratoriv-grup-smerti-yaki-viyavilisya-studentami-medikami-zmi-887068.html.

510. Ухвала Колегії суддів судової палати у кримінальних справах апеляційного суду Дніпропетровської області від 10 берез. 2016 р. Справа № 182/3014/15-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/56361518.

511. Ухвала Шевченківського районного суду м. Києва від 7 квіт. 2014 р. Справа № 761/10495/14-к. *Єдиний державний реєстр судових рішень :* [сайт]. URL: http://reyestr.court.gov.ua/Review/38305124.

512. Федотов Н. Н. Форензика – компютерная криминалистика. М. : Юрид. мир, 2007. 360 с.

513. Филиппов А. Г. К вопросу об особенностях расследования отдельных видов и групп преступлений. *Особенности расследования отдельных видов и групп преступлений*. Свердловск, 1980. С. 23–27.

514. Фокина А. А. Роль криминалистической характеристики преступлений в укреплении связи науки криминалистики и практики расследования. *Криминалистика и судебная экспертиза*. 1990. Вып. 41. С. 17–21.

515. Фролов О. П. Поняття та основні риси обшуку у формі спеціальної операції. *Міжнародний юридичний вісник: актуальні проблеми сучасності (теорія та практика)*. 2018. Вип. 1–2. С. 318–324.

516. Халілев Р. А. Система принципів оперативно-розшукової політики з протидії злочинності на грунті етно-конфесій них суперечностей. *Учені записки Таврійського національного університету ім. В. І. Вернадського*. 2010. № 1. Т. 23 (62). С. 328–336. (Серія «Юридичні науки»).

517. Хараберюш І. Ф., Мацюк В. Я., Некрасов В. А., Хараберюш О. І., Хараберюш І. Ф. Використання оперативно-

технічних засобів у протидії злочинам, що вчиняються у сфері нових інформаційних технологій : монографія. Київ : КНТ, 2007. 196 с.

518. Харабуга Ю. С., Білий С. Б. Дослідження мобільних телефонів і смарт-карт до них у межах комп'ютерно-технічної експертизи. *Теорія та практика судової експертизи і криміналістики.* 2009. Вип. 9. С. 454–458.

519. Харабуга Ю. С. Комп'ютерно-технічне дослідження мобільних телефонів, смартфонів та SIM-карт. *Криміналістика та судова експертиза.* 2014. Вип. 59. С. 335–342.

520. Хатунцев Н. А. О специальных знаниях, необходимых при исследовании компьютерных средств и систем. *Актуальные проблемы российского права.* 2010. № 1. С. 332–339

521. Хахановський В. Кіберзлочинність: застосування сучасних технологій при вчиненні злочинів – проблеми досудового розслідування та міжнародної співпраці. *Правова інформатика.* 2007. № 1 (13). С. 68–73.

522. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинів. *Юридичний часопис Національної академії внутрішніх справ*. 2011. № 1 (1). С. 89–93.

523. Хомколов В. П. Организация управления оперативно-розыскной деятельностью: системный поход. М. : Закон и право ; ЮНИТИ, 1999. 191 с.

524. Цехан Д. М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ : монографія / за ред. О. О. Подобного. Одеса : Юрид. літ., 2011. 216 с.

525. Цивільне право України. Загальна частина / за ред. І. А. Бірюкова, Ю. О. Заіки. Київ : Алеута, 2014. 510 с.

526. Цимбал П. В., Омельчук Л. В. Перспективи удосконалення інституту судової експертизи у кримінальному процесуальному законодавстві України. *Юридичний часопис Національної академії внутрішніх справ* 2013. № 1. С. 75–81.

527. Черкасов В. Н. Дело «балаковских» хакеров. Факты и размышления. *Информационная безопасность регионов.* 2009. № 2 (5); 2010. № 1 (6); 2010. № 2 (7); 2011. № 1 (8). С. 158–163.

528. Чернявський С. С. Фінансове шахрайство: методологічні засади розслідування : монографія. Київ : Хай-Тек Прес, 2010. 624 с.

529. Чуприна О. Співвідношення понять «персональні дані», «інформація про особу», «конфіденційна інформація про особу». *Підприємство, господарство і право.* 2013. № 1. С. 104–108.

530. Чурилов С. Н. Криминалистическая методика: история и современность. М. : Маркетинг, 2002. 370 с.

531. Шавер Б. М. Об основных принципах частной методики расследования преступлений. *Социалистическая законность.* 1938. № 1. С. 42–56.

532. Шалева О. І. Електронна комерція : навч. посіб. Київ : Центр учб. літ., 2011. 216 с.

533. Шахбазян К. С. Міжнародно-правові основи регулювання відносин в мережі Інтернет : дис... канд. юрид. наук : 12.00.11. Київ, 2009. 222 с.

534. Шиканов В. И. Актуальные вопросы уголовного судопроизводства и криминалистики в условиях современного научно-технического прогресса. Иркутск : Восточ.-Сибир. кн. изд-во, 1978. 190 с.

535. Шиканов В. И. Проблемы использования специальных познаний и научно-технических новшеств в уголовном судопроизводстве : автореф. дис. … д-ра юрид. наук : 12.00.09. М., 1980. 31 с.

536. Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации. Луганск : РИО ЛИВД, 1999. 64 с.

537. Шилін М. Національна безпека: проблеми правового забезпечення діяльності суб'єктів сектору безпеки та можливі шляхи вирішення. *Освіта і наука у сфері національної безпеки: проблеми та пріоритети розвитку :* матеріали Міжнар. наук.-практ. конф. (Острог, 1 груд. 2017 р.) / за заг. ред. М. С. Романова. Острог : Нац. ун-т «Острозька академія», 2017. 180 с.

538. Шевчишен А. В. Легальні дефініції слідчих (розшукових) та негласних слідчих (розшукових) дій. *Формування правових позицій щодо розслідування міжнародних злочинів* : зб. наук. пр., матеріали конф. (семінарів, круглих столів). Київ : КНУВС, 2016. С. 260–263.

539. Шевчишен А. В. Поняття спеціального досудового розслідування (in absentia) та його функціональне призначення у кримінальних провадженнях щодо корупційних злочинів у сфері службової діяльності та професійної діяльності, пов'язаної з наданням

публічних послуг. *Вісник кримінального судочинства.* 2017. № 2 С. 125–134.

540. Шевченко Е. С., Михайлюченко Н. Н. Киберпространство как элемент обстановки совершения преступлений. *Академический юридический журнал*. 2015. № 1. С. 52–59.

541. Шевчук В. М. Тактичні операції у криміналістиці: теоретичні засади формування та тактика реалізації : монографія Харків : Апостіль, 2013. 440 с.

542. Шендрик В. В., Сафронов С. О., Крєпаков І. О., Жилін Є. В. Боротьба з порнографією: криміналістичні та оперативно-розшукові аспекти : науково-практичний посібник. Харків, 2010. 216 с.

543. Шепітько В. Ю. Допит : наук.-практ. посіб. Харків : Крим-Арт, 1998. 214 с.

544. Шепітько В. Ю., Журавель А. В., Авдєєва Г. К. Інновації в криміналістиці та їх впровадження в діяльність органів досудового слідства. *Питання боротьби зі злочинністю.* 2011. № 21. С. 39–45

545. Шепітько В. Ю. Криміналістика : підручник. Київ, 2010. 496 с.

546. Шепітько В. Ю. Криміналістика : енцикл. слов. (укр.-рос. і рос.-укр.): 1500 термінів / з ред. В. Я. Тація. Харків : Право, 2001. 554 с.

547. Шепитько В. Ю. Тактика расследования преступлений, совершаемых организованными группами и преступными организациями. Харьков, 2000. 88 с.

548. Шептулин А. П. Диалектический метод познания. М. : Политиздат, 1983. 320 с.

549. Шмонин А. В. Методика расследования преступлений : учеб. пособие. М. : Юстицинформ, 2006. 464 с.

550. Шмонин А. В. Методология криминалистической методики : монография. М., 2010. 416 с.

551. Шурухнов Н. Г. Криминалистика : учебник. 2-е изд., испр. и доп. М. : Эксмо, 2008. 720 с.

552. Щербаковский М. Г., Кравченко А. А. Применение специальных знаний при раскрытии и расследовании преступлений. Харьков : Ун-т внутр. дел, 1999. 78 с.

553. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : навч. посіб. Харків : ХНУВС, 2010. 112 с.

554. Щербаковський М.Г. Призначення та провадження судових експертиз. Харків : Фактор, 2011. 400 с.

555. Щур Б. В. Теоретичні основи формування та застосування криміналістичних методик : дис. … д-ра юрид. наук : 12.00.09. Харків, 2011. 407 с.

556. Юрчишин В. Д. Висновок експерта як джерело доказів у кримінальному процесі України : дис. … канд. юрид. наук : 12.00.09. Івано-Франківськ, 2007. 227 с

557. Юдин Э. Г. Системный подход и принцип деятельности. М., 1978. 391 с.

558. Яблоков Н. П. Научные основы методики расследования. *Криминалистика* : учебник. М., 1995. 708 с.

559. Яремчук В. О. Організація і тактика залучення спеціаліста при проведенні слідчих (розшукових) дій : монографія / за ред. В. Ю. Шепітька. Харків : Апостіль, 2015. 227 с.

560. Crime scene cyberspace. *Globe*. 2012. No. 3. Sept. URL: https://www1.ethz.ch/zisc/events/ETHglobe_ZISC_SEP2012.pdf.

561. April Mara, Norm Origin and Development in Cyberspace: Models Of Cybernorm Evolution. *Washington University Law Quarterly*. 2000. No. 78. P. 59–80.

562. Barlow J. P. A Declaration of the Independence of Cyberspace. URL: https://w2.eff.org/Censorship/Internet_censorship_bills/barlow_0296.declaration.

563. Clean IT – Leak shows plans for large-scale, undemocratic surveillance of all communications. 2012. 21 sep. URL: https://edri.org/cleanit.

564. Gibson W. Count Zero. An Ace Science Fiction Book. New York, 1986. URL: http://www.onread.com/fbreader/1414365/.

565. Complexity Science – Complexity Science Complexity Science. www.complexity.org.uk (en-US). Процитовано 2018-11-07. URL: https://www.crayon.com.

566. Heim M., Helsel Ed. S. K., Roth J. P. The Metaphysics of Virtual Reality. *Virtual Reality: Theory, Practiceand Promise.* London, 1991. P. 27–33.

567. James R. Hansen Technology and the History of Aeronautics: An Essay. URL: http://www. centennialofflight.net/essay/ Evolution_of_Technology/Tech-OV1.htm.

568. Liu Yuping and Shrum L. J. What is Interactivity and is it Always Such a Good Thing? Implications of Definition, Person, and

Situation for the Influence of Interactivity on Advertising Effectiveness. *Journal of Advertising.* 2002. No. 31 (4). P. 53–64. URL: https://www.yupingliu.com/files/papers/liu_shrum_interactivity.pdf.

569. Keith N., Hampton, Lauren F. Sessions, Eun Ja Her, Lee Rainie Social Isolation and New Technology. How the internet and mobile phones impact Americans' social networks. URL: http://www.pewinternet.org/ 2009/11/04/social-isolation-and-new-technology.

570. PRECEDENTUA–2016 / [В. Лужковська, В. Щепотка, В. Капустинський та ін.]. Київ : КВІЦ, 2017. 326 с.

571. SEO Словник : соц. мережа. URL: //igroup.com.ua/seo-articles/sotsialna-merezha/.

Наукове видання

Самойленко Олена Анатоліївна

ОСНОВИ МЕТОДИКИ РОЗСЛІДУВАННЯ ЗЛОЧИНІВ, ВЧИНЕНИХ У КІБЕРПРОСТОРІ

Монографія

За редакцією доктора юридичних наук, професора А.Ф. Волобуєва

Підписано до друку 10.01.2020 р.
Формат 60х84/16 Папір офсетний. Ум. друк. арк. 22,09
Наклад 300 прим. Замовлення 0041
Видавництво та друкарня "ТЕС"
(Свідоцтво ДК № 771) Одеса, Канатна 81/2.
Тел.:(0482) 42-90-98, (0482) 42-89-72