

МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

ВОЛКОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ



УДК 343.98

**ПОЧАТКОВИЙ ЕТАП РОЗСЛІДУВАННЯ СТВОРЕННЯ
ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ
ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ**

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

Автореферат
дисертації на здобуття наукового ступеня
кандидата юридичних наук

Дніпро–2023

Дисертацією є рукопис

Роботу виконано в Науково-дослідному інституті публічного права.

Науковий керівник –

кандидат юридичних наук, доцент

Солдатенко Олена Анатоліївна,

Дніпропетровський державний університет внутрішніх справ,

професор кафедри кримінального процесу

та стратегічних розслідувань.

Офіційні опоненти:

доктор юридичних наук, професор

Дрозд Валентина Георгіївна,

Державний науково-дослідний інститут МВС України,

начальник 3-го науково-дослідного відділу науково-дослідної

лабораторії проблем правового та організаційного

забезпечення діяльності Міністерства;

кандидат юридичних наук, доцент

Дубівка Ірина Володимирівна,

Національна академія внутрішніх справ,

доцент кафедри кримінального процесу.

Захист відбудеться 19 травня 2023 року о 12.00 годині на засіданні спеціалізованої вченої ради Д 08.727.02 у Дніпропетровському державному університеті внутрішніх справ за адресою: 49000, м. Дніпро, просп. Гагаріна, 26.

Із дисертацією можна ознайомитись у загальній бібліотеці Дніпропетровського державного університету внутрішніх справ (м. Дніпро, просп. Гагаріна, 26).

Автореферат розіслано 18 квітня 2023 року.

**Учений секретар
спеціалізованої вченої ради**



В.С. Березняк

ЗАГАЛЬНА ХАРАКТЕРИСТИКА РОБОТИ

Актуальність теми. Кримінальні правопорушення у сфері інформаційних технологій у сучасних умовах розвитку українського суспільства набули суттєвої поширеності. Оновлення національної правової системи поставило перед правоохоронними органами невідкладні завдання щодо захисту гарантованих Конституцією України прав. Порушення таких прав під час користування електронно-обчислювальною технікою, мережі Інтернет переважно відбувається за допомогою спеціально створених або пристосованих шкідливих програмних засобів, використання яких призводить до суспільно негативних наслідків у вигляді матеріальних збитків, викрадення, спотворення чи знищення конфіденційної інформації. Водночас посилення боротьби зі злочинами потребує науково-обґрунтованої методики.

У засобах масової інформації, в офіційних джерелах зустрічаються повідомлення про наслідки створення, використання та розповсюдження шкідливих програмних засобів у вигляді виходу з ладу ЕОМ, комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також різного обладнання пов'язаного з цим, про економічні та моральні збитки як наслідок несанкціонованого втручання і неконтрольованого розповсюдження шкідливих програмних засобів. Одним із засобів, якщо і не вирішення проблеми створення шкідливих програм чи технічних засобів з метою протиправного використання, розповсюдження або збуту, то принаймі гальмування її загострення є притягнення винних осіб до юридичної відповідальності, зокрема, кримінальної.

Таким чином, протидія злочинам проти створення шкідливих програм чи технічних засобів із метою протиправного використання, розповсюдження або збуту наразі набуває першочерговості, в тому числі і для правоохоронних органів. З огляду на значущість кримінально-правового інструментарію законодавець окремо виділив норми про кримінальну відповідальність за створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут. Таке рішення було викликане, перш за все, поширеністю таких правопорушень за умови їх високої латентності та важливістю вказаних інформаційних об'єктів для суспільства.

Виходячи з аналізу кримінальних проваджень на території України, зазначені правопорушення мають тенденцію до зростання, оскільки як свідчить статистика, за період з 2013 по 2017 роки їх кількість становила 103 зареєстрованих факти про вчинення, що менше, більш як у 2.5 рази показника за період 2018-2022 років (278 зареєстрованих правопорушень). Окрім цього, слід, на нашу думку звернути увагу на те, що всього було прийнято рішення про повідомлення про підозру осіб-правопорушників у 119 кримінальних провадженнях (за період 2018-2022 років), проти 22 таких рішень в період 2013-2017 років.

Судово-слідча практика відчуває гостру потребу в сучасних методичних рекомендаціях щодо проведення досудового розслідування кримінальних правопорушень зазначеної категорії особливо на його початковому етапі. Та обставина, що ключові завдання досудового розслідування проти (щодо) створення шкідливих програм чи технічних засобів з метою протиправного використання, розповсюдження або збуту вирішуються саме на його початковому етапі, й обумовлює актуальність обраної теми дисертації. У криміналістичній же науці ці питання залишаються малодослідженими. Необхідно зазначити, що останнім часом на законодавчому рівні проведено значну роботу щодо врегулювання суспільних відносин у сфері протидії створенню, використанню та розповсюдженню шкідливих програмних засобів. Однак розроблення лише нормативно-правової бази для ефективного регулювання і охорони суспільних відносин у цій сфері недостатньо.

Проблемами розслідування створення, використання та розповсюдження шкідливих програмних засобів в останні роки приділяли певну увагу в своїх дослідженнях такі вчені як: К. Архіпова, Ю. Батурин, В. Бахін, П. Біленчук, Т. Бірюкова, В. Бурлака, В. Бутузов, С. Великанов, А. Волобуєв, В. Гавло, Ю. Гаврилин, Г. Гапотченко, В. Гончаренко, В. Гора, І. Горбаньов, В. Дрозд, І. Дубівка, Р. Дударець, І. Європіна, Я. Ілляш, М. Коваленко, Я. Конюшенко, В. Коршунов, В. Кузнецов, М. Макаров, Т. Михайліна, О. Моїсеєв, Р. Недов, Д. Письменний, О. Пінчук, С. Прутяний, Р. Сабадаш, М. Салтевський, Н. Селіванов, О. Солдатенко, О. Снігерьов, А. Старушкевич, А. Тарасюк, О. Татаров, Л. Удалова, М. Хавронюк, В. Хахановський, М. Цуцкірідзе, С. Чернявський, А. Шевчишен та інші. Зазначені роботи були присвячені досудовому розслідуванню окремих видів злочинів проти створення шкідливих програм чи технічних засобів із метою протиправного використання, розповсюдження або збуту. Значною мірою проведено дослідження ґрунтувалося на концептуальних положеннях таких кандидатських дисертацій як Б. Теплицького «Техніко-криміналістичне забезпечення розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж електрозв'язку» (2021 рік), О. Мотлях «Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій» (2005 рік). Були використані й праці вітчизняних і зарубіжних учених у галузі кримінології, кримінального та кримінального процесуального права.

Зв'язок роботи з науковими програмами, планами, темами. Тема дисертації ґрунтується на Плані дій з реалізації Національної стратегії у сфері прав людини на період до 2020 року (розпорядження Кабінету Міністрів України від 23 листопада 2015 р. № 1393-р), Стратегії реформування судоустрою, судочинства та суміжних правових інститутів на 2015-2020 роки (указ Президента України від 20 травня 2015 р. № 276/2015), Національній стратегії у сфері прав людини (Указ Президента України від 25 серпня 2015 р. № 501/2015), Рішенні Ради національної безпеки і оборони України «Про

заходи щодо посилення боротьби зі злочинністю в Україні» від 06 травня 2015 р. (Указ Президента України від 16 червня 2015 р. № 341/2015 року), Стратегії сталого розвитку «Україна – 2020» (Указ Президента України від 12 січня 2015 р. № 5/2015), Пріоритетних напрямках розвитку правової науки на 2016–2020 роки, затверджених постановою загальних зборів Національної академії правових наук України від 03 березня 2016 р., відповідає Переліку пріоритетних напрямів наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років (наказ МВС України від 16 березня 2015 р. № 275), тематиці наукових досліджень і науково-технічних (експериментальних) розробок на 2020–2024 роки (наказ МВС України № 454/2020).

Мета і задачі дослідження. *Метою* дисертації є формування теоретичних засад і практичних рекомендацій, спрямованих на удосконалення початкового етапу розслідування злочинів у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів.

Поставлена мета зумовила необхідність вирішення таких *задач*:

– охарактеризувати стан наукових досліджень щодо формування методики розслідування створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– сформулювати поняття та визначити сутність створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

– обґрунтувати криміналістичну класифікацію створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– визначити основні джерела криміналістичної значимої інформації під час досудового розслідування створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– проаналізувати способи створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– надати криміналістичну характеристику особі-правопорушнику, що створює з метою використання, розповсюдження або збуту шкідливі програмні чи технічні засоби;

– змодельювати типові слідчі ситуації та програми дій слідчого на початковому етапі досудового розслідування створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– проаналізувати засади криміналістичного версіювання у досудовому розслідуванні створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– визначити і обґрунтувати особливості тактики проведення окремих слідчих (розшукових) дій у досудовому розслідуванні створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів;

– встановити специфіку використання спеціальних знань під час розслідування створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів.

Об'єкт дослідження – кримінально-процесуальні правовідносини, що виникають, змінюються та припиняються на початковому етапі досудового розслідування кримінальних правопорушень щодо створення шкідливих програм чи технічних засобів з метою протиправного використання, розповсюдження або збуту.

Предмет дослідження – початковий етап розслідування створення використання, розповсюдження або збуту шкідливих програмних чи технічних засобів.

Методи дослідження. У методологічному підході до розв'язання поставлених завдань та мети дослідження, автором було застосовано широкий інструментарій, що включає в себе як загальнонаукові методи, котрі відкрили можливість охарактеризувати зміст і сутність злочинної діяльності (підрозділ 1.1., 1.2., 1.3., 1.4.) та процесу здійснення досудового розслідування (підрозділи 2.1., 2.2., 2.3., 3.1., 3.2.) наприклад, у результаті застосування методів порівняння та спостереження), так і специфічні методи пізнання юридичної дійсності та наукової матерії, наприклад: *історико-правовий* – котрий уможливив проведення історіографічного аналізу процесів становлення інституту кримінально-правової охорони відповідної галузі правовідносин, а також функціонування механізму досудового розслідування (підрозділи 1.1, 1.2, 2.1); *порівняльно-правовий* – котрий уможливив комплексний і системний аналіз законодавчої та правозастосовної практики не лише в межах окремих історичних періодів, а й у розрізі функціонування аналогічних інститутів права в інших, закордонних країнах (підрозділи 2.1, 2.2, 3.2, 3.3); *догматичний* – що вможливив комплексний і змістовний аналіз усіх понятійно-категоріальних елементів (підрозділи 1.1., 1.2., 2.1., 2.3.); *системний* – що дозволив послідовно, структуровано та комплексно підійти до вирішення поставлених завдань й вирішувати їх у порядку накопичення, від концептуальних до локальних (підрозділи 1.2, 1.3); *соціологічний* – для проведення власного соціологічного опитування та аналізу вже проведених досліджень, що коригують практику правозастосування та допомогли в виявленні нових проблемних питань, а також пошуці шляхів їх розв'язання (2.2., 2.3.); *статистичний* – що був застосований під час дослідження матеріалів кримінальних проваджень, а також судової та іншої статистики пов'язаної зі здійсненням досудового розслідування відповідного кола кримінальних правопорушень (розділи 1.4., 2.2., 2.3.).

Емпіричну базу дослідження склали Конституція України, Закони та постанови Верховної Ради України, ратифіковані Україною міжнародні договори, конвенції, угоди, укази Президента України, декрети та постанови Кабінету міністрів України, що регулюють суспільні відносини у сфері попередження, розкриття та розслідування злочинів, чинні відомчі нормативні акти та інструктивні документи Міністерства внутрішніх справ України,

статистичні та аналітичні матеріали Національної поліції України, Офісу Генерального прокурора, Державної судової адміністрації; результати вивчення 623 кримінальних проваджень щодо злочинів такої категорії; зведені дані опитування 275 слідчих та працівників оперативних підрозділів Національної поліції України, а також 258 учасників кримінальних проваджень, які брали участь в опитуванні у ході здійснення досудового розслідування про кіберзлочини; досвід роботи автора в слідчих підрозділах Міністерства внутрішніх справ України, Національній поліції України та у судовій системі.

Наукова новизна одержаних результатів полягає в тому, що за характером і змістом розглянутих проблем дисертація є першим в Україні монографічним дослідженням, в якому комплексно проведено дослідження початкового етапу розслідування створення, використання та розповсюдження шкідливих програмних засобів, розроблено його теоретичні засади та надано практичні рекомендації щодо підвищення ефективності практичної діяльності органів досудового розслідування. У межах проведеного дослідження отримано результати, що містять відповідні ознаки наукової новизни, а саме:

вперше:

– розроблено застосування антивірусних програмних засобів, а також спеціально розроблених програмно апаратних комплексів з метою вилучення необхідної інформації, під час проведення слідчих (розшукових) дій, значно підвищує результативність здійснення такого розслідування та окреслено алгоритм використання здобутих у такий спосіб доказів у досудовому розслідуванні відповідної категорії кримінальних проваджень;

– сформульовано криміналістичний зміст таких понять як «шкідливі програмні засоби», котрі розглядаються як спеціально створені для перешкоджання нормальному функціонуванню електронно-обчислювальних машин і програмних пристроїв компоненти чи цілі програми, а також «шкідливі технічні засоби», що розглядається як змодельовані пристрої та елементи обладнання, котрі за своїм функціональним призначенням здатні нанести шкоду електронно-обчислювальним машинам і пристроям чи програмному забезпеченню відповідного обладнання;

удосконалено:

– розуміння та наукову концепцію, щодо розмежування криміналістичних методик здійснення досудового розслідування використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також інших, супутніх протиправних посягань у відповідній сфері;

– криміналістичні підходи щодо класифікації та визначення сутності особи, яка використовує, розповсюджує або збуває шкідливі програмні чи технічні засоби, що безпосередньо пов'язується з процесами в досудовому розслідуванні, наприклад виявленням додаткових джерел доказів, котрі доводять винуватість відповідної особи;

– розуміння типологічного підходу до розв'язання завдань в досудовому розслідуванні використання, розповсюдження або збуту

шкідливих програмних чи технічних засобів, а також положень криміналістичної методики щодо програмування дій слідчого на початковому етапі такого процесу, на підставі заяви про вчинення кримінального правопорушення, а також допитів потерпілого та свідків;

– техніко-юридичні уявлення про процедуру збору доказової інформації слідчим, прокурором, а також спеціалістом, під час проведення низки слідчих (розшукових) дій, що передбачають обов'язкове вилучення матеріальних носіїв (об'єктів матеріального світу), котрі містять в собі цифрові (електронні) докази;

дістало подальший розвиток:

– концептуальне розуміння злочинності в сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, що дозволяє в подальшому формувати уявлення про типовість програм дій слідчого на початковому етапі здійснення такого досудового розслідування, що значно спрощує роботу не лише молодим, а й значно більш досвідченішим працівникам;

– сегмент криміналістичної методики здійснення досудового розслідування використання, розповсюдження або збуту шкідливих програмних чи технічних засобів в частині вдосконалення змістовного та сутнісного наповнення категорії «обстановка вчинення», що вважається досить розгалуженою в вітчизняній юриспруденції та потребує подальшого уточнення в контексті здійснення досудового розслідування інших кримінальних правопорушень в сфері незаконного використання шкідливих програмних чи технічних засобів, що не підпадають під кваліфікаційні ознаки відповідного складу кримінального правопорушення;

– позиція автора про необхідність ґрунтовного доопрацювання не лише положень КК України, а й кримінального процесуального законодавства й доповнення останнього додатковими нормами й положеннями щодо кваліфікації окремих форм використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, що носять суспільно-небезпечний характер, а також учинення зазначеного в умовах дії правового режиму воєнного стану.

Практичне значення одержаних результатів полягає в тому, що сформульовані та аргументовані в дисертації теоретичні положення, висновки й пропозиції впроваджено та надалі може бути використано у:

законотворчій діяльності – під час опрацювання змін і доповнень до КПК України (акт Інституту законодавства Верховної Ради України від 16 травня 2019 року № 22/108-1-15);

практичній діяльності органів досудового розслідування у кримінальних провадженнях про кримінальні правопорушення, пов'язані з несанкціонованому втручанні в ЕОТ, створення, використання та розповсюдження ШПЗ (акт впровадження Головного слідчого управління Національної поліції України № 30085 від 10 листопада 2022 року)

науково-дослідній роботі – під час подальшого опрацювання

проблемних питань пов'язаних із формуванням окремих аспектів методики досудового розслідування кримінальних проваджень, пов'язаних із несанкціонованим втручанням в ЕОТ, створення, використання та розповсюдження ШПЗ (акт впровадження Науково-дослідного інституту публічного права від 11 листопада 2022 року);

навчальному процесі – при підготовці розділів підручників, лекційних матеріалів, розробленні методичних рекомендацій при викладанні розділів методики розкриття та розслідування окремих видів злочинів курсів «Криміналістики», та спецкурсу «Актуальні проблеми розкриття та розслідування злочинів», а також при проведенні занять за відповідними дисциплінами в системі підготовки та підвищення кваліфікації слідчих та працівників оперативних підрозділів (акт впровадження Національної академії внутрішніх справ від 18 травня 2018 року).

Апробація результатів дисертації. Основні положення та висновки дослідження доповідалися автором на міжнародних і всеукраїнських науково-практичних конференціях, а саме: «Аспекти взаємодії оперативних підрозділів та слідчих апаратів на стадії перевірки матеріалів стосовно несанкціонованого доступу у сфері комп'ютерних технологій». (м. Київ, 2005 р.); «Кадрове забезпечення експертної діяльності при розслідуванні злочинів у сфері створення, розповсюдження і збуту шкідливих програмних засобів». (м. Тернопіль, 2006 р.); «Виявлення доказової інформації при розслідуванні створення, використання, розповсюдження і збуту шкідливих програмних засобів». (м. Запоріжжя, 2007 р.); «Специфічність інформації як об'єкт посягання на приватність» (Львів, 2008 р.); «Знаряддя вчинення злочину при розслідуванні злочинів пов'язаних з створенням, використанням, розповсюдженням і збутом шкідливих програмних засобів» (м. Тернопіль, 2008 р.); «Злочини в банківській сфері, що вчиняються за допомогою спеціально створених шкідливих програмних засобів» (м. Севастополь, 2010 р.); «Поняття, види та протидія Інтернет-злочинності в глобальних соціальних мережах» (м. Хмельницький, 2010 р.); «Заходи забезпечення кібербезпеки підприємницької діяльності» (м. Київ, 2018 р.); «Актуальні проблеми діяльності органів досудового розслідування в умовах воєнного стану» (м. Дніпро, 2022 р.).

Публікації. Основні положення та результати дисертації відображено у вісімнадцяти наукових працях, із яких вісім наукових статей у виданнях, включених до переліку наукових фахових видань України, одна у періодичному науковому виданні іншої держави за профілем дисертації, дев'ять тез доповідей на науково-практичних конференціях.

Структура та обсяг дисертації. Дисертація складається з основної частини (вступу, трьох розділів, що вміщують дев'ять підрозділів, висновків), списку використаних джерел і додатків. Загальний обсяг дисертації становить 197 сторінок, з яких 155 сторінок основного тексту. Список використаних джерел налічує 130 найменувань і займає 13 сторінок, додатки викладено на 30-и сторінках.

ОСНОВНИЙ ЗМІСТ РОБОТИ

У **вступі** обґрунтовано актуальність теми дисертації; визначено її зв'язок із науковими програмами, планами, темами; сформульовано мету, задачі, об'єкт, предмет, методи дослідження; розкрито наукову новизну, практичне значення отриманих результатів; надано відомості про апробацію і публікації автора, структуру та обсяг дисертації.

Розділ 1 «Науково-методологічний підхід формування криміналістичної методики розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» складається з чотирьох підрозділів.

У підрозділі 1.1 *«Стан наукових досліджень проблем криміналістичної характеристики та початкового етапу розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів»* констатовано, що відповідне питання широко досліджувалось науковцями та дослідниками, а також активно використовується в законодавстві України, що створює підґрунтя для його широкого та обґрунтованого тлумачення.

Праці, зокрема й міжнародних дослідників уможливили досягнення автором сталої думки щодо розуміння поняття й сутності явища «шкідливих програмних чи технічних засобів», довести, що визначення даного кримінального правопорушення побудоване на міждисциплінарному кримінально-правовому та криміналістичному розумінні феномену протиправної поведінки, пов'язаної з використанням новітніх інформаційних технологій.

Відсутність чіткого визначення поняття шкідливих програмних засобів дозволило правопорушникам у деяких випадках уникати відповідальності за їх учинення, ускладнило роботу правоохоронних та судових органів у частині уніфікованого застосування законодавства, покликаного подолати кіберзлочинність, що також наразі є досить дискусійним у наукових колах. Важливим також є те, що відповідне питання є полідисциплінарним і тому, автором було проаналізовано значну частку позицій і думок дослідників, зокрема, з технічних галузей знань, що безпосередньо надають відповідні технічні характеристики шкідливим програмним чи технічним засобам і дозволяють формувати низку юридичних критеріїв, що є межами поведінки у зазначених правовідносинах і впливають на можливість притягнення до кримінальної відповідальності.

Автором обґрунтовується, що шкідливим програмним засобом є такий вид контенту (код, скрипт, програмне забезпечення), який існує в кіберсередовищі, спеціально створений, конструктивно призначений та технічно придатний для несанкціонованого втручання в роботу електронно-обчислювальної техніки та призводить до будь-якого порушення нормального функціонування (порядку обігу) інформації та впливає на споживання

технічних ресурсів електронно-обчислювальної техніки.

У підрозділі 1.2 «Способи створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» розкрито зміст і сутність поняття способу вчинення кримінальних правопорушень щодо створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. Доведено, що відповідна категорія охоплює собою ті кримінально карані діяння, що вчиняються шляхом застосування розробок шкідливого програмного забезпечення у вигляді створення, копіювання, оптимізації самовідтворення та інкорпорації у програмне забезпечення або його розповсюдження із використанням можливостей програмних комп'ютерних мереж, що власне й утворює механізм вчинення кримінального правопорушення.

Особливість характеристики способу вчинення відповідного кримінального правопорушення полягає у його технологічних особливостях, що мають бути використані зловмисником обов'язково (що власне й обґрунтовано в інших підрозділах), оскільки його професійна (кібернетична) підготовленість є однією з умов можливості використання саме такого способу вчинення кримінального правопорушення.

У підрозділі 1.3 «Криміналістична класифікація, обстановка та слідова картина, під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» аргументовано, що зміст і сутність криміналістичної класифікації кримінальних правопорушень у сфері відтворення з метою використання, розповсюдження або збуду шкідливих чи технічних програмних засобів полягає в відокремленні всіх імовірних форм його учинення в межах конкретно визначеної мети.

Оскільки криміналістична класифікація в даному розрізі поєднує в собі як критерії визначені в межах відповідного складу кримінального правопорушення в Кримінальному кодексі України так і сукупність криміналістико-теоретичних ознак основний акцент автором було зроблено на встановлення змісту й сутності таких понять як «використання», «розповсюдження», «збут», а також «шкідливі програмні засоби» та «шкідливі технічні засоби», що в залежності від співвідношення їх наявності чи відсутності в складі кримінального правопорушення є підставою для коригування методики досудового розслідування відповідного правопорушення.

Водночас, у загальному контексті було доведено, що кримінальним правопорушенням у сфері створення, використання, розповсюдження чи збуту шкідливих програмних засобів слід вважати винне кримінально каране діяння, вчинене одноосібно чи групою осіб із метою нанесення негативних наслідків іншому комп'ютерному програмному забезпеченню для отримання матеріальної чи іншої нематеріальної вигоди, що завдало збитків охоронюваним законом інтересам шляхом порушення функцій програмного чи інформаційно-комунікативного забезпечення комп'ютерного обладнання, а також комунікативних мереж і електронних накопичувальних пристроїв.

У підрозділі 1.4 «Характеристика осіб, які створюють, використовують, розповсюджують або збувають шкідливі програмні чи технічні засоби» встановлено, що криміналістична характеристика особи-правопорушника, є однією з найбільш важливих у контексті формування методики досудового розслідування відповідного виду кримінального правопорушення. Перш за все це зумовлено тим, що вказана особа має низку типових рис і притаманних ознак, що уможлиблюють вчинення нею такого кримінального правопорушення в цілому, а також дозволяють реалізовувати власні злочинні наміри.

Отже, комплексно, особою, що вчиняє відповідне кримінальне правопорушення є фізична, осудна особа, котра досягла 16-річного віку, має навички володіння комп'ютерними технологіями, свідомо застосовує їх з метою замаху на нормальний порядок функціонування програмного забезпечення інших комп'ютерних засобів, або мереж зв'язку. Найбільш характерною є вікова риса, оскільки молодші за віком особи швидше опановують комп'ютерні технології й суто технічно мають можливості до вчинення відповідного кола правопорушень навіть не свідомо, будучи введеними в оману особами, що зацікавлені у протиправному використанні шкідливих програмних (технічних) засобів.

Окрім цього, окремо слід зазначити, що такі особи, з урахуванням доступності курсів і тренінгів із комп'ютерної обізнаності та інших способів розширення знань про кібернетичні технології, як правило не усвідомлюють повною мірою змісту та сутності відповідного злочинного посягання, оскільки технічна конструкція того чи іншого програмного (технічного) засобу здебільшого є універсальними алгоритмами, що можуть застосовуватись до будь-яких комп'ютерних пристроїв. Наразі встановлено, що наявна низка випадків, коли особи-правопорушники, що створили з метою збути шкідливі програмні засоби, частіше характеризуються високим рівнем девіантності поведінки, відсутністю розуміння не просто меж прав і свобод людини і громадянина, а воліють до зловживання власними переважаючими знаннями в широко застосовній галузі (комп'ютерній) з метою отримання прибутку чи для власного задоволення. Тобто, злочинцем є осудна кваліфікована за інформаційно-програмним фахом, або професійно підготовлена особа чи група осіб, котрі використовують програмне комп'ютерне забезпечення з метою шкідливого впливу на програмні засоби персональних комп'ютерів, серверів або мережевого зв'язку.

Розділ 2 «Організація розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» складається з двох підрозділів.

У підрозділі 2.1 «Аналіз первинної інформації та висунення версій на початковому етапі розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» проаналізовано засади криміналістичного версіювання у досудовому розслідуванні кримінальних правопорушень у сфері створення з метою використання, розповсюдження або

збуту шкідливих програмних чи технічних засобів та обґрунтовується позиція про те, що криміналістична характеристика злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів уявляє собою результати аналізу складових, які відображають характерні особливості даного кримінального правопорушення, відмежовуючи його від суміжних злочинів шляхом критеріальних ознак, що вимагає компаративного структурного аналізу.

Залежно від характеру вихідних даних на початковому етапі розслідування можуть складатися різноманітні слідчі ситуації, що одразу програмуються таким чином, що вможлиблює результативне досудове розслідування та встановлення всіх об'єктивних факторів. Автором досягнуто висновку, що побудова версій проводиться слідчим безперервно, у процесі надходження до нього інформації.

Такий теоретико-правовий інструмент як криміналістичне версіювання, в умовах необхідності проведення значної кількості слідчих (розшукових) дій, прийняття процесуальних рішень, одночасного апелювання критично високою кількістю інформації, що тією чи іншою мірою характеризує вчинене (вчинюване чи таке що готується/завершилось) кримінальне правопорушення дозволяє слідчому ефективно та своєчасно реагувати на всі загрози та перепони щодо результативності здійснення досудового розслідування. З точки зору досудового розслідування відповідної категорії кримінальних правопорушень у сучасному правознавстві, версіювання є дієвим інструментом, що дозволяє прогресувати в процесі розслідування, в спосіб накопичення процесуально значимої інформації, саме тому взаємодія всіх суб'єктів здійснення досудового розслідування та осіб, які ними залучаються є критично важливою, зокрема й уданому розрізі.

У підрозділі 2.2 *«Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів»* розкрито сутність типових слідчих ситуацій та напрямки їх розв'язання при розслідуванні кримінальних правопорушень. Встановлено, що конкретна слідча обстановка (слідча ситуація) умовно має свою структуру, й у залежності від наявності/відсутності низки компонентів у ній, залежить алгоритм коригування подальшого досудового розслідування (іноді – зумовлюють відповідну черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування даного виду кримінального правопорушення). Систематизація типових слідчих ситуацій у розслідуванні кримінальних правопорушень вказаної категорії помагає в необхідності включати до класифікаційного процесу як типові криміналістичні категорії так і ті, що не є традиційними, характерними для специфічної злочинної діяльності.

На початковому етапі досудового розслідування злочинів типові слідчі ситуації, пов'язані зі створенням, використанням розповсюдженням та збутом шкідливих програмних засобів залежать від обсягу та джерел отриманої

інформації про кримінальне правопорушення, відомостей про правопорушника, його вмінь та навичок а також його місцеперебування. Визначення характеру тактичних завдань дозволяє конкретизувати процес збирання доказів, визначивши найбільш доцільну в окремій слідчій ситуації проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів у певній послідовності.

Найбільш універсальною послідовністю дій слідчого на відповідному етапі досудового розслідування кримінального правопорушення в указаній сфері є те, що, перш за все підлягає встановленню факт шкідливості такого програмного чи технічного засобу, що встановлюється в спосіб проведення експертного дослідження. Наступним має стати встановлення кола осіб причетних до його створення, використання, розповсюдження чи збуту, що в свою чергу охопить також визначення мотивів і мети злочинної діяльності відповідних осіб, факт наявності специфічних знань (щодо створення чи використання відповідного програмного чи технічного засобу).

Розділ 3 «Проведення слідчих (розшукових) дій під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» складається з двох підрозділів.

У підрозділі 3.1 *«Організаційно-тактичні особливості проведення слідчих (розшукових) дій під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів»* обґрунтовується позиція про те, що слідчий, як основний суб'єкт здійснення досудового розслідування конкретного кримінального провадження має права, повноваження та обов'язки, щодо вибору конкретного процесуального інструментарію в тій чи іншій ситуації. Водночас, у ході дослідження автору вдалось обґрунтувати позицію про те, в залежності від сфери вчинення кримінального правопорушення, його способу та конкретного виду, попередньо може бути зрозуміло, які саме слідчі (розшукові) дії належить провести першочергово.

Доведено, що тактичні особливості проведення тих чи інших слідчих (розшукових) дій залежать від низки факторів і обставин, що безпосередньо впливають не лише на їх вибір, а й на формат і методи проведення, а також корелюються з обставинами вчинення кримінального правопорушення, зумовлюються конкретними слідчими ситуаціями, наявними слідчими версіями, Механізм проведення слідчих (розшукових) дій залежить від поведінки осіб, відносно яких проводяться такі дії, а також взаємопов'язані з інтелектуальною та тактичною можливістю слідчого реалізовувати ті чи інші форми збору доказової інформації. Неупереджений підхід слідчого у даному випадку виступає ключовою засадою успішного розслідування, яке базуватиметься, крім процесуальних норм, ще й на інформаційно-технічному досвіді слідчого та експертів, які залучаються до процесу дослідження слідчої картини злочину.

Автором доведено, що в досудовому розслідуванні відповідної

категорії кримінальних правопорушень обов'язковим є проведення низки таких слідчих (розшукових) дій: призначення експертизи (що детально розглядається в окремому підрозділі), огляд (як приміщення де вчинялось кримінальне правопорушення, так і веб-ресурсів, що можуть бути пошкоджені, а також інших матеріальних і не матеріальних (візуальних образів) об'єктів, що є носіями процесуально важливої доказової інформації), обшук), а також інших процесуальних дій, які спрямовані на отримання інформації з матеріальних джерел (тимчасовий доступ до речей і документів), а також одержання показів від учасників кримінального провадження (допит, одночасний допит двох чи більше вже допитаних осіб для з'ясування причин розбіжностей у їхніх показаннях).

У підрозділі 3.2 «Використання спеціальних знань під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» розкрито сутність та зміст, а також роль і значення інституту використання спеціальних знань у досудовому розслідуванні тих кримінальних проваджень, що містять специфічні джерела доказової інформації різноманітного характеру (такі об'єкти містять як інформацію про «шкідливість» відповідного програмного (технічного) засобу, так і дають змогу долучити до матеріалів кримінального провадження інформацію про конструктивні й технічні (кібернетичні) особливості та властивості відповідних об'єктів, слідові приналежності до конкретних осіб та інші криміналістично значущі елементи).

Автором доводиться позиція, що особливими й недостатньо обґрунтованими як з теоретико-правового так і з правозастосовного аспекту є судові експертизи, котрі призначаються з метою дослідження комп'ютерних об'єктів, оскільки відповідний інститут є досить специфічним і не широко застосовним. Специфіка об'єктів досліджень зумовлює окремий порядок їх підбору, підготовки, зберігання, направлення на дослідження та самого проведення експертних досліджень і застосовуваних з цією метою методик. Адже об'єкт експертизи є невід'ємною і визначальною ознакою видової належності судово-експертного дослідження, важливим джерелом відомостей про ті чи інші події. Синтез спеціальних знань з різних експертних спеціальностей можливий за наявності суміжних галузей знань, котрі пов'язані або загальними методами дослідження, або загальними теоретичними концепціями.

Констатовано, що в процесі призначення експертних досліджень, превалюють комплексні експертизи, що спрямовані на надання характеристики не лише комп'ютерному обладнанню й приладам, а й програмному забезпеченню, змісту й характеру заподіяної шкідливим програмним (технічним) засобом шкоди. Комплексні експертизи призначають в разі наявності в досліджуваному об'єкті різноманітних слідів, зумовлених складною системою інформаційних полів. Констатовано, що в умовах необхідності ефективного й належного та результативного доказування вини осіб-правопорушників, під час досудового розслідування кримінальних

правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів експертне дослідження є невід'ємним елементом і має бути призначене однозначно.

ВИСНОВКИ

У дисертації на основі вивчення наукових джерел і нормативно-правових актів, узагальнення слідчої і судової практики, результатів анкетування та інтерв'ювання практичних працівників, запропоновано вирішення наукового завдання забезпечення початкового етапу розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів науковими положеннями, що мають значення для криміналістичної методики, а також практики розслідування цього виду протиправних діянь. За результатами проведеного дослідження сформульовано висновки, пропозиції та рекомендації, що можуть мати як теоретичне, так і практичне значення.

1. Охарактеризовано стан наукових досліджень щодо формування методики розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів і дало підстави обґрунтувати позицію про те, що вони мають певні закономірності та стали уявлення про основні елементи понятійно-категоріального апарату, які наразі потребують оновлення.

2. Надано авторське розуміння кримінального правопорушення у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів як винне кримінально каране діяння, вчинене одноосібно чи групою осіб із метою нанесення негативних наслідків іншому комп'ютерному програмному забезпеченню для отримання матеріальної вигоди чи іншого нематеріального задоволення, що завдало матеріальні чи інші нематеріальні збитків охоронюваним законом інтересам шляхом порушення функцій програмного чи інформаційно-комунікативного забезпечення комп'ютерного обладнання, а також комунікативних мереж і електронних накопичувальних пристроїв.

3. Встановлено, що криміналістична класифікація таких злочинів базується на міждисциплінарному науково-практичному досвіді не тільки загально-юридичних, але й спеціально юридичних дисциплін, а також на базі спеціальних технічних знань із галузей інформатики, програмування й інших наук. Зважаючи на це злочини у сфері створення, використання та розповсюдження шкідливих програмних засобів, будучи комп'ютерними злочинами потребують компаративного структурного аналізу

4. Обґрунтовано низку тез через визначення основних джерел криміналістичної значимої інформації під час досудового розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. Так,

аналізом елементів обстановки вчинення таких злочинів встановлено, що шкідливі програмні засоби можуть бути наступних видів: комп'ютерні віруси, котрі представляють собою програмні засоби, призначені для зміни функціональних особливостей програмного забезпечення, пошкодження операційної системи комп'ютерних програм, або знищення комп'ютерних програм; ШПЗ призначені для нейтралізації засобів захисту інформації; програми модифікатори, котрі при проникненні до програмного забезпечення здійснюють доступ до його модифікації та змінюють функціональні основи програмного забезпечення з метою несанкціонованого використання; програми епідемії, які поширюють шкідливу модифікацію програмного забезпечення адаптованих до їх модифікаційних можливостей програмних засобів шляхом активного впливу на ключові ідентифікатори потенційних об'єктів через мережі Інтернет, або в межах інформаційних носіїв.

Предмет злочинного посягання у злочинах передбачених ст. 361-1 КК України є обов'язковою ознакою складу цього злочину, оскільки у диспозиції статті міститься безпосередня вказівка на шкідливі програмні засоби. Безпосереднє дослідження й аналіз предмета цього складу є обов'язковою ознакою та підлягає обов'язковому встановленню та доказуванню, для решти злочинів шкідливі програмні засоби можуть виступати знаряддями чи засобами вчинення злочину.

5. Досліджено спосіб вчинення кримінального правопорушення, який пов'язаний з технологічними особливостями створення, використання, розповсюдження шкідливих програмних засобів та може бути класифікованими за різними підставами, які в подальшому будуть мати значення для криміналістичної характеристики. Основна класифікація ґрунтується на поділі всіх способів на дві основні групи: активні і пасивні. Встановлено, що під поняттям способу вчинення злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів слід розуміти інформаційно-технічний захід, вчинений шляхом застосування програмних розробок шкідливого програмного забезпечення у вигляді створення, копіювання, оптимізації самовідтворення та інкорпорації у програмне забезпечення або його розповсюдження із використанням можливостей програмних комп'ютерних мереж.

6. Сформовано криміналістичний «портрет» правопорушника, котрий вчиняє злочини, пов'язані із використанням шкідливих програмних засобів. Встановлено, що він уявляє собою фізичну, осудну особу, котра досягла 16 – річного віку, має навички володіння комп'ютерними технологіями, свідомо застосовує їх з метою замаху на функціональність програмного забезпечення інших комп'ютерних засобів, або мереж зв'язку. Особою злочинця виступає осудна кваліфікована за інформаційно-програмним фахом, або професійно підготовлена особа чи група осіб, котра використовує програмне комп'ютерне забезпечення з метою шкідливого впливу на програмні засоби персональних комп'ютерів, серверів або мережевого зв'язку.

7. Типові слідчі ситуації та напрямки їх розв'язання при розслідуванні

злочинів зумовлюють відповідну черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування даного виду злочинів. Серед цих заходів найбільш суттєве значення мають такі напрями, як отримання та аналіз доказів, що пов'язані із створенням та використанням шкідливих програмних засобів, подолання протидії слідчим діям та залучення у слідчі заходи експертів у сфері інформаційних технологій і програмування.

Систематизація типових слідчих ситуацій у розслідуванні злочинів пов'язаних зі шкідливими програмними засобами полягає у тому, що під час розслідування злочинів, що вчинені з використанням комп'ютерів, їх систем та іншої електронної техніки слідчий має справу як із традиційними для криміналістики, так і з нетрадиційними слідами злочинної діяльності та речовими доказами.

На початковому етапі досудового розслідування злочинів типові слідчі ситуації, пов'язані зі створенням, використанням розповсюдженням та збутом шкідливих програмних засобів залежать від обсягу та джерел отриманої інформації про злочин, відомостей про правопорушника, його вмінь та навичок а також його місцеперебування. Визначення характеру тактичних завдань дозволяє конкретизувати процес збирання доказів, визначивши найбільш доцільну в окремій слідчій ситуації проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів у певній послідовності.

8. Проаналізувавши засади криміналістичного версіювання у досудовому розслідуванні кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів автором обґрунтовується позиція стосовно того, що криміналістична характеристика злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів є результатами аналізу складових, які відображають характерні особливості даного злочину, відмежовуючи його від суміжних злочинів шляхом критеріальних ознак та вимагає компаративного структурного аналізу. Такі ознаки і формують структуру криміналістичної характеристики досліджуваного злочину, якими є: 1. спосіб вчинення злочину; 2. слідова картина; 3. особа злочинця; 4. предмет безпосереднього посягання. Така структура може служити інформаційною базою для висування версій у кримінальних провадженнях про зазначені види злочинів. Усі ці складові, є вихідними даними й основою для криміналістичного версіювання.

Залежно від характеру вихідних даних, при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж та мереж електрозв'язку на початковому етапі розслідування можуть складатися різноманітні слідчі ситуації. Доводиться позиція про те, що побудова версій проводиться слідчим безперервно, по мірі надходження до нього інформації. Навіть на початковому етапі розслідування, оглядаючи місце події члени СОГ зобов'язані обмінюватися інформацією, що дає можливість висувати для тактичного відпрацювання нові версії або ж

відмовитися від раніше висунутих.

8. Тактика проведення слідчих (розшукових) дій залежить від конкретних обставин вчинення злочину, зумовлена слідчими ситуаціями, висунутих слідчих версій, запланованих слідчих заходів зі встановлення осіб, що вчинили (вчинив) злочин та очікуваних результатів за результатами їх проведення. Тактика їх проведення залежить від поведінки осіб, які здійснюють доказування, і прийомів конкретних слідчих (розшукових) дій, спрямованих на збирання і дослідження доказів, встановлення об'єктивної істини по справі та прийняття у кримінальному провадженні обґрунтованого рішення. Неупереджений підхід слідчого у даному випадку виступає ключовою засадою успішного розслідування, яке базуватиметься, окрім процесуальних норм, ще й на інформаційно-технічному досвіді слідчого та експертів, які залучаються до процесу дослідження слідчої картини злочину.

Здійснюючи досудове розслідування злочинів зазначеної категорії слідчий має проводити низку слідчих (розшукових) дій (призначення експертиз, проведення оглядів, обшуків), а також інших процесуальних дій, що спрямовані на отримання інформації з матеріальних джерел (тимчасовий доступ до речей і документів), а також одержання показів від учасників кримінального провадження (допит, одночасний допит двох чи більше вже допитаних осіб для з'ясування причин розбіжностей у їхніх показаннях).

9. Автором досягнуто висновку про те, що застосування спеціальних знань у процесі досудового розслідування відповідної категорії кримінальних правопорушень є надзвичайно важливим, оскільки не всю доказову інформацію можна зібрати шляхом інших слідчих (розшукових) дій, а дослідження об'єктів вилучених із місць події, чи інших місць проведення слідчих (розшукових) дій потребує використання професійних знань. Наразі проведення комп'ютерно-технічних експертиз та інших видів спеціальних досліджень, на нашу думку не достатньо врегульовано в законодавстві України, а кадрові та інші організаційні спроможності Експертної служби Міністерства внутрішніх справ України не завжди в повному обсязі можуть покрити потреби суб'єктів органів досудового розслідування.

Окремо обґрунтовано позицію про те, що залучення до процесу дослідження експертів різних спеціальностей а також категорій експертної діяльності є об'єктивною необхідністю під час дослідження як інформації. Що зберігається на комп'ютерних пристроях, так і безпосередньо самого технічного обладнання (його придатності до використання в злочинних цілях, а також працездатності загалом). Розглянуті положення здебільшого висвітлюють загальні питання використання спеціальних знань у процесі кримінальних проваджень. Такі ж питання у ситуаціях, коли мова йде про розслідування правопорушень, пов'язаних зі створенням із метою використання, розповсюдження чи збуту, а також розповсюдження чи збут шкідливих програмних або технічних засобів, мають специфіку, на аналізі якої слід зосередити дослідження.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

Наукові праці, у яких опубліковані основні наукові результати дисертації:

1. Волков О. О. Особливості проведення допиту підозрюваних та обвинувачених при розслідуванні злочинів, пов'язаних з незаконним створенням, розповсюдженням або збутом шкідливих програмних засобів. *Вісник Луганського державного університету внутрішніх справ ім. Е.О. Дідоренка*. Луганськ : РВВ ЛДУВС. 2008. Вип. № 4. С. 196–205.

2. Волков О. О. До проблеми підготовки фахівців правоохоронних органів по боротьбі з кіберзлочинністю. *Правова інформатика*. 2008. № 1(17). С. 67–77.

3. Волков О. О. Особливості проведення допиту свідків при розслідуванні злочинів, пов'язаних з незаконним створенням, розповсюдженням або збутом шкідливих програмних засобів. *Південноукраїнський правничий часопис*. 2008. № 1 С. 137–141.

4. Волков О.О. Об'єктивна сторона складу злочину, передбаченого ст. 361-1 КК України: кримінально-правові, процесуальні та криміналістичні аспекти. *Кримінальна юстиція в Україні: сучасний стан та перспективи розвитку*. Луганськ : РВВ ЛДУВС. 2010. Ч. 3. С. 258–265.

5. Волков О. О. Криміналістична характеристика злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів. *Митна справа. Спеціальний випуск № 2/2013*. С. 55–60.

6. Волков О. О. Поняття шкідливого програмного засобу, призначеного для несанкціонованого втручання в роботу електронно-обчислювальної техніки. *Науковий вісник Національної академії внутрішніх справ*. 2018. № 1 (106). С. 217-230.

7. Волков О.О. Способи вчинення кримінальних правопорушень у сфері використання, розповсюдження або збуту шкідливих програмних чи технічних засобів: окремі аспекти криміналістичної характеристики. *Науковий вісник публічного та приватного права*. 2021. Випуск 6. Том 2. С. 209-214.

8. Волков О.О. Типові слідчі ситуації на початковому етапі досудового розслідування кримінальних правопорушень у сфері створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. *Науковий вісник публічного та приватного права*. 2022. Випуск 4. С. 145-149.

9. Волков О. Криміналістичні засади здійснення досудового розслідування незаконного використання електронно-обчислювальних машин: до питання характеристики особи злочинця. *KELM*. 2022. № 7. С. 49-53.

Наукові праці, які засвідчують апробацію матеріалів дисертації:

10. Волков О. О. Аспекти взаємодії оперативних підрозділів та слідчих апаратів на стадії перевірки матеріалів стосовно несанкціонованого доступу у сфері комп'ютерних технологій. *Тези доповідей міжвузівської курсантської (студентської) наук -практ. конф.* (Київ, 17-18 трав. 2005 р.) Ч.2. К. : Нац. акад. внутр. справ. України, 2005. С. 127–130.

11. Волков О. О. Кадрове забезпечення експертної діяльності при розслідуванні злочинів у сфері створення, розповсюдження і збуту шкідливих програмних засобів. *Правовий досвід на шляху до євроінтеграції: матеріали першої міжн. наук. -практ. інтернет-конф.* (Тернопіль, 30 листоп. 2006 р.). Тернопіль, 2006. С. 21–24.

12. Волков О. О. Виявлення доказової інформації при розслідуванні створення, використання, розповсюдження і збуту шкідливих програмних засобів. *Удосконалення діяльності ОВС України з попередження й розкриття злочинів та інших правопорушень: матеріали всеукр. наук. -практ. конф.* (Запоріжжя, 2 листоп. 2007 р.): / у 2 ч. Запоріжжя : Юридичний інститут МВС України, 2007. Ч. 1 С. 79–83.

13. Волков О. О. Специфічність інформації як об'єкт посягання на приватність. *Право на приватність: тенденції і перспективи: всеукр. наук. -практ. конф.* (Львів, 14 листоп. 2008 р.). Львів : Львів. держ. універ. внутр. справ, 2008. С. 40–41.

14. Волков О. О. Знаряддя вчинення злочину при розслідуванні злочинів пов'язаних з створенням, використанням, розповсюдженням і збутом шкідливих програмних засобів. *Розвиток України в XXI столітті: економічні, соціальні, екологічні, гуманітарні та правові проблеми: матеріалами III міжнар. наук. -практ. інтер. -конф.* (Тернопіль, 15 жовт. 2008 р.). Тернопіль : Терноп. нац. економ. універ. 2008. С. 43–46.

15. Волков О. О. Злочини в банківській сфері, що вчиняються за допомогою спеціально створених шкідливих програмних засобів. *Протидія злочинам, які вчиняються з використанням комп'ютерних мереж: тези допов. міжнар. наук. -практ. конф.* (Севастополь, 1-2 жовт. 2010 р.). Севастополь, 2010. С. 156–160.

16. Волков О. О. Поняття, види та протидія Інтернет-злочинності в глобальних соціальних мережах. *Співпраця поліції/міліції зі службами інтернет-сайтів (аукціонів, соціальних мереж, тощо) у боротьбі з інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє в європейському союзі: тези допов. Міжнар. наук. -практ. конф.* (Хмельницький, 16-17 листоп. 2010 р.). Хмельницький: УМВС України в Хмельницькій області, 2010. С. 28–33.

17. Волков О. О. Заходи забезпечення кібербезпеки підприємницької діяльності. *Глобальні виміри захисту економічної конкуренції: тези доп. II міжнар. наук. -практ. конф.* (Київ, 28 лют. 2018 р.). К. : Центр комплексних

досліджень з питань антимонопольної політики. Антимонопольний комітет України, 2018. С. 31-34.

18. Волков О.О. Криміналістична характеристика особи злочинця в сфері використання електронно-обчислювальних машин. *Актуальні проблеми діяльності органів досудового розслідування в умовах воєнного стану: Матеріали науково-практичного семінару* (м. Дніпро, 26 травня 2022 року). Ред. кол. А. В. Захарко, А. Г. Гаркуша, В. М. Федченко. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2022. С.216-118.

АНОТАЦІЯ

Волков О.О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. – *На правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 «Кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність». – Дніпропетровський державний університет внутрішніх справ, Дніпро, 2022.

У дисертації здійснено комплексне дослідження правових, теоретичних та організаційно-тактичних засад кримінального провадження на початковому етапі розслідування злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів із огляду на нормативні положення чинного кримінального та кримінального процесуального законодавства України.

Проаналізовано стан теоретичної розробленості проблем початкового етапу розслідування злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів. Визначено, що одним із видів доказів КПК України визначає документ, до яких може бути віднесено різні носії інформації у тому числі й електронні, які мають інше походження, досліджено їх характеристики.

Визначено, що надана криміналістична класифікація таких злочинів базується не тільки на міждисциплінарному науково-практичному досвіді не тільки загально-юридичних, але й спеціально-юридичних дисциплін, на базі спеціальних технічних знань з галузей інформатики, програмування та інших наук. Основна їх класифікація, ґрунтується поділом всіх способів на дві основні групи: активні і пасивні.

Отримало подальший розвиток криміналістичне визначення поняття способу вчинення злочину, дещо відмінного від кримінально – правового визначення способу вчинення злочину, як ознаки об'єктивної сторони складу злочину. Визначено, що спосіб вчинення досліджуваного злочину, тісно пов'язаний з технологічними особливостями створення, використання, розповсюдження або збуту шкідливих програмних засобів.

Обґрунтовано, що, спосіб вчинення злочину, передбаченого ст. 361⁻¹ КК України, безпосередньо виражений у формі створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Запропоновано власне визначення поняття способу вчинення злочинів у сфері створення з метою протиправного використання, розповсюдження чи збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Встановлено існування кореляційної залежності у зв'язках між способом учинення злочину й особою злочинця, між місцем, часом учинення злочину й особою правопорушника та між механізмом слідоутворення та іншими структурними елементами криміналістичної характеристики злочину такими як предмет безпосереднього посягання.

Сформовано криміналістичний «портрет» правопорушника, котрий вчиняє злочини, пов'язані із використанням шкідливих програмних засобів. Встановлено, що він є фізичною осудною особою, яка досягла 16 – річного віку, має навички володіння комп'ютерними технологіями, свідомо застосовує їх із метою замаху на функціональність програмного забезпечення інших комп'ютерних засобів, або мереж зв'язку. Особою злочинця виступає осудна кваліфікована за інформаційно-програмним фахом, або професійно підготовлена особа чи група осіб, котра використовує програмне комп'ютерне забезпечення з метою шкідливого впливу на програмні засоби персональних комп'ютерів, серверів або мережевого зв'язку.

Визначено, що безпосереднім предметом злочинного посягання виступають шкідливі програмні засоби, котрими є системне програмне забезпечення, програмні блоки та окремі програми котрі створені для здійснення шкідливого впливу на інше програмне забезпечення шляхом зміни його функціональних особливостей, або будь-якого іншого порушення права власності і права використання програмних комп'ютерних засобів.

Систематизовано типові слідчі ситуації у розслідуванні злочинів, пов'язаних зі шкідливими комп'ютерними програмами, що полягають у тому, що під час розслідування злочинів, вчинених із використанням комп'ютерів, систем та іншої електронної техніки слідчий має справу як із традиційними для криміналістики, так і з нетрадиційними слідами злочинної діяльності та речовими доказами.

Зроблено висновки, що тактика проведення слідчих (розшукових) дій залежить від конкретних обставин вчинення злочину, запланованих слідчим заходам по встановленню осіб, які вчинили (вчинив) злочин та очікуваних результатів за результатами їх проведення. Тактика їх проведення залежить від поведінки осіб, які здійснюють доказування, і прийомів конкретних слідчих дій, спрямованих на збирання і дослідження доказів, встановлення об'єктивної істини по справі та прийняття у кримінальному провадженні обґрунтованого

рішення.

Отримало свій подальший розвиток поняття експерта, у зв'язку з чим запропоновано доповнити статтю 69 КПК України вказівкою щодо встановлення обов'язкової вимоги до статусу судового експерта як його приналежність до державного реєстру атестованих судових експертів, а також доповнення Кримінального процесуального кодексу України нормою, що визначала б саме поняття судової експертизи.

Ключові слова: початковий етап розслідування, способи вчинення злочинів, кримінальне провадження, шкідливі програмні засоби, досудове розслідування, тактика проведення слідчих (розшукових) дій, слідова картина, криміналістична класифікація злочинів, джерела криміналістично значимої інформації, типові слідчі ситуації, висування слідчих версій, використанні спеціальних знань.

SUMMARY

Volkov O.O. Initial stage of investigation of the creation, use, distribution or sale of malicious software or hardware. – *The manuscript.*

Dissertation for the degree of Candidate of Law in the specialty 12.00.09 "Criminal Procedure and Criminology; forensic examination; operational-search activity". – Dnipropetrovsk State University of Internal Affairs, Dnipro, 2022.

The dissertation carried out a comprehensive study of the legal, theoretical, organizational and tactical foundations of criminal proceedings at the initial stage of investigation of crimes in the field of creation, use and distribution of malicious software, taking into account the normative provisions of the current criminal and criminal procedural legislation of Ukraine.

The state of theoretical development of the problems of the initial stage of investigation of crimes in the field of creation, use and distribution of malicious software is analyzed. It is determined that one of the types of evidence of the CPC of Ukraine determines the document, which can include various information carriers, including electronic ones, which have a different origin, investigated their characteristics.

It is determined that the provided forensic classification of such crimes is based not only on the interdisciplinary scientific and practical experience of not only general legal, but also special legal disciplines, on the basis of special technical knowledge in the fields of computer science, programming and other sciences. Their main classification is based on the division of all methods into two main groups: active and passive.

The forensic definition of the concept of the method of committing a crime, which is somewhat different from the criminal and legal definition of the method of committing a crime, as a sign of the objective side of the crime, has been further

developed. It is determined that the method of committing the crime under study is closely related to the technological features of the creation, use, distribution or sale of malicious software.

It is justified that, the method of committing a crime under Art.361⁻¹ of the Criminal Code of Ukraine, directly expressed in the form of creation for the purpose of illegal use, distribution or sale of malicious software or hardware, as well as their distribution or sale.

The actual definition of the concept of the method of committing crimes in the field of creation for the purpose of illegal use, distribution or sale of malicious software or hardware, as well as their distribution or sale is proposed.

The existence of a correlation has been established in the relationship between the method of committing a crime and the person of the offender, between the place, time of the crime and the person of the offender and between the mechanism of trace formation and other structural elements of the forensic characteristics of the crime, such as the subject of direct encroachment.

A forensic "portrait" of an offender who commits crimes related to the use of malicious software has been formed. It has been established that he is a physical, sane person who has reached the age of 16, has computer skills, consciously uses them to attempt the functionality of software of other computer tools or communication networks. The perpetrator's person is a sane person qualified in the information and software specialty, or a professionally trained person or group of persons who uses computer software for the purpose of harmful effects on the software of personal computers, servers or network communications.

It is determined that the direct subject of criminal encroachment is malicious software, which are system software, software blocks and individual programs that are specially created to have a harmful effect on other software by changing its functional features, or any other violation of the right of ownership and the right to use software computer tools.

Typical investigative situations in the investigation of crimes related to malicious computer programs have been systematized, which consist in the fact that during the investigation of crimes committed using computers, systems and other electronic equipment, the investigator deals with both traditional forensics and unconventional traces of criminal activity and material evidence.

It was concluded that the tactics of conducting investigative (investigative) actions depends on the specific circumstances of the crime, planned by the investigative measures to identify the persons who committed (committed) the crime and the expected results based on the results of their conduct. The tactics of their conduct depends on the behavior of the persons carrying out the evidence and the methods of specific investigative actions aimed at collecting and examining evidence, establishing objective truth in the case and making an informed decision in criminal proceedings.

The concept of an expert has received its further development, in connection with which it is proposed to supplement Article 69 of the Criminal Procedure Code of Ukraine with an instruction on establishing a mandatory requirement for the status of a forensic expert as his belonging to the state register of certified forensic experts, as well as to supplement the Criminal Procedure Code of Ukraine with a norm that would define the very concept of forensic examination.

Keywords: initial stage of investigation, methods of committing crimes, criminal proceedings, malicious software, pre-trial investigation, tactics of investigative (inquiry) actions, trace picture, forensic classification of crimes, sources of forensically significant information, typical investigative situations, nomination of investigative versions, use of special knowledge.