УДК 343
DOI https://doi.org/10.32850/sulj.2021.2.25

ТАКТИКА ПРОВЕДЕННЯ СЛІДЧОГО ОГЛЯДУ МІСЦЯ ВЧИНЕННЯ КІБЕРДИВЕРСІЇ

Пелещак О. Р.

Швидка інформатизація суспільства, розвиток новітніх технологій сприяють не лише покращенню умов роботи, пришвидшенню робочих процесів, розширенню кордонів співпраці, але й виникненню нових видів злочинів. Серед них порушення безпеки громадян, збереження конфіденційності персональних даних, захисту комерційної й інших видів таємниць, втрата важливої інформації через технічні збої, протиправні посягання на електронні бази й інформаційні ресурси, найбільш небезпечними серед них є кібердиверсії, що загрожують системам вітчизняного державного та військового управління, економіці та промисловості, життю і здоров'ю громадян України. Ситуація ускладнюється відсутністю відповідних норм у Кримінальному кодексі України, Кримінальному процесуальному кодексі України та Кодексі України про адміністративні правопорушення, а також відсутністю в них інституту електронних доказів, що в сукупності перешкоджає притягненню особи до кримінальної відповідальності.

Метою статті є дослідження тактики проведення слідчого огляду місця вчинення кібердиверсії.

У статті розглянуто підготовчий, робочий і заключний етапи проведення слідчого огляду місця вчинення кібердиверсії, специфічні обставини та криміналістичні особливості. Перший етап по суті організаційний та починається з ухвалення рішення про проведення слідчого огляду.

Висвітлено заходи підготовчого, організаційного характеру та загальний алгоритм дій учасників слідчого огляду. Акцентовано увагу на процесі виявлення та фіксації електронних доказів.

Доведено, що лише правова освіченість, технічна обізнаність учасників слідчого огляду в новітніх інформаційних технологіях та наявність відповідного матеріально-технічного і програмного забезпечення визначають успіх проведеного слідчого огляду і кримінального провадження загалом.

Ключові слова: *слідчий огляд, тактика проведення, кібердиверсія, електронні докази, новітні технології.*

Peleshchak O. R. Tactics of conducting an investigative examination of cyber sabotage crime scene

Rapid computerization of society, the development of new technologies contribute not only to improving working conditions, speeding up work processes, expanding the boundaries of cooperation but also the emergence of new types of crime. These include ensuring the safety of citizens, maintaining the confidentiality of personal data, protection of commercial and other secrets, loss of important information due to the technical failures, illegal encroachments on electronic databases and information resources and the most dangerous among them are cyber sabotage, threatening the systems of domestic state and military administration, economy and industry as well as life and health of citizens of Ukraine. The situation is complicated by the lack of relevant rules in the Criminal Code of Ukraine, the Criminal Procedure Code of Ukraine and the Code of Ukraine on Administrative Offenses, as well as the lack of the institution of electronic evidence, which together prevent a person from being prosecuted.

The purpose of the article is to study the tactics of investigative inspection of the cyber sabotage crime scene.

The article considers the preparatory, working and final stages of the investigative examination of the cyber sabotage crime scene, specific circumstances and forensic features. The first stage, in its essence, is organizational and begins with the decision to conduct an investigative review.

Measures of preparatory and organizational character and the general algorithm of actions of participants of investigative examination are covered in the article. Emphasis is placed on the process of detecting and recording electronic evidence.

It is proved that only legal education as well as technical knowledge of the participants of the investigative examination in the latest information technologies and the availability of appropriate material, technical and software determine the success of the conducted investigative examination and criminal proceedings in general.

Key words: *investigative examination, tactics, cyber sabotage, electronic evidence, new technologies.*

Постановка проблеми та її актуальність. Швидка інформатизація суспільства, розвиток новітніх технологій сприяють не лише покращенню умов роботи, пришвидшенню робочих процесів, розширенню кордонів співпраці, але й виникненню нових видів злочинів. Проблем, які потребують постійного доопрацювання та вдосконалення методів і засобів їх вирішення, стає все більше. Серед них гарантування безпеки громадян, збереження конфіденційності персональних даних, захист комерційної й інших видів таємниць, втрата важливої інформації через технічні збої, протиправні посягання на електронні бази й інформаційні ресурси [1, с. 303], найбільш небезпечними серед них є кібердиверсії, що загрожують системам вітчизняного державного та військового управління, економіці та промисловості, життю і здоров'ю громадян України [2, с. 226]. Майже кожного дня в засобах масової інформації з'являються повідомлення про здійснення кібератак на державні підприємства, установи, організації. Ситуація ускладнюється відсутністю відповідних норм у Кримінальному кодексі України, Кримінальному процесуальному кодексі України (далі – КПК України) та Кодексі України про адміністративні правопорушення, а також відсутністю в них інституту електронних доказів, що в сукупності перешкоджає притягненню особи до кримінальної відповідальності.

Аналіз матеріалів кримінальних проваджень, відкритих за ознаками злочинів досліджуваної категорії, свідчить про те, що у 20% учинених злочинів у кіберпросторі місце використання технічних засобів для неправомірного доступу до комп'ютерної інформації перебувало за межами України, у 40% таких злочинів – місце підготовки злочину (розроблення вірусу, програм зламу, добору паролів); у 10% злочинів – місце (комп'ютер, сервер або стример) обробки інформаційного продукту як предмета посягання [3, с. 112]. Ми ж розглянемо ситуацію, коли кібердиверсію вчинено на території України, є можливість безпосереднього доступу до місця скоєння злочину. Важливо, щоб доказова база була зібрана на законних підставах, оскільки лише тоді вона матиме статус законно отриманих доказів [4]. Особливої ваги в цьому світлі набуває саме початковий етап розслідування. Для отримання початкової інформації про вчинення злочину до початку кримінального провадження слідчий може провести тільки огляд місця події, основними завданнями якого є встановлення обставин події, виявлення, фіксація, вилучення й оцінка слідів злочину, отримання інформації, необхідної для побудови та перевірки версій і проведення подальшої розшукової роботи.

Аналіз останніх досліджень і публікацій. В Україні питання захисту критичної інфраструктури, як найбільш частого об'єкта кібердиверсій, загалом регулюється Директивою Ради Європейського Союзу «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» від 8 грудня 2008 р., рішенням Ради національної безпеки і оборони (далі – РНБО) України «Про вдосконалення заходів забезпечення захисту об'єктів критичної інфраструктури» від 29 грудня 2016 р., рішенням РНБО України «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури» від 16 лютого 2017 р., рішенням РНБО «Про невідкладні заходи з нейтралізації загроз енергетичній безпеці України та посилення захисту критичної інфраструктури» від 16 лютого 2017 р., розпорядженням Кабінету Міністрів України (далі – КМУ) «Про схвалення Концепції створення державної системи захисту критичної інфраструктури» від 6 грудня 2017 р., постановою КМУ «Про затвердження Порядку проведення огляду стану кіберзахисту критичної інформаційної інфраструктури, державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом» від 11 листопада 2020 р. [5].

Одним із чинників ризику для державних підприємств, установ і організацій є застосування шкідливого програмного забезпечення або програм із прихованими небезпечними складовими частинами, державними органами. Ця проблема актуальна не лише для України. Так, 7 червня 2021 р. Президент США Джо Байден підписав розпорядження про кібербезпеку, яке включає нові вимоги щодо безпеки до постачальників програмного забезпечення, які продають програмне забезпечення уряду США. Ці новації зачіпають і приватний сектор. У документі йдеться про розробку пілотних програм для створення рейтингів та спеціального маркування для позначення безпечного споживчого програмного забезпечення. Також пропонується створити спеціальний державний орган для виявлення, розслідування кібердиверсій, обміну інформацією з іншими державними органами, що в сукупності має визначити майбутнє правил кібербезпеки [6].

В Україні ж із метою забезпечення безперебійного та стійкого функціонування об'єктів критичної інфраструктури, запобігання проявам несанк-

ціонованого втручання в їхнє функціонування, прогнозування та запобігання кризовим ситуаціям на об'єктах критичної інфраструктури, підвищення рівня їхнього захисту, безпеки та стійкості до загроз будь-якого типу розроблено проєкт закону «Про критичну інфраструктуру та її захист» від 18 березня 2021 р. [7].

Безпосередньо порядок залучення працівників органів досудового розслідування поліції й Експертної служби Міністерства внутрішніх справ на спеціалізованій пересувній лабораторії на стадії досудового розслідування, а також обов'язки та повноваження працівників як спеціалістів під час проведення огляду місця події визначає Інструкція про порядок залучення працівників органів досудового розслідування поліції та Експертної служби Міністерства внутрішніх справ України як спеціалістів для участі у проведенні огляду місця події, затверджена наказом Міністерства внутрішніх справ України від 3 листопада 2015 р.

Тактика проведення саме слідчого огляду місця події є предметом досліджень багатьох науковців, серед них В.І. Алексєйчук, О.В. Батюк [8], П.Д. Біленчук, Ю.О. Гресь, В.О. Комаха, О.В. Одерій, О.А. Самойленко, К.О. Чаплинський, Б.В. Черняховський та багато інших. Проте специфічні обставини та криміналістичні особливості, що впливають на тактику проведення слідчого огляду місця вчинення кібердиверсії, потребують більш прискіпливого дослідження з метою розроблення відповідних рекомендацій та необхідності проведення роботи над типовими помилками.

Метою статті є дослідження тактики проведення слідчого огляду місця вчинення кібердиверсії.

Виклад основного матеріалу.

1. Підготовчий етап проведення слідчого огляду місця вчинення кібердиверсії

Відповідно до п. 1 ст. 237 КПК України з метою виявлення та фіксації відомостей щодо обставин учинення кримінального правопорушення слідчий, прокурор проводять огляд місцевості, приміщення, речей та документів.

Дана слідча дія дає змогу встановити великий обсяг доказів, які належать до складу злочину (об'єкт, об'єктивна сторона, суб'єкт та суб'єктивна сторона), потребує застосування відповідних тактичних прийомів і засобів криміналістичної техніки.

Умовно науковці поділяють процес здійснення слідчого огляду на три взаємопов'язані етапи: підготовчий, робочий і заключний. Перший, по суті організаційний, є безпосередньою підготовкою до наступного робочого етапу та починається з ухвалення рішення про його проведення.

До виїзду на місце проведення огляду місця події у кримінальних провадженнях щодо вчинення кібердиверсій безпосереднім обов'язком слідчого є встановлення і документальна фіксація підстав та законності проведення слідчого огляду. Потім проводяться такі обов'язкові підготовчі й організаційні заходи, як забезпечення охорони місця події й об'єктів огляду до прибуття слідчо-оперативної групи (далі – СОГ), з'ясування особливостей імовірного місця вчинення злочину та потенційних об'єктів огляду, за можливості припинення або послаблення шкідливих наслідків злочину, забезпечення присутності осіб, що можуть надати інформацію щодо факту події. Аналіз вищезазначених чинників надасть змогу визначити необхідний склад СОГ, яка забезпечить належний супровід і технічну підтримку слідчого. До них варто віднести інспектора-криміналіста, оперативних працівників підрозділу боротьби з кіберзлочинністю, працівників СБУ й інших спеціалістів, що забезпечать пошук, фіксацію, вилучення, опис та інтерпретацію слідів за допомогою спеціальних знань, а також відеофіксацію огляду місця події. Наявність криміналістичної валізи для фіксації та вилучення матеріальних слідів злочину, необхідного криміналістичного технічного і програмного забезпечення спеціаліста, який супроводжує слідчий огляд, та інструментів для вилучення обладнання є обов'язковою.

У разі необхідності доступу до інформації з обмеженим доступом чи персональних даних, які могли стати об'єктом правопорушення чи необхідні для встановлення обставин злочину, застосовуються ст. ст. 159, 160 КПК України. У такому разі виноситься ухвала суду про надання дозволу на тимчасовий доступ до такої інформації з метою її огляду та, у разі необхідності, копіювання.

Після прибуття на місце події члени СОГ з'ясовують обставини вчинення кримінального правопорушення, встановлюють свідків, прикмети осіб, які вчинили кримінальне правопорушення, та ймовірні шляхи їх відступу, уживають заходів для переслідування транспортних засобів, що використовувалися злочинцями, у разі необхідності.

Потім виконуються такі дії: фіксація часу прибуття на місце проведення огляду, час початку слідчої дії; під час проведення огляду у власності заявника/потерпілого, отримання у присутності понятих добровільної письмової згоди на огляд

місцевості, приміщення й іншого майна; встановлення місць зовнішнього підключення до будівлі електропостачання, комунікаційних і мережевих кабелів, організація їхньої охорони на час проведення огляду; збір попередніх відомостей (опитування) від осіб, які перебувають на місці події, для врахування обставин, що можуть мати значення для проведення огляду, встановлення змін на місці події, осіб, які їх учинили, із якою метою; усунення з місця події всіх сторонніх осіб; пошук та залучення понятих (не менше двох осіб) з розрахунку кількості приміщень, у яких розташовані окремі елементи комп'ютерної системи; остаточне визначення кола інших учасників огляду (коригування складу слідчої групи); інструктаж учасників огляду, повідомлення та, у разі потреби, роз'яснення їхніх прав і обов'язків; проведення інших невідкладних дій і вжиття заходів, спрямованих на покращення умов огляду (забезпечення штучного освітлення, наявність автономних пристроїв живлення для технічних засобів тощо) [9, с. 61].

Щодо понятих, як показує практика, знайти їх іноді буває нелегко, до того ж підбір понятих нерідко потребує значного часу, що негативно позначається на своєчасності проведення слідчої дії. У разі вчинення кібердиверсії до понятих пред'являється така вимога, як компетентність у тій чи тій галузі знань. Поняті повинні бути обізнані з особливістю роботи комп'ютерних і телекомунікаційних систем, бути обізнаними у комп'ютерній техніці та процесах роботи з електронною / цифровою інформацією щонайменше на рівні впевнених користувачів, для забезпечення факту усвідомлення та підтвердження останніми суті дій учасників слідчої групи. Інакше вони не можуть адекватно сприймати та, у разі необхідності, відтворювати сприйняте під час провадження даної слідчої дії [10, с. 25]. Для забезпечення таємниці слідства варто залучати понятих із числа осіб, не пов'язаних трудовими відносинами із власниками інформації, на яку було здійснено кібернапад.

На початковому етапі також вирішують питання щодо витребування необхідної інформації від провайдерів, інших установ, що обслуговують об'єкт. Після цього підготовчий етап уважається завершеним.

2. Робочий етап проведення слідчого огляду місця вчинення кібердиверсії

Безпосередній огляд слідчим місцевості, приміщень, предметів, комп'ютерної техніки та документів, зокрема й електронних, для побудови слідчих версій учинення кібердиверсії є змістом робочого етапу проведення слідчого огляду. Безперервне вдосконалення та розвиток інформаційних та електронних систем впливають на збільшення кола завдань, які необхідно вирішити, тому в кожній конкретній ситуації вони визначаються індивідуально.

Під час огляду місця події, згідно з порядком, закріпленим у КПК України, фіксуються відомості щодо обставин учинення кримінального правопорушення, вилучаються речі та документи, які мають значення для кримінального провадження, та речі обмеженого доступу, зокрема й матеріальні об'єкти, які можуть допомогти з'ясувати обставини, що підлягають доказуванню. Забезпечується їх належне зберігання з метою подальшого направлення для проведення експертного дослідження.

Насамперед проводиться загальний огляд місця події (визначення меж місця проведення огляду, складання плану-схеми розташування об'єктів огляду, мережевих з'єднань комп'ютерів, серверів, каналів електрозв'язку тощо), встановлюється необхідний у конкретній ситуації спосіб та послідовність проведення огляду, вибір позицій відеозйомки.

Особливостями огляду й опису слідів кібердиверсії є вчинення злочину в кіберпросторі (безпосередньо або з віддаленим доступом). Знаряддями безпосереднього доступу можуть виступати флешки, диски, накопичувачі, периферійне обладнання, електронні ключі, особисті коди користувачів тощо. Мережеве устаткування, сервери, модеми, прилади супутникового зв'язку тощо віднесені до знарядь віддаленого доступу.

Способи доступу до комп'ютерної інформації також поділяються на безпосередні й опосередковані (віддалені). Під час реалізації способів безпосереднього доступу інформація знищується, блокується, модифікується, копіюється, а також може бути порушена робота комп'ютера, комп'ютерної системи або мережі шляхом передачі відповідних команд із комп'ютера, на якому інформація зберігається. Безпосередній доступ можуть здійснювати особи, які працюють з інформацією, а також особи, які спеціально проникають у закриті зони та приміщення, де провадиться обробка інформації. Іноді злочинець із метою вилучення інформації, залишеної користувачами після роботи комп'ютера, обстежує робочі місця програмістів у пошуках чорнових записів, роздруківок, ділового листування («прибирає сміття») або здійснює перегляд і відновлення стертих програм.

Під час реалізації способів опосередкованого / віддаленого доступу до комп'ютерної інформа-

ції відбувається: підключення до лінії зв'язку, мереж законного користувача, одержання таким чином доступу до його системи, а також віддалене проникнення в чужі інформаційні мережі для отримання необхідної у справі інформації [11, с. 43–44].

Після загального огляду слідчим здійснюється детальний кількісно-якісний огляд місця події. За вказівкою слідчого спеціаліст-криміналіст опрацьовує зазначені об'єкти на предмет наявності різноманітних відбитків, можливих механічних пошкоджень, наявності, нашарування/відсутності сторонніх речовин чи пилу, біологічних слідів ДНК чи одорологічних слідів тощо. Під час пошуку та фіксації дактилоскопічних слідів варто враховувати можливі наслідки застосування магнітного порошку, а також узгоджувати зі спеціалістом застосування різноманітних за спектром дії пристроїв пошуку, щоб не завдати шкоди носіям інформації, мікросхемам тощо.

Під час розгляду версії несанкціонованого втручання шляхом фізичного підключення до комп'ютерного устаткування безпосередній користувач має перевірити внутрішній вміст комп'ютерного устаткування на предмет наявності чи відсутності комп'ютерних комплектуючих, пристроїв пам'яті, мікросхем тощо, слідчим проводиться огляд отриманого з метою визначення конкретного користувача. Водночас оперативно-технічний працівник СОГ оглядає точки мережевого й електропідключення на предмет можливого пошкодження кабелів (надрізання, втиснення, припаювання тощо). На цьому етапі важливо не вимикати електроживлення пристроїв та механічно не роз'єднувати електричні ланцюги, не від'єднувати частини. Усі виявлені речові докази мають бути герметично запаковані, промаркіровані й опечатані для забезпечення якісного судового експертного дослідження та подальшого висновку.

На окрему увагу заслуговує огляд паперових документів, а саме журналів обліку роботи з комп'ютерним устаткуванням, роздруківок текстів комп'ютерних програм, технічної, технологічної й іншої документації. Увагу варто акцентувати на наявності підчищень, виправлень, додаткових записів, порядку нумерації сторінок, вкладень, розпоряджень на виконання певних програмно-технічних робіт із комп'ютерним устаткуванням чи заміні програмного забезпечення, уведенні додаткової інформації, не передбаченої технологічним процесом, відповідності форм запису такої інформації встановленим правилам тощо [9, с. 62].

Після детального огляду й аналізу матеріальної складової частини місця події спеціаліст розпочинає роботу з електронною інформацією. Саме від професійної роботи спеціаліста (спеціалізація якого процесуально підтверджена) часто залежать виявлення та фіксація електронних доказів кібердиверсії. Саме досконале знання організаційно-технічних особливостей пошуку і вилучення електронно-обчислювальної техніки (далі – ЕОТ) працівниками національної поліції, володіння актуальними знаннями щодо видів ЕОТ, особливостей її використання, наявності можливостей зняття інформації з електронних інформаційних систем, обсягу та характеристики інформації, що передається з / на зовнішні сервери [12, с. 118], є передумовою процесуально грамотної і технічно правильної фіксації інформації в комп'ютерах, комп'ютерних мережах і системах. Чинниками, які обов'язково варто враховувати, є наявність великого об'єму інформації, прихованих від користувача даних, програм самознищення чи видалення певної інформації з електронного журналу щодо дій зловмисника тощо. Неправильне поводження або тлумачення вищезазначених електронних слідів злочину, порушення вимог щодо їх фіксації можуть призвести до ускладнення встановлення достовірності, виникнення непорозумінь та правових маніпуляцій у суді.

Наступним етапом огляду місця події кібердиверсії є виявлення та фіксація так званих електронних слідів за допомогою відповідного програмного забезпечення. Фіксується будь-яка зміна файлової системи (зміна місця розташування, вмісту, форматів, характеристик окремих файлів, їх вилучення чи додавання нових, зміни контенту програмних таблиць, стану кластерів), які, на думку спеціаліста, можуть бути пов'язані з подією злочину. Показниками зовнішнього впливу і втручання в систему також є зміни змісту формату файлових характеристик, зміна алгоритму роботи програм. Дотримання принципів належності та допустимості всіх виявлених та зафіксованих електронних доказів у кримінальному провадженні на цьому етапі забезпечується взаємодією слідчого, прокурора та спеціаліста.

Увагу слідчого, прокурора та спеціаліста варто зосередити на таких слідах злочину, як: інформація, що зберігається на комп'ютерних носіях (зміни у файловій системі; шкідливі програмні засоби, небезпечні файлові програми); програми-файли із прямими посиланнями на вебсторінки в мережі Інтернет; програми, які автономно здійснюють копіювання, блокування, модифіка-

цію чи знищення інформації; файлове програмне забезпечення для підбору паролів доступу тощо [9, с. 64].

Отже, слідчий має не лише оглянути, а, у разі необхідності, вилучити комп'ютерне й інше устаткування, щодо якого є підстави вважати, що воно було використано особами, які підозрюються у вчиненні кібердиверсії, для подальшого проведення експертних досліджень техніки, програмного забезпечення, телекомунікаційних систем і засобів. Особливу увагу варто зосередити на роботі із сервером у разі використання правопорушниками систем віддаленого доступу. Під час вилучення комп'ютерного / мережевого обладнання необхідно обов'язково встановити та враховувати наслідки, які спричинить відсутність зазначених технічних засобів.

Прокурорам / процесуальним керівникам треба мати на увазі, що огляд місця події може проводитися до внесення відомостей про вчинення злочину до ЄРДР. У такому разі, відповідно до ч. 2 ст. 168 КПК України, тимчасове вилучення електронних інформаційних систем або їхніх частин, мобільних терміналів, систем зв'язку для вивчення фізичних властивостей, які мають значення для кримінального провадження, не здійснюється.

У разі необхідності вилучення таких систем потрібно в порядку ст. 160 КПК України звернутися до слідчого судді із клопотанням про надання тимчасового доступу до речей і документів [10, с. 42].

У разі наявності підозри на витік інформації з обмеженим доступом або персональної інформації необхідно врахувати та перевірити всі слідчі версії щодо несанкціонованого доступу, визначити способи протидії.

Під час огляду локальних комп'ютерів, комп'ютерної мережі та віддалених ресурсів рекомендовано дотримуватися такого алгоритму дій: 1) зафіксувати та зберегти інформацію, яка відображається на моніторі; 2) перевірити налаштування BIOS і завантажити операційну систему з робочого примірника; 3) приєднати зовнішній носій інформації, на який здійснюватимуть копіювання криміналістично значущої інформації для досудового розслідування; 4) запустити програму запису зображення екрана монітора для додаткової фіксації процесу огляду; 5) перевірити апаратне та програмне забезпечення комп'ютера, які його ідентифікують, налаштування мережевого адаптера; 6) створити файл-образ (еталон) для перевірки правильності підрахунку контрольних сум за допомогою призначеної для цього програми; 7) провести детальний огляд інформації, що збережена на комп'ютері; 8) запустити браузер і ввести ідентифікаційні дані віддаленого ресурсу, провести огляд зовнішнього інформаційного ресурсу / сайту, його наповнення; 9) установити IP-адресу сайту, шляхи проходження у процесі обміну інформацією між сайтом і відповідним комп'ютером; 10) для кваліфікованого збереження (вилучення) виявленої інформації здійснювати побітове копіювання на під'єднаний спеціалістом зовнішній носій зберігання інформації; 11) за допомогою криміналістичного програмного забезпечення вивести на екран монітора інформацію про контрольну суму кожного файлу, значущого для слідства, що зафіксований на зовнішньому носії, зберегти її у відповідному окремому файлі; 12) після копіювання всієї виявленої, значущої для кримінального провадження інформації підключити другий відформатований зовнішній носій зберігання інформації та скопіювати на нього всю інформацію з контрольного носія; 13) відключити контрольний та робочий носії із зібраною / збереженою інформацією, вилучити диск із робочим примірником криміналістичного програмного забезпечення, здійснити пакування контрольного примірника носія з доказовою інформацією способом, який унеможливить доступ до нього, опечатати й засвідчити на бирці з печаткою та підписами учасників слідчої дії, понятих; 14) зафіксувати порядок і зміст зазначених вище дій у протоколі огляду, обов'язково зазначити контрольну суму інформації, зауваження, клопотання і доповнення від учасників слідчої дії [9, с. 64–65].

Під час проведення огляду місця події необхідно постійно звертати увагу понятих на зміст, місце розташування та характеристики виявленої важливої для подальшого розслідування інформації.

2. Заключний етап проведення слідчого огляду місця вчинення кібердиверсії

Результатом проведеного огляду комп'ютера, мережі чи віддаленого інформаційного ресурсу стає протокол огляду з відповідними додатками. Важливим є дотримання всіх вимог, що забезпечують належне вилучення об'єктів для комп'ютерно-технічної експертизи й експертизи програмного забезпечення. Саме експерт має вирішувати питання щодо наявності в електронних доказах ознак стороннього втручання, що регулюється відповідними нормами КПК України

На цьому етапі необхідно коректно завершити всі відкриті у процесі слідчого огляду програми для уникнення можливої зміни, пошкодження чи втрати доказової інформації. Із цією ж метою категорично заборонено вмикати вилучену техніку чи

користуватися вилученим програмним забезпеченням після завершення слідчого огляду. Усі вилучені об'єкти мають бути надійно та за всіма правилами криміналістичного забезпечення запаковані. Саме від деталізації та грамотної фіксації всіх виявлених слідів кібердиверсії залежать надалі повнота й ефективність судових експертних висновків.

Висновки. У сучасних реаліях правопорушники активно використовують кіберпростір як місце вчинення протиправних діянь, там же й містяться сліди їхньої неправомірної діяльності. Боротьба зі злочинністю в кіберпросторі та необхідність її посилення вимагає від правоохоронців розроблення та впровадження у практичну діяльність новітніх оперативно-розшукових заходів та методів, які б ураховували вищезазначену специфіку їх функціонування.

Отже, постійне вдосконалення нормативно-правової бази, науково-дослідні розробки, підготовка методичних рекомендацій, алгоритмів дії учасників, удосконалення методики складання протоколу слідчого огляду місця вчинення кібердиверсії стають необхідністю й обов'язковою передумовою проведення розслідування та подальшого притягнення до кримінальної відповідальності причетних. Висвітлений у статті перелік дій учасників слідчого огляду місця події кібердиверсії не є вичерпним, оскільки зі швидким розвитком технологій удосконалюються засоби, методи та способи вчинення кібератак.

У цьому ракурсі на перший план виходять якість та повнота відображення виявлених у процесі слідчого огляду місця кібердиверсії відомостей, зокрема й електронних, відображених у протоколі огляду місця події, планах та схемах, матеріалах відеозйомки й інших засобах фіксації, що забезпечують наочність, повноту й об'єктивність важливої для розслідування інформації.

Проведення слідчого огляду під час розслідування фактів кібердиверсій потребує належної правової освіченості та технічної обізнаності учасників у новітніх інформаційних технологіях, які не лише є об'єктом вивчення, але й можуть слугувати для покращення якості, пришвидшення та повноти процесу збирання й аналізу інформації під час огляду місця події. Сучасні технології можуть допомагати фіксувати необхідну доказову інформацію засобами цифрових технологій (не лише загальновідомими, а, наприклад, за допомогою 3D-сканування), вимірювати відстані між об'єктами та фіксувати детальне місце їх розташування для точнішої побудови схем і планів місця події, швидше та якісніше обробляти результати огляду за допомогою новітнього програмного забезпечення.

Література

1. Курман О.В. Тактичні та організаційні особливості початку досудового розслідування несанкціонованого втручання в роботу електронно-обчислювальних машин, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Право і суспільство*. 2019. № 4. С. 303–308.

2. Пелещак О.Р. Кібердиверсія як форма сучасної диверсійної діяльності. *Науковий вісник Львівського державного університету внутрішніх справ. Серія «Юридична»*. 2017. № 3. С. 225–243.

3. Самойленко О.А. Основи методики розслідування злочинів, вчинених у кіберпросторі : монографія / за заг. ред. А.Ф. Волобуєва. Одеса : ТЕС, 2020. 372 с.

4. Practical aspects of criminal and law characteristics of cyber crimes in Ukraine / N. Ustrytska et al. *Journal of Legal, Ethical and Regulatory*. 2020. Vol. 23. Iss. 2. P. 1–6.

5. URL: https://zakon.rada.gov.ua/laws/show/z1392-15#Text (дата звернення: 07.07.2021).

6. Canizares Alexander, Corol Paul. Executive order aims to protect software supply chains. May 17, 2021. URL: https://www.reuters.com/legal/legalindustry/executive-order-aims-protect-software-supply-chains-2021-06-14/ (дата звернення: 07.07.2021).

7. Про критичну інфраструктуру та її захист : проєкт закону від 18 березня 2021 р. URL: http://search.ligazakon.ua/l_doc2.nsf/link1/JI04668A.html (дата звернення: 07.07.2021).

8. Батюк О.В. Криміналістичне забезпечення протидії злочинам на об'єктах критичної інфраструктури : монографія. Луцьк : СДП Гадяк Ж.В. ; Волинь-поліграф, 2021. 455 с.

9. Черняховський Б.В. особливості проведення слідчого огляду під час розслідування несанкціонованого втручання в роботу комп'ютерів, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. *Науковий вісник Національної академії внутрішніх справ*. 2020. № 2 (115). С. 59–68.

10. Документування результатів огляду місця події: правові і криміналістичні основи фіксації доказової інформації : монографія / П.Д. Біленчук та ін. ; за ред. П.Д. Біленчука. Київ : ННІПСК КНУВС, 2009. 88 с.

11. Амелін Р.В., Соколова Я.А. Рекомендації щодо особливостей досудового розслідування та процесуального керівництва у кримінальних провадженнях про злочини, вчинені з використанням електронно-обчислювальних машин (комп'ютерів), систем

Пелещак О. Р.,
здобувач освітнього ступеня доктора філософії
в галузі права кафедри кримінального процесу та
криміналістики
Львівського державного університету
внутрішніх справ

та комп'ютерних мереж і мереж електрозв'язку. Київ, 2017. 66 с. URL: https://www.gp.gov.ua›userfiles › metodichka_... (дата звернення: 07.07.2021).

12. Благута Р.І., Мовчан А.В. Новітні технології у розслідуванні злочинів: сучасний стан і проблеми використання : монографія. Львів : ЛьвДУВС, 2020. 256 с.