МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
ДНІПРОПЕТРОВСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова
праця на правах рукопису

ВОЛКОВ ОЛЕКСАНДР ОЛЕКСАНДРОВИЧ

УДК 343.985.7

ДИСЕРТАЦІЯ
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

Подається на здобуття наукового ступеня кандидата юридичних наук

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають покликання на відповідне джерело

_____ **О. О. Волков**

Науковий керівник **Солдатенко Олена Анатоліївна,**
кандидат юридичних наук, доцент

Дніпро – 2023

АНОТАЦІЯ

Волков О. О. Початковий етап розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів. – Кваліфікаційна наукова праця 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, 2023.

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 з огляду на нормативні положення чинного кримінального та кримінального процесуального законодавства України.

Автором звертається увага на те, що 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 гальмування її загострення є притягнення винних осіб до юридичної відповідальності, зокрема, кримінальної.

Визначено основні проблеми, пов'язані з розслідуванням такого виду злочинів, що мають певні закономірності, встановлено місце шкідливих програмних чи технічних засобів у структурі складу злочину та види таких шкідливих програмних засобів, визначено предмет злочину для ст. 361–1

КК України, який є обов'язковою ознакою та підлягає обов'язковому встановленню та доказуванню, тоді як для інших злочинів XVI Розділу КК України шкідливі програмні засоби можуть виступати як знаряддя чи засоби вчинення злочину. Сформульовано поняття та сутність злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів. Зважаючи на кримінально-правові положення, розроблено і сформульовано поняття шкідливого програмного засобу.

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, що може бути різним носієм інформації, зокрема й електронним.

Отримало подальший розвиток положення теорії кримінального права в частині пеналізації протиправних діянь, пов'язаних із використанням шкідливих програмних засобів, оскільки безпосереднє використання має більшу суспільну небезпеку, ніж створення з метою використання, і потребує більш ефективної кримінально-правової охорони.

Визначено, що надана криміналістична класифікація таких злочинів базована не тільки на міждисциплінарному науково-практичному досвіді, не тільки на загальноюридичних, але й спеціальноюридичних дисциплінах, на базі спеціальних технічних знань із галузей інформатики, програмування та інших наук. Основна їхня класифікація ґрунтована на розподілі всіх способів на дві основні групи: активні і пасивні.

Отримало подальший розвиток криміналістичне визначення поняття способу вчинення злочину, яке дещо відрізняється 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 або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Установлено 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, зокрема такими, як предмет безпосереднього посягання.

Обґрунтовано позицію, що сліди вчинення злочину, пов'язаного зі створенням, розповсюдженням чи використанням шкідливих програмних засобів мають неоднорідний зміст і форму, оскільки можуть бути синтезовані як із комп'ютерного приладу, що потребуватиме подальшого їх дослідження з використанням спеціальних знань, так і особисто від зловмисника, що також вимагає проведення слідчих (розшукових) дій, наприклад, допиту однієї особи або допиту кількох осіб. Крім цього, наголошено, що методи, способи та форми дії відповідних програмних засобів, взаємопов'язаність їх функціонування з іншими подібними програмами та причинно-наслідковий зв'язок із самим зловмисником є обов'язковими для доказування винуватості останнього.

Сформовано криміналістичний «портрет» правопорушника, що вчиняє злочини, пов'язані з використанням шкідливих програмних засобів. Установлено, що це фізична осудна особа, яка досягла шістнадцятирічного 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, яка 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, зокрема, системне програмне забезпечення, програмні блоки та окремі програми, спеціально 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.

Визначено типові слідчі ситуації та напрями їх розв'язання при розслідуванні злочинів, що зумовлюють відповідну черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування такого злочину. Серед цих заходів найбільш суттєве значення мають такі напрями, як отримання та аналіз доказів, що пов'язані зі створенням та використанням шкідливих програмних засобів, подолання протидії слідчим діям та залучення до слідчих заходів експертів у сфері інформаційних технологій і програмування.

Систематизовано типові слідчі ситуації в розслідуванні злочинів, пов'язаних зі шкідливими комп'ютерними програмами, які полягають у тому, що під час розслідування злочинів, учинених із використанням комп'ютерів, систем та іншої електронної техніки, слідчий має справу як з 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 слідчих заходів щодо встановлення осіб / особи, що вчинили / вчинила злочин, та очікуваних результатів за результатами їх проведення. Тактика проведення залежить від поведінки осіб, які здійснюють доказування, і прийомів конкретних слідчих дій, спрямованих на збирання й дослідження доказів,

установлення об’єктивної істини у справі та прийняття в 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, а саме його приналежність до державного реєстру атестованих судових експертів, а також доповнення Кримінального процесуального кодексу України нормою, яка визначала б саме поняття судової експертизи.

Розкрито зв’язок дисертаційної роботи з науковими програмами, планами та темами, визначено завдання та методи, використані в процесі дослідження обраної теми. Внесено науково обґрунтовані пропозиції щодо практики застосування чинного кримінального процесуального законодавства України з досліджуваних питань.

Проведена наукова розвідка дала змогу сформулювати теоретичні положення та практичні рекомендації щодо здійснення досудового розслідування в кримінальних провадженнях на початковому етапі розслідування злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів.

Автором уперше визначено порядок 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. Крім цього «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, є базовою термінологєю в здійснюваній категорії досудових розслідувань.

Автором констатовано та додатково утверджено 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.

Чільне місце та належна роль в структурі наукової новизни виділяється тому, що 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.

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 значущої інформації, типові слідчі ситуації, висування слідчих версій, використанні спеціальних знань.

SUMMARY

Volkov O.O. The initial stage of the investigation of criminal offenses in the field of creation for the purpose of use, distribution or sale of malicious software or technical means. – Qualifying scientific work on manuscript rights.

Dissertation for obtaining the scientific degree of candidate of legal sciences on the specialty 12.00.09 "Criminal process and criminology; forensic examination; operational and search activity". - Dnipropetrovsk State University of Internal Affairs, Dnipro, 2023.

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

The author draws attention to the fact that in the mass media and in official sources there are reports about the consequences of the creation, use and distribution of malicious software in the form of failure of computers, computers, automated systems, computer networks or telecommunication networks , as well as various related equipment, about economic and moral damages as a result of unauthorized intervention and uncontrolled distribution of malicious software. One of the means, if not the solution to the problem of the creation of malicious programs or technical means for the purpose of illegal use, distribution or sale, then to slow down its aggravation is to bring the guilty persons to legal responsibility, in particular, criminal.

The main problems associated with the investigation of this type of crime, which have certain regularities, have been identified, the place of malicious software or technical means in the structure of the crime and the types of such malicious software have been determined, the subject of the crime for Art. 361–1 of the Criminal Code of Ukraine, which is a mandatory feature and is subject to mandatory establishment and proof, while for other crimes of Chapter XVI of the

Criminal Code of Ukraine, malicious software can act as tools or means of committing a crime. The concept and essence of crimes in the sphere of creation, use and distribution of malicious software are formulated. Considering the provisions of criminal law, the concept of malicious software was developed and formulated.

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

The provisions of the theory of criminal law in terms of criminalization of illegal acts related to the use of malicious software received further development, since direct use has a greater public danger than creation for the purpose of use and requires more effective criminal law protection.

It was determined that the provided forensic classification of such crimes is based not only on 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 informatics, programming and other sciences. Their main classification is based on the division of all methods into two main groups: active and passive.

The criminological definition of the concept of the method of committing a crime, which is somewhat different from the criminal-legal definition of the method of committing a crime, has received further development, as a sign of the objective side of the composition of the crime. It was determined that the method of committing the investigated crime is closely related to the technological features of the creation, use, distribution or sale of malicious software.

It is substantiated that, the method of committing the crime provided for in 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 harmful software or technical means, as well as their distribution or sale.

A proper 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 technical means, as well as their distribution or sale, is proposed.

The existence of a correlational dependence in the connections between the way the crime was committed and the person of the criminal, 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 assault, was established.

It is substantiated that the mechanism of the formation of computer traces takes place on three levels of computer information representation: 1) physical, on which physical fields act; 2) logical, on which computer programs operate; 3) semantic, on which the criminal acts using software and technical means. It is also determined that computer traces are also divided by location: 1) local (located in computer tools); 2) network (located on servers and communication equipment).

A forensic "portrait" of an offender who commits crimes related to the use of malicious software has been created. It has been established that he is a physical, sane person who has reached the age of 16, has the skills to master computer technologies, and knowingly uses them with the aim of encroaching on the functionality of the software of other computer devices or communication networks. The person of the criminal is a convict qualified in information and software, or a professionally trained person or group of persons who uses computer software for the purpose of having a harmful effect on the software of personal computers, servers or network communication.

It was determined that the direct object of criminal encroachment is malicious software, which are system software, software blocks and separate programs that are specially created to exert a harmful influence on other software by changing its functional features, or any other violation of property rights and rights use of computer software.

Typical investigative situations and the directions of their resolution in the investigation of crimes are defined, which determine the appropriate sequence of investigative actions and other tactical and forensic measures of the investigation of this crime. Among these measures, such areas as obtaining and analyzing evidence related to the creation and use of malicious software, overcoming resistance to investigative actions and involving experts in the field of information technologies and programming in investigative measures are of the most significant importance.

Systematized typical investigative situations in the investigation of crimes related to malicious computer programs, which consist in the fact that during the investigation of crimes committed with the use of computers, systems and other electronic equipment, the investigator deals with traditional forensics , as well as with non-traditional traces of criminal activity and material evidence.

It is substantiated that the tactics of carrying out individual investigative actions at the initial stage of the investigation of these crimes are determined by investigative situations and investigative versions, which are checked in the process of such investigative actions as extraction, inspection, search, interrogation, examination and other investigative measures. It was determined that the impartial approach of the investigator is the key basis of a successful investigation, which will be based, in addition to procedural norms, on the information and technical experience of the investigator and experts who are involved in the process of researching the crime scene.

It was concluded that the tactics of conducting investigative (search) actions depend on the specific circumstances of the crime, the planned investigative measures to establish the persons who committed (perpetrated) the crime and the expected results as a result of their conduct. The tactics of their conduct depend on the behavior of the persons who carry out the evidence, and the methods of specific investigative actions aimed at collecting and researching evidence, establishing the objective truth in the case and making a reasoned decision in criminal proceedings.

The concept of an expert 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 membership in the state register of certified forensic experts, as well as supplementing the Criminal Procedure Code of Ukraine with a norm that would define the very concept of forensic examination.

The work reveals the connection of research with scientific programs, plans and topics, lists the tasks and methods used in the process of researching the specified topic. Scientifically based proposals have been made regarding the practice of applying the current criminal procedural legislation of Ukraine on the issues under investigation.

The conducted research made it possible to formulate theoretical provisions and practical recommendations for the implementation of pre-trial investigation in criminal proceedings at the initial stage of the investigation of crimes in the field of creation, use and distribution of malicious software.

One of the means, if not the solution to the problem of the creation of malicious programs or technical means for the purpose of illegal use, distribution or sale, then to slow down its aggravation is to bring the guilty persons to legal responsibility, in particular , criminal. In addition, "malicious software", which is considered as specially created to interfere with the normal functioning of electronic computing machines and software devices, components or entire programs, as well as "harmful technical means", which is considered as simulated devices and equipment elements, which by their functional intended to cause damage to electronic computing machines and devices or software of the corresponding equipment, is the basic terminology in the category of pre-trial investigations carried out.

The author ascertained and additionally confirmed the understanding and scientific concept regarding the demarcation of forensic methods of carrying out a pre-trial investigation of the use, distribution or sale of harmful software or

technical means, as well as other, concomitant illegal encroachments in the relevant field.

A prominent place and due role in the structure of scientific novelty is highlighted because forensic approaches to the classification and identification of the person who uses, distributes or sells malicious software or technical means, which is directly related to the processes in the pre-trial investigation, for example, the identification of additional sources of evidence , which prove the guilt of the relevant person.

Keywords: initial stage of investigation, methods of committing crimes, criminal proceedings, harmful software tools, pre-trial investigation, tactics of conducting investigative (search) actions, trace pattern, forensic classification of crimes, sources of forensic information, typical investigative situations, nomination of investigative versions, use of special knowledge.

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.

ЗМІСТ:

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ

АЕОМ	Автоматизована електронно-обчислювальна машина
АС	Автоматизована система
АТМ	Автоматизований банківський термінал
ВП	Відділ поліції
ГУНП	Головне управління Національної поліції
ДСБЕЗ	Державна служба по боротьбі з економічними злочинами
ЕОТ	Електронно-обчислювальна техніка
ЖМД	Жорсткий магнітний диск
ЗЕОТ	Засіб електронно-обчислювальної техніки
ІС	Інформаційна система
ІТС	Інформаційно-телекомунікаційна система
КК України	Кримінальний кодекс
КПК України	Кримінальний процесуальний кодекс
МВС України	Міністерство внутрішніх справ
НСД	Несанкціонований доступ до інформації
ОВС	Орган внутрішніх справ
ОГП	Офіс Генерального прокурора
СБУ	Служба безпеки України
ст.	Стаття
ч.	Частина
ШПЗ	Шкідливий програмний засіб

ВСТУП

Обґрунтування вибору теми дослідження. Кримінальні правопорушення у сфері інформаційних технологій в 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-обчислювальної техніки, мережі Інтернет як правило відбувається за допомогою спеціально створених або пристосованих шкідливих програмних засобів використання яких призводить до суспільно негативних наслідків у вигляді матеріальних збитків, викрадення, спотворення або 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 гальмування її загострення є притягнення винних осіб до юридичної відповідальності, зокрема, кримінальної.

Таким чином протидія злочинам проти створення шкідливих програм чи технічних засобів з 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 при їх високій латентності та важливістю вказаних інформаційних об’єктів для суспільства.

Виходячи з аналізу кримінальних проваджень на території України, вказані 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). Крім 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 такі вчені як: К.С. Архіпова, Ю.М. Батурин, В.П. Бахін, П.Д. Біленчук, Т.П. Бірюкова, В.В. Бурлака, В.М. Бутузов, С.В. Веліканов, А.Ф. Волобуєв, В.К. Гавло, Ю.В. Гаврилин, Г.М. Гапотченко, В.І. Гончаренко, В.К. Гора, І.М. Горбаньов, В.Г. Дрозд, І.В. Дубівка, Р.М. Дударець, І.В. Європіна, Я.М. Ілляш, М.М. Коваленко, Я.Ю. Конюшенко, В.М. Коршунов, В.В. Кузнецов, М.А. Макаров, Т.В. Міхайліна, О.М. Моїсеєв, Р.С. Нєдов, Д.В. Письменний, О.І. Пінчук, С.О. Прутяний, Р.В. Сабадаш, М.В. Салтевський, Н.А. Селіванов, О.А. Солдатенко, О.П. Снігерьов, А.В. Старушкевич, А.В. Тарасюк, О.Ю. Татаров, Л.Д. Удалова, М.І. Хавронюк, В.Г. Хахановський, М.С. Цуцкірідзе , С.С. Чернявський, А.В. Шевчишен та інші, які присвячені досудовому розслідуванню окремих видів злочинів проти створення шкідливих програм чи технічних засобів з метою противопровного використання, розповсюдження або збуту. Значною мірою проведене дослідження ґрунтувалося на концептуальних положеннях таких кандидацьких дисертацій як Б.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.І. 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, грантами. 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 напрямах 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;

- змоделювати 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 противоправного 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 (додаток В); 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.).

Структура та обсяг дисертації. 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.

РОЗДІЛ 1. НАУКОВО-МЕТОДОЛОГІЧНИЙ ПІДХІД ФОРМУВАННЯ КРИМІНАЛІСТИЧНОЇ МЕТОДИКИ РОЗСЛІДУВАННЯ СТВОРЕННЯ, ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

1.1. Стан наукових досліджень проблем криміналістичної характеристики та початкового етапу розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Розвиток науково-технічного прогресу у сфері інформаційних технологій останнім часом зумовлює не тільки активізацію всіх сфер сучасного життя, але й виникнення та вдосконалення багатьох форм суспільних відносин, які виникають. Це виражається у різних формах обміну інформацією, формах фінансових розрахунків у бізнесі, особливостях PR-технологій у медіа-просторі тощо. Безумовно подібна динаміка є позитивною на шляху суспільного прогресу, оскільки вона засвідчує неодмінний розвиток науково-технічної думки, незважаючи на традиційність багатьох світових культур, зокрема у країнах ісламського світу. Гігантські обсяги інформації почали зберігатися в електронному вигляді та оброблятися з допомогою електронно-обчислювальних машин (комп'ютерів), подальший розвиток зв'язку зумовив появу міжнародних комп'ютерних мереж, зокрема Internet, що дало змогу одержувати та обробляти інформацію в глобальних масштабах.

Водночас у багатьох країнах, до яких слід віднести й Україну, поряд із позитивними особливостями розвитку інформаційних технологій, спостерігаються й негативні прояви тотальної інформатизації суспільних відносин. До таких негативних проявів можна зарахувати злочинність у сфері використання електронно-обчислювальних машин (комп'ютерів) та комп'ютерних мереж (Розділ XVI КК України), зокрема й такий злочин, як

створення, використання, розповсюдження або збут шкідливих програмних засобів. Програмні засоби останнім часом набули важливого інформаційно-технічного, економічного та гуманітарного значення, оскільки вони виступають інструментом використання й обробки інформації. Після появи глобальних комп'ютерних мереж виникла можливість вчинення протиправних дій щодо інформації в електронному вигляді.

Саме тому суспільна небезпека подібних злочинів із розвитком інформаційного суспільства постійно зростає, що зумовлює конструювання й постійне вдосконалення протидії подібним деліктним проявам як у сучасній юридичній науці, так і в правозастосовній практиці.

У цьому контексті необхідно погодитися із твердженням В. Г. Хахановського, який наголошує, що однією з головних умов підвищення рівня протидії злочинності є широке використання сучасних досягнень науково-технічного прогресу, які останніми роками найсуттєвіше проявляються у сфері інформаційних технологій. В органах та підрозділах Національної поліції України накопичено чималий досвід застосування новітніх комп'ютерних технологій у процесі запобігання злочинам, їх розкриття та розслідування, провадження слідчих дій, здійснення судових експертиз, у вирішенні інших криміналістичних завдань. Проте розробка, упровадження та використання інформаційних систем і технологій у Національній поліції України, як справедливо зазначає автор, має здебільшого безсистемний, стихійний характер, оскільки здійснюється як Департаментом інформаційно-аналітичної підтримки НП України, Управлінням кримінального аналізу НП України, Департаментом інформаційних технологій МВС України, так і окремо іншими галузевими підрозділами. Зазвичай окреслені процеси потребують узгодженості, унормування, урахування законодавчих та підзаконних нормативно-правових актів [121, с. 3].

Окрім цього, аналізуючи це вкрай важливе питання, на наш погляд, необхідно залучити ґрунтовні наукові розробки понятійно-теоретичного

інструментарію, який дозволить охарактеризувати основні визначення, категорії й поняття, котрі є значною мірою дискусійними в сучасній криміналістичній науці.

Саме криміналістична наука є найбільш ефективною в контексті вивчення кримінальних правопорушень, у сфері використання ЕОМ, систем та комп'ютерних мереж, зокрема, пов'язаних зі створенням, використанням, розповсюдженням шкідливих програмних засобів. До того ж криміналістика як наукова дисципліна й узагальнення практики є інструментом дослідження різних форм і способів учинення зазначеної специфічної категорії кримінальних правопорушень.

Таку позицію підтверджує й думка А. С. Білоусова, який наголошує, що в науковій літературі злочини, що вчиняють із використанням комп'ютерних засобів і систем, часто називають «комп'ютерними злочинами». До того ж цю дефініцію потрібно вживати не в кримінально-правовому аспекті, оскільки це лише ускладнює кваліфікацію діяння, а в криміналістичному, тому що вона пов'язана не з кваліфікацією, а власне зі способом вчинення й приховування злочину і, відповідно, з методикою його розкриття й розслідування [14, с. 5]. Саме тому методологійно криміналістика є основою формування наукових знань у сфері боротьби зі злочинами у сфері шкідливих програмних засобів.

Поняття злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів є інструментом наукового знання відносно нового часу, оскільки бурхливий розвиток інформаційних технологій припадає на другу половину XX століття і є складником у сфері комп'ютерної злочинності.

У той час вітчизняна юридична наука не ставила перед собою завдань розробки подібних формулювань, оскільки будь-яких загроз наявній системі електронної інформації ще не виникало. Ці проблеми постали перед законодавцем та науковцями пізніше.

На думку О. А. Федотова, Україну, яка поступово ставала повноправним членом міжнародної спільноти, теж не могла обійти ця

проблема. Саме з цієї причини в Україні в 1994 році встановлено кримінальну відповідальність за порушення роботи автоматизованих систем (ст. 198 Кримінального кодексу України (далі – КК України) 1960 р.), під яким розуміли «…умисне втручання в роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або її носіїв, а також розповсюдження програмних і технічних засобів, призначених для незаконного проникнення в автоматизовані системи і здатних спричинити перекрученим або знищення інформації чи носіїв інформації» [66; 120, с. 37].

На цьому етапі злочини у сфері шкідливих програмних засобів передбачені в міжнародних нормативних актах та національному кримінальному законодавстві, але їх термінологічні основи були сформульовані загалом, без належної конкретизації, як «програмні й технічні засоби, призначені для незаконного проникнення в автоматизовані системи і здатні спричинити перекручення або знищення інформації чи носіїв інформації».

Недосконаліть цих перших термінологічних формулювань вимагала подальшого їхнього розвитку й удосконалення, а тому й подальшого наукового осмислення.

Саме тому логічно буде розглянути розвиток термінологічного інструментарію поняття злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів у міжнародних правових актах, у національному законодавстві, а також у підходах науковців щодо їх визначення, структури й характерних типологійних ознак.

Від найперших формулювань і до сьогодні поняття правопорушень у сфері використання ЕОМ, їх види, а також терміни, якими вони визначалися, продовжували розвиватися й удосконалюватися, науково збагачуючи зміст цієї категорії.

Як констатує І. В. Європіна, відповідно до доктрини сучасного міжнародного кримінального права злочини з використанням шкідливих комп’ютерних технологій (інакше «кіберзлочини») віднесені до злочинів

міжнародного характеру. Перелік видів кіберзлочинів визначає Конвенція про кіберзлочинність (2001 р.), яка називає серед інших такі: незаконний доступ до комп'ютерної системи, нелегальне перехоплення технічними засобами комп'ютерних даних, втручання в комп'ютерні дані, втручання у функціонування комп'ютерної системи, підробка та шахрайство, пов'язані з комп'ютерами, правопорушення, пов'язані з дитячою порнографією тощо [41, с. 129].

У п. 14 Доповіді Комітету II Десятого Конгресу ООН 1960 р. із попередження злочинності й поводження з правопорушниками зазначено, що існує дві категорії злочинів: 1) кіберзлочини у вузькому розумінні («комп'ютерні» злочини) – будь-яке протиправне діяння, здійснюване шляхом електронних операцій, метою якого є подолання захисту комп'ютерних систем й оброблюваних ними даних; 2) кіберзлочини в широкому розумінні (злочини, пов'язані з використанням комп'ютерів) – будь-яке протиправне діяння, що вчинюють через комп'ютерну систему або мережу, зокрема такі злочини, як незаконне зберігання, пропонування або розповсюдження інформації через комп'ютерні системи або мережі [38, с. 338].

Спочатку використання ЕОМ при вчиненні традиційних правопорушень було передбачене «класичними» статтями КК і кваліфіковане відповідно до об'єкта злочину – як крадіжка, шахрайство тощо.

У зв'язку з розвитком інформаційних технологій визначення «комп'ютерний злочин» поступово трансформувалося в поняття «злочини у сфері інформатизації», під яким розуміють злочини, електронна обробка інформації за яких була знаряддям їх учинення або їхнім об'єктом. До кола проблем, об'єднаних таким поняттям, потрапили: шахрайство з кредитними магнітними картками, злочини у сфері телекомунікацій (шахрайство з оплатою міжнародних телефонних розмов), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів тощо [70].

На думку вчених-криміналістів, зокрема П. Д. Біленчука, В. К. Лисиченка, В. В. Лісового та інших, до цієї групи належать також і такі, що пов'язані з використанням доказів комп'ютерного походження при розслідуванні традиційних злочинів. Відповідно до міжнародної класифікації злочинів у сфері інформаційних технологій останні мають свої види й коди [70]. Наприклад, використання шкідливих програм пов'язане з несанкціонованим втручанням у роботу системи чи перехопленням інформації (QA), її зміною чи пошкодженням (QD), несанкціонованим копіюванням (QR), розкраданням комерційної таємниці (QZE) тощо [11].

У той же час, криміналістичні особливості злочинності, пов'язаної з використанням шкідливих програмних засобів, знайшли своє узагальнення в термінологічному тлумаченні законодавчих актів іноземних держав.

Різні країни пішли неоднаковими шляхами при кримінально-правовому регулюванні вказаних вище діянь. У багатьох державах відповідальність за вчинення злочинів у сфері інформатизації настає за традиційними статтями кримінального законодавства (крадіжка, шахрайство, підробка тощо). Деякі з них уже мають спеціальні норми в кримінальному законодавстві, що дають визначення вказаним явищам і передбачають відповідальність за їх вчинення, інші – тільки в процесі прийняття відповідних законів. Так, у законодавстві низки європейських країн (Австрія, Данія, Франція) передбачена кримінальна відповідальність за неправомірне втручання у функціонування інформаційно-обчислювальних систем. Наприклад, зі змісту норм кримінального права Великобританії випливає, що його санкції застосовують до зловмисників, які заподіяли за допомогою ЕОМ шкоди чи користувались інформацією у своїх цілях. Кримінальна поліція ФРН до таких злочинів зараховує всі протиправні дії, за яких електронна обробка інформації є знаряддям їх учинення і (чи) їх об'єктом [70, с. 86].

З огляду на ситуацію, що склалася, законодавець у Кримінальному кодексі України (надалі – КК України) 2001 року передбачив окремий Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин

(комп'ютерів), систем та комп'ютерних мереж». Останній містив три статті, відповідно до яких встановлювалась кримінальна відповідальність за протиправні діяння в галузі використання комп'ютерної інформації, а саме:

1) незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (ст. 361 КК України);

2) викрадення, привласнення, вимагання комп'ютерної інформації або заволодіння нею шляхом шахрайства або зловживання службовим становищем (ст. 362 КК України);

3) порушення правил експлуатації автоматизованих електронно-обчислювальних систем (ст. 363 КК України) [72, с. 808–818].

У цьому контексті О. А. Федотов наголошує, що законодавець увів низку нових понять, які раніше не простежувалися не лише в кримінально-правовій термінології, а й у законодавстві, яке регулює інформаційні відносини. Ці терміни потребували й потребують пояснень, обґрунтованих на розумінні як технічних характеристик нових засобів обробки інформації, так і сутності самої інформації нової криміналістичної категорії. Слід також зазначити, що сучасні «хакери» є настільки винахідливими, що законодавці не встигають визначати нові сфери зловживань, які вчиняють в інформаційних системах [120, с. 38].

Однак уведення трьох зазначених вище статей у кримінальне законодавство України повною мірою не задовольнило ані науковців, ані практичних працівників, які безпосередньо мали справу з розкриттям та розслідуванням «комп'ютерних» злочинів. Усе це призвело до перегляду кримінально-правових норм (ст.ст. 361–363-1 КК України) і внесення суттєвих змін до чинного КК України. Зокрема, було доповнено саму назву Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» та розширено кількість правових норм із трьох до шести [120, с. 39].

Розділ XVI КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» характеризує особливості досліджуваної категорії злочинів таким чином:

- несанкціоноване втручання в роботу інформаційних (автоматизованих), електронних комунікаційних, інформаційно-комунікаційних систем, електронних комунікаційних мереж (ст. 361 КК України);

- створення з метою протиправного використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1 КК України);

- несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації (ст. 361-2 КК України);

- несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, учинені особою, яка має право доступу до неї (ст. 362 КК України);

- порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них обробляється (ст. 363 КК України);

- перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1 КК України) [39].

Указані новації в Законі України про кримінальну відповідальність призвели до пожвавлення розвитку наукової думки в багатьох галузях

юридичної науки. Не залишилися на узбіччі осмислення цих кримінально-правових положень і представники криміналістичної науки.

Так, на думку О. П. Снігерьова та В. О. Голубєва, злочини у сфері комп'ютерних програм умовно можна розподілити на дві великі категорії: злочини, пов'язані з втручанням у роботу комп'ютерів, і злочини, у яких використовують комп'ютери як необхідні технічні засоби [107].

Цю думку розвиває Н. А. Розенфельд, наголошуючи, що несанкціонований доступ до комп'ютерної інформації або умисне розповсюдження шкідливих комп'ютерних програм іноді є способом вчинення злочину, предмет якого відрізняється від предмета комп'ютерних злочинів, або вчиняється з метою полегшення іншого злочину, усунення перешкод щодо його вчинення або приховування його [98, с. 194].

Водночас слід підтримати думку Д. В. Пашнєва про те, що надане вище визначення не дає чіткого розуміння структури системи комп'ютерних злочинів відповідно до КК України, а Н. А. Розенфельд, вочевидь, взагалі не відносить до комп'ютерних названі злочини [90].

У цьому контексті, уважаємо більш слушною дефініцію В. О. Голубєва, який визначає злочин у сфері шкідливих комп'ютерних програм як порушення роботи ЕОМ чи мереж ЕОМ. Зокрема, автор зазначає, що порушення роботи ЕОМ, системи ЕОМ або їхньої мережі містить у собі збій у роботі ЕОМ, системи ЕОМ або їх мережі, що перешкоджає нормальному функціонуванню обчислювальної техніки за умови збереження її фізичної цілісності (наприклад, відображення неправильної інформації на моніторі, порушення порядку виконання команд, розрив мережі тощо) [29, с. 37].

Визначаючи систему комп'ютерних злочинів, А. Ф. Волобуєв виділяє три групи злочинів.

Перша група – це злочини, у яких специфічні властивості комп'ютера виступають як безпосередній предмет посягань (розкрадання машинного часу, несанкціоноване втручання в процес обробки інформації, несанкціоноване використання комп'ютерної інформації, знищення

комп’ютерних даних або програм, несанкціоноване копіювання комп’ютерних програм).

Друга група – злочини, учинені шляхом використання комп’ютерної системи як засобу досягнення злочинної мети. Водночас автор уважає, що оскільки комп’ютер тут використаний як знаряддя, то такі злочини називати комп’ютерними не можна. На його думку, вони повинні мати назву відповідно до предмета посягання та способу заволодіння ним, наприклад, розкрадання грошей (власності) шляхом привласнення (зловживання службовим становищем, шахрайства) з використанням комп’ютера. Тобто це традиційні злочини, для вчинення яких з’явився новий засіб.

Третя група – злочини, пов’язані з комп’ютером. Насамперед до цієї категорії зараховують:

а) злочини, у яких комп’ютер виступає як предмет безпосереднього посягання, як матеріальна цінність (наприклад, крадіжка комп’ютера);

б) злочини, у яких комп’ютер виконує роль допоміжного засобу зв’язку між співучасниками або сховища певної інформації [24].

Водночас Д. В. Пашнєв, аналізуючи комп’ютерні засоби як знаряддя злочину (зокрема програми), наголошує, що злочини вчиняють або з прямого доступу до комп’ютерного засобу, у якому зберігаються дані, або з віддаленого доступу з використанням інших комп’ютерних засобів, або за допомогою засобів, спеціально пристосованих для доступу до комп’ютерної інформації інтегрованих і вбудованих засобів – комп’ютерних програм. У будь-якому разі ці дії неможливо вчинити без використання комп’ютерних технологій як засобу вчинення злочину. Що ж стосується четвертої групи, то очевидно, що при вчиненні будь-якого злочину комп’ютерні технології можуть бути засобом інформаційного забезпечення злочинної діяльності, тобто збору, зберігання, обробки, передачі комп’ютерної інформації, що належить до злочину. Проте ці злочини не можуть бути віднесені до комп’ютерних, адже в них комп’ютерні технології не використовують як

засіб. Такі злочини не є специфічно комп’ютерними, що характеризуються особливим способом та слідовою картиною [90].

Висловлена в такий спосіб думка науковця, на наш погляд, є не зовсім коректною, оскільки автор використав термін неоднозначного значення «засіб» у незрозумілій інтерпретації. У контексті його висловлювання не зрозуміло, про який «засіб» ідеться – чи це матеріальний об’єкт у загальному значенні, чи факультативна ознака об’єктивної сторони складу злочину з термінології кримінального права. Проте ця неточність не впливає на сформовану автором систему комп’ютерних правопорушень. Тим більше, що це обумовлено ще й не зовсім вдалим формулюванням законодавця, на чому ми зупинимося пізніше.

Окрім різних концепцій учених, класифікаційні основи криміналістичних ознак злочинів, пов’язаних із шкідливими програмними засобами, однозначно відображені у ст. 361-1 КК України, яка, як вже було зазначено вище, установлює кримінальну відповідальність за створення з метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв'язку. Аналізуючи вказану статтю, науковці розділяють шкідливі програмні та технічні засоби, оскільки, як ті, так і інші, можуть бути засобом учинення такого злочину. Але їх обов’язковою ознакою є здатність впливати на процес обробки інформації, його спотворення, у результаті чого інформація (її носії) може бути знищена чи перекручена.

Зокрема, Т. В. Міхайліна, яка досліджувала питання кваліфікації злочинів, передбачених ст. 361-1 КК України, визначила, що обов’язковою ознакою фактично всіх складів злочинів є *знаряддя* їх вчинення – відповідні програмні й технічні засоби, за допомогою яких учиняють посягання й вони (засоби) підлягають конфіскації згідно з вимогами санкцій до статей 361, 361-1, 361-2, 362, ч. 2 ст. 363-1 КК [73, с. 459–464].

Не заперечуємо й того факту, що шкідливі програмні й технічні засоби в зазначених злочинах, за винятком, передбаченим ст. 361-1 КК України, можуть виступати знаряддями або засобами вчинення злочину. Предметом цих злочинів будуть електронно-обчислювальні машини, автоматизовані системи, комп'ютерні мережі, мережі електрозв'язку.

Предметом злочину, що передбачений ст. 361-1 КК України, є шкідливі програмні або технічні засоби, призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Цієї думки дотримується переважна більшість представників кримінально-правової науки [63, с. 536; 78, с. 946].

Такої самої практики дотримуються й суди при розгляді кримінальних проваджень. Так, Білогірський районний суд Хмельницької області виправдав підсудних О. і С., яких звинувачували в учинені злочину, передбаченого ст. 361-1 КК України, за відсутності предмета злочину, і, відповідно, за відсутності в їхніх діях складу злочину.

Згідно з висновком експерта від 27 серпня 2014 року № 56 кт програма «Keylogger Net» (у використанні якої їх звинувачено), що міститься на USB флеш-накопичувачі «Silicon Power» й надана для дослідження, буде мати ознаки шкідливого програмного забезпечення за умови, якщо її встановлення відбувається без відома власника (адміністратора безпеки) автоматизованої системи або без відома власника конкретного персонального комп'ютера. Цих умов дійсно не було дотримано, і це означає, що предмета злочину не було.

Згодом до такої самої думки щодо місця шкідливих програмних або технічних засобів у структурі складу злочину, передбаченого ст. 361–1 КК, дійшла і Т. В. Міхайліна [73].

Під комп'ютерною програмою Закон України «Про авторське право та суміжні права» розуміє набір інструкцій у вигляді слів, цифр, кодів, схем, символів чи в будь-якому іншому вигляді, виражених у формі, придатній для

зчитування комп'ютером, які приводять його в дію для досягнення певної мети або результату (це поняття охоплює як операційну систему, так і прикладну програму, виражені у вихідному або об'єктному кодах) [93].

Виходячи з диспозиції ст. 361–1 КК України, кримінально-караним є розповсюдження шкідливих програмних або технічних засобів. Як приклад таких дій можна змоделювати ситуацію: особа за допомогою програмного або технічного засобу «зламує» систему захисту комп'ютерної мережі й запускає в неї вірус [43, с. 60]. Такі випадки є характерними злочинними проявами сьогодення. Наприклад, за даними слідчого відділу УСБУ в Донецькій області невстановленими особами за допомогою інтернет-сайтів vzlomat.org, vkbot.org та іншими систематично здійснюється розповсюдження програмного забезпечення, яке згідно з висновком УНДІСТСЕ СБ України № 280 від 27.03.2013 року [128] віднесено до шкідливого програмного забезпечення. Ці сайти зареєстровані на підприємствах, котрі знаходяться в різних населених пунктах України. Хост-провайдерами зазвичай у таких випадках визначають осіб під вигаданими прізвищами.

Водночас не можна не звернути уваги на те, що наведене в досліджуваній статті визначення є некоректним з погляду сутності поняття «розповсюдження комп'ютерного вірусу». За особливостями розповсюдження комп'ютерні віруси поділяють на файлові, бутові (завантажувальні) та мережні. До файлових вірусів відносять такі, що розповсюджуються шляхом упровадження в командні, виконавчі файли або файли драйверів, які завантажуються, тобто програм, до яких звертається і з якими працює користувач, Бутові віруси, або віруси, що завантажуються, розповсюджуються шляхом «зараження» завантажувального сектора гнучкого або жорсткого носія. Мережні віруси використовують для свого розмноження можливості спеціального програмного забезпечення, яке організовує функціонування комп'ютерної мережі. Наслідки використання таких вірусів здебільшого полягають у переповненні пам'яті комп'ютера, підключеного до

мережі, копіями вірусу, що призводить до неможливості роботи з інформацією, яка міститься в цій ЕОМ [43, с. 60].

Отже, розповсюдження комп'ютерного вірусу можна здійснити трьома способами: упровадженням вірусу в програми; «зараженням» завантажувального сектора носія; розповсюдженням вірусу з використанням мережного програмного забезпечення [49].

Якщо розуміти закон розповсюдження комп'ютерного вірусу зазначеним у статті 361-1 КК України способом, то можна зробити висновок, що диспозиція статті не повною мірою охоплює всі можливі способи розповсюдження комп'ютерного вірусу, які відомі в інформатиці та зустрічаються в практиці. Так, наприклад, наприкінці грудня 1987 року студент університету Clausthal-Zellerfeld (Німеччина) розробив вірус Christmas Tree (Різдвяна ялинка). Цей вірус належав до категорії мережних, і наслідки його роботи полягали в блокуванні комп'ютерів, підключених до мережі. Згідно з програмою його автора вірус розповсюджувався шляхом використання звичайного механізму електронної пошти [49].

Подібні суспільно небезпечні дії, якби вони були здійснені в Україні, не можна було б кваліфікувати за статтею 361-1 КК України. Дії автора цього вірусу не підпадають під ознаки розповсюдження вірусу, передбаченого статтею 361-1 КК України, оскільки програмне забезпечення функціонування електронної пошти не є програмним засобом, призначеним для незаконного проникнення в роботу автоматизованих систем, тобто в такому випадку комп'ютерний вірус не розповсюджувався за допомогою шкідливого програмного або технічного засобу [43, с. 63].

Як констатує Т. В. Міхайліна, диспозицію статті 361–1 розширено, порівняно з попередньою редакцією ст. 361 КК України, що встановлювала кримінальну відповідальність лише за розповсюдження комп'ютерних вірусів. Можна погодитись з тим, що вживання терміна шкідливі програмні «засоби» є більш доречним, оскільки існує велика кількість програм, які за

своєю природою не є вірусами, але здатні спричинити порушення в роботі електронно-обчислювальних машин [73].

Найпоширенішими різновидами шкідливих програмних засобів, які підпадають під дію цієї статті, є комп'ютерні віруси – комп'ютерні програми, здатні після проникнення до операційної системи ЕОМ чи до автоматизованої системи порушити нормальну роботу комп'ютера, АС чи комп'ютерної мережі, а також знищити, пошкодити чи змінити комп'ютерну інформацію [77, с. 946]. Характерною ознакою вірусів вважають їх здатність до самовідтворення та до модифікації програми, до якої вони приєднані; програми, призначені для нейтралізації паролів та інших засобів захисту комп'ютерних програм чи комп'ютерної інформації від несанкціонованого доступу; програми-шпигуни, які після їх проникнення до певної АС, комп'ютерної мережі, операційної системи ЕОМ чи окремої комп'ютерної програми забезпечують несанкціонований доступ сторонньої особи до інформації, яка зберігається в ЕОМ, АС, мережі чи програмі або ж непомітно для власника чи законного користувача здійснюють несанкціоновану передачу такої інформації сторонній особі [77, с. 947].

Для більш конкретного розмежування програмних засобів від інших технічних засобів необхідно звернути увагу на те, що під технічними засобами слід розуміти будь-які технічні пристрої, за допомогою яких без використання комп'ютерних програм здійснюють вплив на роботу ЕОМ [79, с. 977]. Це різного роду прилади, устаткування тощо, із допомогою яких можливе або безпосереднє підключення до АЕОМ, їх систем або комп'ютерних мереж чи каналів передачі даних, або які здатні шляхом формування сигналів, полів, середовищ створити умови для несанкціонованого доступу до інформації з метою ознайомлення з такою інформацією особами, які не мають права доступу до неї, або з метою впливу на процес обробки інформації в ЕОМ, порушення роботи АЕОМ, їх систем чи комп'ютерних мереж, перекручення або знищення комп'ютерної інформації чи її носіїв [116, с. 690].

Учинення злочинів шляхом використання, розповсюдження чи збуту шкідливих програм деякі автори, зокрема Л. В. Борисова, пропонують трактувати, як будь-яке протиправне діяння, що здійснюється за допомогою програмних або технічних засобів і має на меті впливати на засоби комп'ютерної безпеки та дані, що обробляють або зберігають в комп'ютерній системі, структури їх розміщення в пам'яті ЕОМ, програми управління базами даних, якщо вони призвели до знищення, блокування, модифікації або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ і їх мереж, а також другорядні чи побічні загрози, зокрема такі, як підготовка до більш серйозних атак – передача комп'ютерних паролів, ключів кодування, кодів доступу тощо. Криміналістичну характеристику комп'ютерних злочинів розглядають як ймовірна модель орієнтувальної інформації, яка містить криміналістично значущі ознаки й слугує для конкретизації цілей та напрямів розслідування. Об'єднувальним принципом є видові склади злочинів і найбільш характерні способи їх вчинення [16, с. 46].

Як зазначає В. О. Голубєв, категорія «комп'ютерні злочини» містить у собі всі протизаконні дії, якщо електронне опрацювання інформації було знаряддями їх вчинення або предметом посягання [28, с. 133]. Слід підтримати таку позицію вченого, оскільки вона універсалізовано узагальнює дві основних тенденції у визначенні поняття досліджуваного злочину: 1. Комп'ютерні програми як знаряддя; 2. Комп'ютерні програми як предмет посягання.

Теорія кримінального права визначає знаряддя й засоби вчинення злочину, як речі матеріального світу, використовуючи які, або за допомогою яких у той чи інший спосіб полегшується вчинення злочину (виконання його об'єктивної сторони) [61, с. 104]. Знаряддя й засоби вчинення злочину вважають факультативними (необов'язковими) ознаками об'єктивної сторони злочинів, передбачених статтями 361, 361–2, 362, 362–1, 363-1 КК України. Їх жодним чином не згадують у диспозиціях вказаних кримінально-правових норм.

Предметом злочину визнають речі (фізичні утворення) матеріального світу, з приводу яких чи у зв'язку з якими вчинений злочин [61, с. 104]. Впливаючи на предмет, використовуючи його властивості, заподіюється шкода суспільним відносинам, які виступають об'єктом злочину.

В. В. Кузнецов обґрунтував висновок про те, що інформація, зокрема й комп'ютерна, також може виступати предметом злочину [68, с. 82]. Оскільки в диспозиції статті 361–1 КК України міститься безпосередня вказівка на шкідливі програмні чи технічні засоби, предмет злочину для цього складу є обов'язковою ознакою й підлягає обов'язковому встановленню та доказуванню.

Для решти злочинів XVI Розділу КК України шкідливі програмні чи технічні засоби можуть виступати як знаряддя чи засоби вчинення злочину. У цьому контексті було б доцільним зауважити, що в наявному вигляді зазначена кримінально-правова норма виглядає дещо некоректною, оскільки в ній йдеться про шкідливі програмні чи технічні засоби, а в структурі цих складів такі засоби виступають як знаряддя або засоби об'єктивної сторони. Виглядає це як висловлення «дерево дерев'яне». Тому з метою усунення можливих непорозумінь та плутанини було б доцільним змінити в диспозиції статті 361–1 КК термін «знаряддя» на терміни «програмні матеріали» та «технічне обладнання».

Проте, на наш погляд, шкідливі програмні засоби виступають здебільшого як знаряддя, оскільки їх призначення – нанесення шкоди програмному забезпеченню і порушенню роботи комп'ютеризованих систем. І навіть у разі збуту шкідливих комп'ютерних програмних засобів вони не можуть бути предметом отримання прибутку, оскільки використання вартості цих програм є засіб отримання прибутку або нанесення шкідливих наслідків з іншою метою, наприклад, у хуліганських цілях. Водночас подібні шкідливі програми, у разі їх використання, можуть бути предметом посягання тоді, коли за їх допомогою отримують інші шкідливі програми для вчинення злочинів.

Стосовно розуміння об’єктивних проявів незаконних дій із шкідливими програмами серед науковців також не спостерігається одностайного бачення.

Загалом, як підкреслює М. В. Карчевський, у літературі немає єдиного тлумачення самого поняття розповсюдження шкідливих програмних і технічних засобів [44, с. 90]. Тому, виходячи із законодавчої конструкції кримінального правопорушення, передбаченого ст. 361–1 КК України вбачається, що кримінальна відповідальність встановлена за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут.

Аналізуючи об’єктивну сторону злочину, варто звернути увагу на певну непослідовність законодавця при криміналізації видів діянь зі шкідливими програмними чи технічними засобами. Так, у диспозиції досліджуваної статті передбачено кримінальну відповідальність за створення шкідливих програмних чи технічних засобів із метою їх використання, але не криміналізовано використання. Це виглядає дещо нелогічним, оскільки безпосереднє використання, вочевидь, має більшу суспільну небезпечність, ніж створення з метою використання. Таким чином, було б доцільно доповнити частину 1 статті 361–1 КК України таким текстом: «створення з метою використання, розповсюдження або збуту, а також використання, розповсюдження або збут шкідливих програмних чи технічних засобів...».

Таким чином, характеристика понятійних особливостей злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів засвідчує закономірні ознаки поняття, побудовані на нормативних та концептуальних позиціях і засвідчує дискусійність багатьох категорій і понять.

Тому в авторському розумінні злочин у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів – це винне кримінально каране діяння, учинене одноосібно чи групою осіб із метою нанесення негативних наслідків іншому комп’ютерному програмному забезпеченню для отримання матеріальної вигоди чи іншого нематеріального

задоволення, яке нанесло матеріальні чи інші нематеріальні збитки шляхом порушення функцій програмного та інформаційно-комунікативного забезпечення комп'ютерного обладнання, а також комунікативних мереж і електронних накопичувальних пристроїв.

Отже, визначення такого злочину побудоване на міждисциплінарному кримінально-правовому і криміналістичному розумінні феномену протиправної поведінки, пов'язаної з використанням новітніх інформаційних технологій, що, зі свого боку, вимагає розгорнутої криміналістичної характеристики.

Як уже було наголошено, у цьому підрозділові ми цікавилися питаннями наукових досліджень щодо створення, використання та розповсюдження шкідливих програмних засобів. Успішне вирішення цього питання невіддільне від найдокладнішого розгляду сутності самого поняття шкідливих програмних засобів.

Відсутність чіткого визначення поняття шкідливих програмних засобів дає змогу правопорушникам у деяких випадках уникати відповідальності за їх учинення, ускладнює роботу правоохоронних та судових органів в частині уніфікованого застосування законодавства, покликаного подолати кіберзлочинність.

Після того, як Кримінальний кодекс України було доповнено ст. 361–1 КК України «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут», поняття «шкідливий програмний засіб» порівняно з попереднім значенням було викладено у значно ширшому розумінні.

Привертає до себе увагу те, що законодавець установив кримінальну відповідальність не за якісь незаконні маніпуляції з програмними засобами, а за певні дії з шкідливими програмними засобами. Тобто визначальне значення має те, що зазначені програмні засоби є шкідливими. Тому для з'ясування сутності понятійного змісту кримінально-правової норми почнемо з розкриття етимологічного змісту поняття «шкідливий».

За Новим тлумачним словником української мови, «шкідливий» – це такий, що здатний завдавати і завдає шкоди, збитків кому, чому-небудь [81, с. 811]. При цьому законодавець у простому складі цього злочину навіть не згадує про заподіяння будь-якої шкоди, задовольняючись тим фактом, що предметом злочину виступають шкідливі програмні засоби.

Так, відповідно до змісту диспозиції цієї статті головною ознакою віднесення будь-якого програмного засобу до категорії «шкідливий» є не фактичне його використання, а конструктивне (інженерне) призначення. Тобто кримінальна відповідальність настає у трьох чітко визначених випадках: створення шкідливого програмного засобу з метою несанкціонованого втручання в роботу ЕОТ; створення шкідливого програмного засобу з метою розповсюдження або його збуту; розповсюдження або збут шкідливого програмного засобу.

У своїх дослідженнях В. М. Бутузов, С. Л. Остапець та В. П. Шоломивцев під «шкідливими програмними засобами» розуміють створення або пристосування комп’ютерної програми, що призначені для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп’ютерів), автоматизованих систем, комп’ютерних мереж чи мереж електрозв’язку. Але й на їх думку переважно це різноманітні види так званих «комп’ютерних вірусів» [19].

Таке твердження, уважаємо, є не зовсім коректним, адже окрім комп’ютерних вірусів, є багато інших шкідливих програмних засобів, а комп’ютерний вірус є лише одним із їх різновидів.

Програмний засіб за своїм змістом є складним продуктом інтелектуальної діяльності, логічна послідовність виконання певних арифметичних алгоритмів призначена для автоматизації заздалегідь визначених процедур. Програмні засоби нерозривно пов’язані з функціонуванням ЕОТ. За своїм задумом вони призначені для посилення розумових здібностей людини, швидкого оброблення значного масиву

інформації, виконання складних та специфічних обчислень, що вимагається сьогоденням науково-технічного прогресу.

Судова практика зазначає, що програмні засоби можуть бути шкідливими, якщо вони за своїми ознаками здатні несанкціоновано порушити конфіденційність, доступність та цілісність інформації, яка обробляється автоматизованою системою або передається мережами електрозв'язку [109].

До категорії «шкідливий» зараховують також програмний засіб, призначений для несанкціонованого втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку.

Шляхом наукових та практичних спостережень установлено, що саме «прихованість», «деструктивність» та «несанкціонованість» є найголовнішими характеризувальними ознаками шкідливого програмного засобу. Тобто при віднесенні програмного засобу до категорії «шкідливий» спеціаліст експерт повинні насамперед визначати такі основні ознаки.

При встановленні ознак шкідливості програмного засобу необхідно звертати увагу на мету його створення. У разі створення програмного засобу лише для несанкціонованого проникнення для ЕОТ, такий програмний засіб необхідно зараховувати до шкідливого програмного засобу.

Якщо програмний засіб створювався для інших цілей та за своїм конструктивним задумом не містив ознак шкідливості, але був схожий із шкідливим програмним засобом і був використаний для несанкціонованого втручання в роботу ЕОТ (наприклад, перевірка систем захисту комп'ютерних мереж, стійкості до злому інших програмних засобів), то його необхідно віднести до програмного засобу, який пристосований для несанкціонованого втручання, адже, крім шкідливих ознак, він має й інші конструктивні завдання, що були в нього закладені при створенні. В інших джерелах такі програмні засоби визначають як програми подвійного призначення [114].

Однією з ознак шкідливих програмних засобів є функція подолання захисту систем ЕОТ, перешкоджання її нормальній діяльності. Ключовим

моментом дії шкідливих програмних засобів є відсутність добровільної згоди, обізнаності такого втручання в роботу ЕОТ.

Під здатністю програмного засобу до несанкціонованого втручання також необхідно розуміти можливість її самовідтворення за певних умов, масову розсилку, самокопіювання на диск, як на вільні місця, так і замінюючи собою іншу інформацію на жорсткому диску комп'ютера або її шифрування.

Варто наголосити, що будь-який програмний засіб, якщо в ньому міститься хоча б одна деструктивна (шкідлива) або прихована функція, що діє поза волею користувача або оператора, несе в собі суспільну небезпеку. Наприклад, легальне програмне забезпечення, що містить у собі приховану функцію надання віддаленого доступу до комп'ютера користувача та здійснення такого несанкціонованого втручання поза волею його власника або користувача. Такий програмний засіб повинен визнаватись як шкідливий програмний засіб.

Шкідливий програмний засіб має відповідати спеціальним критеріям, які визначають його цільове призначення – несанкціоноване втручання в роботу ЕОТ. Відповідно до критерія оцінки шкідливим програмним засобом можна вважати будь-який програмний засіб, що має приховану деструктивну властивість та визнається за таких умов:

1) призначений для несанкціонованого втручання, зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ, використовується спеціально для цього розроблений програмний код (сигнатура, модуль), що заздалегідь визначений розробником;

2) наявність середовища, через яке було здійснено проникнення: локально, через мережу «Інтернет», окремі оптичні, магнітні носії або конкретну команду на ЕОТ;

3) наявність певної події, яка передувала проникненню ШПЗ або системного алгоритму, за наявності якого почав діяти шкідливий програмний

засіб (наприклад, наявність встановленого клієнт-банку, інтернет-гаманця електронних грошей тощо);

4) самодостатність програмного коду шкідливого програмного засобу для виконання задуму розробника;

5) достатня стійкість шкідливого програмного засобу до подолання систем захисту ЕОТ.

Для віднесення програмного засобу до категорії «шкідливий» він має відповідати одночасно всім визначеним вимогам. Для встановлення цих критеріїв потрібні спеціальні знання, тому для визначення шкідливого програмного засобу призначають судову комп'ютерно-технічну експертизу [96] та її різновид – програмно-комп'ютерну експертизу.

Шкідливий програмний засіб є специфічним джерелом підвищеної небезпеки. Ця специфічність шкідливих програмних засобів полягає саме в їх конструктивному призначенні щодо несанкціонованого втручання в роботу ЕОТ, а також здатності для маскування.

Підсумовуючи викладене, можна констатувати, що шкідливий програмний засіб – це програмний засіб у вигляді коду, скрипта, активного контенту, програмного забезпечення, який існує в кібернетичному середовищі, спеціально створений і конструктивно призначений та технічно придатний для несанкціонованого втручання в роботу електронно-обчислювальної техніки, який не має будь-якого іншого програмного, технічного, господарського, а також прикладного призначення, що призводить до зміни, модифікації, блокування, копіювання або знищення інформації, споживання технічних ресурсів ЕОТ. Таке визначення, на нашу думку буде, найбільш точно відповідає вимогам сьогодення та актуальності заходам протидії кіберзлочинності.

1.2. Способи створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Криміналістичний аналіз учинення злочинів, пов’язаних із шкідливими програмними заходами, являє собою певну структуру, у якій одне з основних місць належить вивченню способів вчинення досліджуваних злочинів, як одного з найбільш специфічних інструментів злочинної діяльності, оскільки вчинити подібні злочини можуть тільки висококваліфіковані спеціалісти, що й ускладнює механізми розслідування, кваліфікації і профілактики таких злочинних проявів.

За результатами соціологічних досліджень, на кіберзлочинність припадає 23 % випадків шахрайства у світі, 17 % – в Україні. Дані також свідчать про те, що кіберзлочини стають більш витонченими, що ускладнює їхнє виявлення й запобігання. Це може призвести до ще більших збитків і втрат у майбутньому. 36 % респондентів в Україні вважають, що кіберзлочинність – це зовнішня загроза, 24 % – внутрішня. На думку 34 % респондентів, загроза може йти як ззовні, так і зсередини організації. Ці показники трохи відрізняються від результатів усесвітнього огляду, оскільки в організаціях інших країн відзначають, що ризик такої злочинності переважно йде ззовні (46 %) і тільки 13 % переконані, що злочин вчиняли співробітники фірм і корпорацій. Основними кібершахраями визнані клієнти й постачальники [45].

Кримінально-правова наука визначає спосіб вчинення злочину як форму прояву суспільно небезпечного діяння, тобто прийоми й методи, які використовував злочинець для вчинення злочину [62, с. 119].

Кримінально-правове визначення поняття способу вчинення злочину як факультативної ознаки об’єктивної сторони складу злочину дещо відрізняється від свого криміналістичного аналогу. Відповідно до положень криміналістичної науки способом вчинення злочину прийнято вважати прояв діяльності суб’єкта (не тільки його поведінку, а й закономірне відтворення використання предметів – засобів діяльності), опосередкований об’єктивними умовами, у яких виникла й розвивалася протиправна дія [9].

Зазвичай така діяльність стосується підготовки, учинення й приховування злочинного діяння. Проте не обов'язково, щоб спосіб мав усі названі елементи. Існують злочини, у яких злочинець через низку причин не здійснює ніяких дій із їх приховання або не може їх здійснити (наприклад, через неадекватний психічний стан злочинця тощо). Але такі факти зустрічаються доволі нечасто. Здебільшого під час учинення злочинів, що вимагають від злочинця інтелектуального підходу, він намагається приховати злочин шляхом знищення залишених слідів, а крім того, і вживання заходів, щоб таких слідів не залишати, фальсифікації обстановки події або самих слідів тощо. Мета цих дій, з одного боку, перешкодити своєчасному виявленню злочину, із другого – перешкодити встановленню особи злочинця [125, с. 284].

Наслідки вчинення злочину з використанням шкідливих програмних засобів не завжди можуть відображати способи їх учинення, оскільки інколи про вчинення такого злочину можуть свідчити тільки негативні соціальні зміни. Спосіб учинення досліджуваного злочину тісно пов'язаний із технологічними особливостями створення, використання, розповсюдження або збуту шкідливих програмних засобів.

Як слушно наголошує Д. В. Пашнєв, у криміналістиці такі злочини варто називати «злочинами, скоєними з використанням комп'ютерних технологій». Такий термін буде вказувати на саму технологію здійснення злочинів, що визначає способи їх скоєння. Крім того, комп'ютерні технології розроблені для обробки інформації в цифровому виді, яка і є, зрештою, предметом злочинного посягання таких злочинів. Таким чином, термін «злочини, скоєні з використанням комп'ютерних технологій» дозволить охопити всі діяння, учинені з використанням досягнень цих технологій, і такі, що посягають на оброблювану комп'ютерну інформацію [91, с. 109]. Отже, спосіб учинення досліджуваного злочину безпосередньо виражений у формі створення, використання, розповсюдження або збуту шкідливих програмних засобів.

Водночас не можна не звернути уваги на те, що наведене в законі визначення є некоректним з погляду сутності поняття «розповсюдження комп'ютерного вірусу». За особливостями розповсюдження комп'ютерні віруси поділяються на файлові, бутові (завантажувальні) та мережні. До файлових вірусів зараховують такі, що розповсюджуються шляхом упровадження в командні, виконавчі файли або файли драйверів, які завантажуються, тобто програм, до яких звертається і з якими працює користувач. Бутові віруси, або віруси, що завантажуються, розповсюджуються шляхом «зараження» завантажувального сектора гнучкого або жорсткого носія. Мережні віруси використовують для свого розмноження можливості спеціального програмного забезпечення, яке організовує функціонування комп'ютерної мережі. Наслідки використання таких вірусів зазвичай полягають у переповненні пам'яті комп'ютера, підключеного до мережі, копіями вірусу, що призводить до неможливості роботи з інформацією, яка міститься в цій ЕОМ [44, с. 87–88].

Отже, як наголошує М. М. Коваленко, розповсюдження комп'ютерного вірусу можна здійснити у три способи: упровадженням вірусу в програми; «зараженням» завантажувального сектора носія; розповсюдженням вірусу з використанням мережного програмного забезпечення [50, с. 140].

Проте, на наш погляд, розглядана класифікація охоплює основні напрями розповсюдження комп'ютерного вірусу, але не відображає їх механічної специфіки щодо кримінального умислу злочинця.

Основним критерієм активного та пасивного ураження як способу вчинення злочину, уважаємо, виступає кримінально-правова характеристика мети вчинення злочину, яка відображає криміналістичні особливості, зокрема слідову картину способів.

Слід зауважити, що питання, пов'язані з наданням характеристики способам поширення ШПЗ, науковці розглядають по-різному, що дає змогу крізь призму наявних критеріїв класифікації звернути увагу на те, що їхній розподіл на активні та пасивні, як основні класифікаційні критерії в системі

криміналістичної характеристики, дозволить зобразити основний елементний і об'єктний склад, що безпосередньо впливає на кваліфікацію відповідного діяння та на процедуру (процес) досудового розслідування.

Водночас надання розуміння щодо розмежування між активними та пасивними способами поширення ШПЗ дає змогу концептуально усвідомити відповідне діяння, оскільки в цьому контексті слід розпочати з основного критерію такого процесу – волі особи й фактично вчиненого діяння, оскільки активним, може бути лише свідома діяльність суб'єкта злочину, у той час як пасивне поширення ШПЗ, на наш думку, також містить у собі вчинення відповідного діяння через необережність.

Тому, на наш погляд, ШПЗ варто ранжувати на такі різновиди: комп'ютерні віруси, що представляють собою програмні засоби, призначені для зміни функціональних особливостей програмного забезпечення, пошкодження операційної системи комп'ютерних програм, або знищення комп'ютерних програм; шкідливі програмні засоби (ШПЗ), призначені для нейтралізації засобів захисту інформації; програми-модифікатори, які 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 мережу «Інтернет», або в межах інформаційних носіїв. Як приклад, працівники Центрального відділення поліції Маріупольського ВП ГУНП в Донецькій області в лютому 2018 року виявили факт розповсюдження через мережу «Інтернет» шкідливого програмного засобу жителем м. Маріуполя.[1*]

[1*] Відомості у кримінальному провадженні № 12018050770000444 викладаються відповідно до вимог ст. 222 КПК України.

Зазначені способи вчинення злочинів є найбільш поширеними. Імовірно, що у зв'язку з розвитком ЕОТ та розширенням сфер її застосування з'являться й нові способи вчинення злочинів, а наявні зазнають істотних змін.

Маючи знання про способи вчинення злочинів згаданої вище категорії, можна організовувати та проводити заходи щодо їх профілактици та упередження. Однак якщо все таки злочин запобігти не вдалося, такі знання дозволять працівникам правоохоронних органів висувати версії щодо осіб, які їх вчинили, про інформованість, підготовленість таких осіб, про залишені ними сліди, що використовувалися ними як знаряддя злочину.

Саме тому злочинці використовують комп'ютер не як матеріальний предмет, що має вартість і завдяки цьому становить матеріальну цінність, а як носій чи технічну систему, що містить носій певної інформації, або ж використовують його як знаряддя доступу до операційної системи чи мережі з метою викрадення чужої інформації, спостереження за нею, унесення змін у комп'ютерні мережі. Також використовують комп'ютер для доступу до інших комп'ютерних засобів, мереж, систем знову ж таки з метою відповідного інформаційного впливу. Таке використання комп'ютера можна визнавати злочином лише в тому випадку, якщо це завдає шкоди або порушує будь-чиї права щодо володіння й розпорядження інформацією. Характерною рисою комп'ютерної злочинності є її безпосередній зв'язок із інформаційною діяльністю, що спирається на використанні зловмисниками інформаційних технологій [31, с. 133].

Учені-криміналісти узагальнюють систему способів вчинення досліджуваного злочину за допомогою шкідливих програмних засобів. Зокрема К. С. Архіпова подає таку класифікацію:

- підробка комп'ютерної інформації. Цей злочин уважають різновидом несанкціонованого доступу з тією різницею, що вчинити його може і стороння особа, і законний користувач, і розробник ІС. В останньому випадку може підроблятися вихідна інформація з метою імітування працездатності ІС і здачі замовнику свідомо несправної продукції. До цього самого виду

злочинів можна віднести підтасування результатів виборів, голосувань, крадіжки коштів тощо [2, с. 79]. Наприклад, за даними Дарницького УП ГУНП, у м. Києві в травні 2016 року невідомі особи, несанкціоновано втрутилась у роботу АТМ банку ПАТ «Укргазбанк» шляхом установлення шкідливого програмного засобу, що змінило процес обробки інформації комп'ютером, і тим самим незаконно заволоділи коштами в розмірі 306 тис. грн., що містилися в касетах диспенсера банкомату.[2*]

- Уведення до програмного забезпечення «логічних бомб» – невеликих програм, які спрацьовують із настанням певних умов і можуть призвести до часткового або повного виведення системи з ладу. Різновидом логічної бомби є «часова бомба», яка спрацьовує в певний момент часу. Ще одним способом модифікації програмного забезпечення є таємне введення до програми (чужої або своєї) «троянського коня» – команд, які дають можливість зі збереженням працездатності програми виконати додаткові, незадокументовані функції, наприклад, пересилати інформацію (зокрема паролі), що зберігаються на комп'ютері. Незважаючи на появу інших різноманітних методів захисту авторських прав, за минулий час цей приклад неодноразово унаслідувався. Так, до Суворовського РВ Одеського МУ ГУНП в Одеській області (на той час) у грудні 2014 року надійшла заява громадянина Є. про те, що невстановлена особа через веб-сайт під виглядом безкоштовних версій програми «Фотошоп» розповсюджувала ШПЗ, що належить до категорії «троянський кінь».[3*]

- Розробка й поширення комп'ютерних вірусів. Сьогодні немає жодного користувача, який би не стискався з комп'ютерними вірусами. Прояви вірусів можуть бути різноманітними – від появи на екрані точки, що світиться (так званий «італійський стрибунець»), до стирання файлів із жорсткого диску, що означає порушення цілісності ІС. Так, до СБУ у м. Тернопіль у лютому 2013 року звернувся житель цього міста К. із тим, що в нього на комп'ютері

[2*] Відомості у кримінальному провадженні № 1201610020005194 викладаються відповідно до вимог ст. 222 КПК України.

[3*] Відомості у кримінальному провадженні № 12014160490006003 викладаються відповідно до вимог ст. 222 КПК України.

несподівано з'явилося повідомлення про те, що «операційну систему windows буде заблоковано в разі несплати на користь зловмисників штрафу в розмірі 220 грн.».[4*]

- Злочинна недбалість у розробці, виготовленні й експлуатації комп'ютерної техніки та програмного забезпечення. Необережне використання комп'ютерної техніки аналогічне недбалому поводженню з будь-яким іншим видом техніки, транспорту тощо. Його особливістю є те, що безпомилкових програм не існує взагалі. Якщо помилка призвела до наслідків, які вимагають покарання винуватців, про винність розробників свідчать:

- наявність у технічному завданні вказівок на те, що в системі може виникнути ситуація, яка призвела до збою (аварії);

- можливість створення контрольного прикладу з даними, які імітують ситуацію, що призвела до збою (аварії) [2, с. 79].

Проте динаміка розвитку науково-технічного прогресу засвідчує необхідність постійного моніторингу та прогнозування розвитку способів учинення злочинів, пов'язаних із шкідливими комп'ютерними засобами, що вимагає залучення фахових знань із різних галузей наук, пов'язаних із програмуванням та інформатикою.

Фахівці у сфері інформаційних технологій виділяють найбільш розповсюджені останнім часом позиції в рейтингу найбільш активних шкідливих програм, котрі виступають засобом поширення шкідливих програмних продуктів, а саме: троянські програми, які перенаправляють жертву на інфіковані сайти; шкідливі програми, що використовують для поширення змінні носії; загрози, призначені для крадіжки конфіденційної інформації; програмне забезпечення для здійснення несанкціонованого доступу в систему [113].

Учені констатують подібні способи вчинення досліджуваного злочину ще з часів поширення управління автоматизованими системами шляхом

[4*] Відомості у кримінальному провадженні № 12013210010000552 викладаються відповідно до вимог ст. 222 КПК України.

комп’ютерних засобів. Саме тоді набув поширення такий вид злочину, як порушення автоматизованих систем, сутність якого полягає в незаконній заміні комп’ютерних даних або програм, наприклад, упровадження «логічної бомби», «троянського коня», «мережевого хробака» тощо. Це злочинні програми типу вірусів, які спричиняють порушення нормального функціонування комп’ютерної мережі. Академічним прикладом впливу такого ШПЗ стали обставини, коли інженер-програміст АвтоВАЗу просив підвищення заробітної плати за посадою, але йому відмовили. Тоді він заклав у програму, яка керує роботою головного складального конвеєра, «логічну бомбу» з метою зупинити конвеєр у певний час. Сам же програміст пішов у відпустку. Коли головний конвеєр зупинився, а інженери-програмісти не змогли його запустити, керівництво заводу викликало з відпустки «вимагача», пообіцявши підвищити заробітну плату, якщо він запустить конвеєр. Це типовий випадок навмисного комп’ютерного злочину, але тоді в СРСР (1987 р.) такого злочину ще не існувало [102, с. 8–9].

У той самий час «спам», у чистому вигляді, як метод розповсюдження ШПЗ усе менше використовується правопорушниками і не є головним інструментом їх поширення [22].

Зі зростанням обсягів безготівкових розрахунків зростає й кількість потерпілих від кібершахраїв. За інформацією НБУ, у 2017 році кількість протиправних операцій за платіжними картами українських банків зросла до 76,6 тис., хоча це й менше порівняно з 95 тис. роком раніше. Тобто на один мільйон гривень видаткових операцій із використанням платіжних карток 77 гривень припадало на незаконні операції, тоді як у 2016 році ця сума становила майже 110 гривень. Загалом у середньому на одну таку незаконну операцію в 2017 році припадало близько 2100 гривень [80, с. 5].

Водночас сучасні шкідливі програми все рідше містять оригінальні ідеї та технологічні знахідки. 2010 рік був значущим із погляду питання боротьби з новітніми загрозами з боку комп’ютерних вірусів. Також треба зосередити увагу на тому, що хакери відходять від стандартних схем заробітку

на комп'ютерних вірусах. На сьогодні більш актуальною стає модель заробітку не шляхом крадіжки номерів банківських карточок або іншої приватної інформації, а створення мережі заражених комп'ютерів (bot-net). У подальшому bot-net може бути використаний для проведення масових DDos атак. Це становить велику небезпеку для інформаційної безпеки в цілому у світі, оскільки кількість атакуючих може складатися з декількох тисяч заражених комп'ютерів, а знищити або знайти центр керування цієї bot-net мережі майже неможливо. У 2010 році створено найтехнологічніший комп'ютерний вірус Stuxnet, який своєю деструктивною діяльністю зупинив роботу АЕС у місті Бушер (Іран). Це перша реалізація вірусу, який був спрямований на ушкодження обладнання промислового класу [88, с. 73].

У цьому напрямі проявили себе й вітчизняні кіберлочинці. Так, до Дарницького управління поліції в м. Києві в березні 2015 року звернувся начальник центру Держспецзвязку К. з інформацією про виявлення створеної невідомими особами за допомогою шкідливих програмних засобів бот-мережі[5*].

Криміналістичне визначення зазначених способів вчинення злочину визначається шляхом застосування спеціалізованих програмних підходів, котрі побіжно описувались вище і серед яких найбільш оптимальним є застосування детермінованої і стохастичної моделі.

При використанні детермінованої моделі розповсюдження комп'ютерних вірусів існує стрімке зростання заражених до певної точки максимуму, після якого відбувається знижується до нуля. Стохастична модель не дає чітких значень, оскільки в ній є тільки один змінний параметр – це час, за який будуть заражені всі комп'ютери. Тож можна зробити висновок, що характер протікання епідемії піддається різким коливанням, обумовленим випадковими причинами, і в тих характерних випадках, коли епідемія розповсюджується дуже повільно або навпаки занадто швидко [123].

[5*] Відомості у кримінальному провадженні № 12015100020002295 викладаються відповідно до вимог ст. 222 КПК України.

Ураховуючи дискурсивні особливості та різноманітні тлумачення висвітлення способу вчинення досліджуваного злочину, необхідно зазначити, що в авторському розумінні спосіб вчинення злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів – це інформаційно-технічний захід, учинений шляхом застосування програмних розробок шкідливого програмного забезпечення у вигляді створення, копіювання, оптимізації самовідтворення та інкорпорації в програмне забезпечення або його розповсюдження із використанням можливостей програмних комп'ютерних мереж.

1.3. Криміналістична класифікація, обстановка та слідова картина, під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Криміналістична класифікація як науковий і практичний метод пізнання є важливим інструментом аналізу злочину, а в такому випадку виступає способом пошуку унікальних криміналістичних елементів, які чітко віддзеркалюють характер і особливості вчинення злочину, надаючи можливість чітко відмежовувати його від суміжних злочинних посягань.

Криміналістична класифікація має розгалужену структуру і є одним із засобів практичної діяльності спеціально розроблених для боротьби зі злочинністю.

Криміналістична класифікація злочинів у сфері створення, використання, розповсюдження шкідливих програмних засобів має базуватись на міждисциплінарному науково-практичному досвіді не тільки загальноюридичних (кримінальне право та кримінальний процес тощо), але й спеціальноюридичних дисциплін (криміналістика, кримінологія, судова медицина тощо), а також на ґрунті спеціальних технічних знань із галузей інформатики, програмування й інших наук. Тому злочини у сфері створення,

використання, розповсюдження шкідливих програмних засобів як комп'ютерні злочини вимагають компаративного структурного аналізу.

Комп'ютерний злочин та його класифікація у криміналістиці торкаються лише питання про використання засобів комп'ютерної техніки, переважно ЕОМ та персональних комп'ютерів, де криміналістична характеристика як головна категорія методології науки криміналістики чітко не визначена і за її елементами не розглядається [12].

Згадка про криміналістичну класифікацію комп'ютерних злочинів з'явилася тільки останнім часом. Як зазначає М. В. Салтевський, криміналістичну характеристику розглядають як фундаментальне поняття загальної теорії науки криміналістики, головний елемент методики розслідування злочинів. Криміналістична характеристика – це інформаційна модель, яка являє собою якісно-кількісний опис типових ознак конкретного виду (групи) злочинів [59], зокрема й комп'ютерних [102, с. 10].

Так само Л. В. Борисова поділяє думку М. В. Салтевського в тому, що «криміналістична характеристика злочинів – це інформаційна модель, що являє собою якісно-кількісну систему опису типових ознак конкретного виду (групи) злочинів», структура якої містить такі відомості: про предмет безпосереднього посягання; спосіб учинення злочину в його широкому розумінні; типову обстановку – «слідову картину» в її широкій інтерпретації (час, місце, злочинні наслідки); особу злочинця та потерпілого з урахуванням їх психологічних особливостей. Значення цих елементів змінюється залежно від виду злочину [103].

Л. В. Борисова також уважає, що з урахуванням масштабів міжнародних телекомунікаційних мереж вихідною інформацією про комп'ютерні злочини є: відомості про предмет замаху – характеристики комп'ютерної інформації та її носіїв, що стають об'єктами криміналістичних досліджень, коли містять в собі сліди вчиненого злочину або такого, що вчиняється, та властиві тому чи іншому способу впливу на комп'ютерну інформацію. Умови розслідування цього виду злочинів у своїй сукупності

утворюють динамічну систему, яка передусім містить у собі необхідність врахування параметра часу. Замість поняття «спосіб вчинення злочину» автор обґрунтовує поняття «спосіб впливу на комп'ютерну інформацію впродовж часу вчинення злочину», яке може бути основою для формування слідчих ситуацій, визначення напряму розслідування, типових наслідків вчинення комп'ютерного злочину (системи слідоутворення) і розкриття злочинів. Таким чином, точний час несанкціонованого доступу можна встановити слідчим оглядом комп'ютера, роздруківок чи дискет, допитом свідків із числа персоналу, який обслуговує комп'ютерну систему, з'ясовуючи час, коли кожний із них працював на комп'ютері, якщо це не зафіксовано автоматично [16, с. 47].

Криміналісти обґрунтовано вказують на те, що злочини у сфері шкідливих комп'ютерних програм мають місце лише в тому випадку коли, з одного боку, комп'ютерна інформація є предметом посягання, а з іншого, комп'ютерна інформація та засоби комп'ютерної техніки виступають у вигляді специфічного знаряддя злочину або його частини, без чого неможливе вчинення злочину [40, с. 7].

На жаль, в останні роки спостерігається нездатність держави своєчасно й ефективно реагувати на прояви кіберзлочинності. За оцінками вітчизняних і зарубіжних дослідників, вирішення проблем розкриття й розслідування злочинів цього виду є завданням більш складним, ніж завдання, що пов'язані з їх попередженням. Звертають увагу й на те, що в Україні рівень латентності комп'ютерних злочинів визначається на сьогодні в 90 %, а із залишку 10 % виявлених комп'ютерних злочинів, розкривається тільки 1 %, ще менший відсоток розкритих злочинів закінчується обвинувальним вироком суду [54, с.76].

У цьому контексті слід погодитись із дослідниками в тому, що це свідчить не лише про труднощі виявлення й розслідування злочинів певної категорії, а й про потребу практики мати відповідні науково обґрунтовані засоби протидії комп'ютерним злочинам [31, с. 130].

Непомітність або скритність є характерною рисою комп'ютерних злочинів. Складність розслідування злочинів цієї категорії значною мірою пов'язана зі складністю встановлення правоохоронними органами факту їх вчинення. Важко встановити матеріальні сліди як наслідки злочину, а це, зі свого боку, заважає своєчасному відкриттю кримінального провадження та початку здійснення досудового розслідування. Ці наслідки не завжди пов'язані з видимими матеріальними збитками, проте й у разі наявних збитків їхня причина не завжди буває зрозумілою.

Наприклад, навмисне введення в комп'ютер шкідливого вірусу часто вважають наслідком непередбаченої помилки користувача, який не зміг своєчасно знешкодити вірус, що потрапив до системи в процесі взаємодії із зовнішньою комп'ютерною мережею тощо. Іноді це відбувається випадково – у результаті перешкод на лініях зв'язку, відмови або ж збоїв обладнання, помилок людини як ланки системи, схемні або системні помилки розробників, якими є структурні, алгоритмічні помилки, можливими також є аварійні ситуації й інші впливи [82, с. 14].

Низьким є рівень розкриття комп'ютерних злочинів і внаслідок складного математичного та апаратного забезпечення комп'ютерних мереж (детальна інформація щодо статистичних показників відображена в додатку А до дисертаційної роботи).

Крім того, навіть з огляду на корисливі мотиви цих злочинів постраждалі не поспішають повідомити правоохоронні органи про виявлені ними факти. Інколи винуватців звільняють із роботи після вчинення злочину або переводять до інших структурних підрозділів того самого підприємства. Відсутність покарання за злочин закономірно тягне за собою відсутність заходів загальної профілактики [31, с. 130].

Це твердження підкріплене й тим, що Державна статистика України засвідчує надзвичайно низький рівень виявлення досліджуваного злочину (ст. 361-1 КК України). Так, у 2018 році – 134, у 2019 році – 191, у 2020 році – 114, а в 2021 році – 35 [85]. Тобто динаміка реєстрації таких злочинів

надзвичайно низька. Найбільш катастрофічною виглядає картина кількості кримінальних проваджень, у яких особам повідомлено про підозру та які направлено до суду з обвинувальним актом: у 2018 році – 81/79, у 2019 році – 152/149, у 2020 році – 81/78, а в 2021 році – 12/10. Тобто статистика кримінального переслідування за вчинення такого злочину засвідчує поодинокі випадки позитивної правозастосовної практики в боротьбі із розповсюдженням шкідливих програмних засобів в Україні останніми роками.

В. Голубєв підкреслює, що інститут криміналістичної характеристики кримінальних правопорушень, пов'язаних із використанням різноманітного шкідливого програмного та технічного компонентів містить в собі низку взаємопов'язаної та логічно скомпонованої інформації про якісні та кількісні показники, що можуть слугувати для використання інституту криміналістичного версіювання. Крім цього, від повноти та якості наданої криміналістичної характеристики залежить точність та змістовність оцінки вчиненого кримінально караного діяння загалом, а поточні дії, реалізовані слідчим (чи іншими учасниками доказового процесу), лише доповнюють уже наявну картину новою інформаційною базою [29, с. 66].

Так, наприклад, механізм учинення злочинів, пов'язаних із шкідливими програмними засобами, здебільшого прихований від потерпілих, якими є законні користувачі комп'ютерними системами та власники комп'ютерної інформації, тобто потерпілий без спеціалізованої експертизи не в змозі виявити процес злочинного посягання та його наслідки. Крім того, і факти витоку інформації можуть бути приховані за допомогою тих самих електронних засобів ще до того, як факт незаконного втручання в роботу системи буде встановлено. У розкритті факту вчинення злочину часто бувають незацікавленими посадові особи, до обов'язків яких входить забезпечення комп'ютерної безпеки.

До того ж, визнання факту несанкціонованого доступу до підвідомчої їм системи ставить під сумнів їхню професійну здатність, належну

кваліфікацію, а неспроможність задіяних заходів комп'ютерної безпеки може викликати серйозні внутрішні ускладнення, наприклад, представники банківської системи здебільшого ретельно приховують виявлені ними злочини, що вчинені з неправомірним втручанням у банківську комп'ютерну мережу, тому що це може згубно вплинути на престиж конкретного банку й призвести до втрати клієнтів. Деякі жертви комп'ютерних злочинів бояться компетентного й відкритого кримінального процесуального розслідування, тому що це може викрити непорядну і навіть незаконну практику користування комп'ютерними мережами: аморальними сайтами, незаконними комерційними операціями за допомогою інформаційних технологій тощо. Також не повідомляють про злочини з остраху на те, що страхові компанії, які покривають збитки в разі настання страхових випадків, можуть збільшити розміри внесків або навіть відмовитися від надання страхового полісу, якщо досліджувані злочини для певної організації є регулярними явищами [31, с. 130].

Отже, зазначені небажані прояви вимагають комплексної предметної криміналістичної характеристики злочинів, пов'язаних із шкідливими комп'ютерними програмами.

Загалом така характеристика є типовою для криміналістичної науки й хронологічно носить засадничий характер. Проте, на нашу думку, питання криміналістичної характеристики відповідної категорії кримінальних правопорушень потребує деталізації у світлі специфіки способів і предметного складу відповідного правопорушення.

А. В. Шмонін також зазначає, що такий процес насамперед характеризує сутність кримінальної протиправної поведінки певного виду, а тому дає змогу сформувати низку пропозицій і рекомендацій щодо алгоритмів реагування на нього, подальшої процедури досудового розслідування й пізнання такого протиправного феномена [126, с. 47], що, на нашу думку, цілком справедливо відображає сутність криміналістичної характеристики як інституту у структурі відповідної галузі, а також

виокремлює її значення для формування методики досудового розслідування загалом.

Тому, визначаючи сутність криміналістичного аналізу, варто враховувати загальновизнане визначення цього терміна, а саме як методу наукового дослідження, шляхом розкладання предмета на складники або розчленування об'єкта засобом логічної абстракції; визначення складу чого-небудь та дослідження складників.

Учинення комп'ютерних злочинів – це завжди сукупність складних дій, що мають кримінально караний та некримінальний характер. Така злочинна діяльність породжує сукупність слідів, створюючи слідову картину, у якій матеріальні та ідеальні сліди розосереджені в часі й в просторі та не мають єдиного матеріального й ідеального носія. Крім того, ці сліди, як зауважують науковці, можуть відбивати різні боки дій різних індивідів [31, с. 133].

Проте складники криміналістичної характеристики злочинів, пов'язаних із шкідливим програмним забезпеченням, мають бути досліджені окремо, із урахуванням специфічних ознак злочину.

У загальному розумінні під криміналістичною характеристикою вчені визначають систему узагальнених даних про типові сліди, способи здійснення й механізми злочину, особу злочинця та інші істотні риси, властивості та особливості злочину й обставинах, які йому сприяють. А також усе те, що допомагає оптимізації розслідування й практичному застосуванню засобів, прийомів і методів криміналістики в розкритті і розслідуванні цього злочину. До цієї системи зараховують основні дані про: способи здійснення злочину й механізм протиправного діяння; способи приховання незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), системи і комп'ютерні мережі; предметом учинення протиправного діяння; обставини й місце вчинення злочину; сліди злочину; предмет злочинного посягання; осіб, які вчинили незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж тощо [29, с. 69].

Саме тому вирішення проблем розкриття й розслідування «комп'ютерних злочинів» тісно пов'язане із здійсненням поглибленого криміналістичного аналізу фактів, знарядь, слідів правопорушень у сфері використання комп'ютерних технологій. Такий аналіз, як зазначають В. К. Гора та В. А. Колесник, дає змогу всебічно вивчити різноманітні прояви цього явища, установити ознаки, що свідчать як про факт вчинення чи підготовки до вчинення злочину, так і про причетність до цього конкретних винуватців та роль кожного у вчиненні злочину [31, с. 135].

Отже, криміналістична характеристика кримінальних правопорушень у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів являє собою результати аналізу складників, які відображають характерні особливості такого злочину, відмежовуючи його від суміжних злочинів шляхом критеріальних ознак. Такі критеріальні ознаки і формують структуру криміналістичної характеристики досліджуваного злочину, до них зараховують: спосіб вчинення злочину; слідова картина; особа злочинця; предмет безпосереднього посягання.

Відповідно виникає необхідність розгорнутого аналізу зазначених структурних компонентів криміналістичної характеристики злочинів із використанням шкідливих програмних засобів. Успішне розкриття та розслідування злочинів значною мірою залежить від якості та кількості криміналістично значущої інформації, її доступності для особи, яка проводить розслідування.

Під такою інформацією насамперед розуміють фактичні дані або відомості, які знаходяться в обумовленому та безпосередньому зв'язку з подією злочину й обставинами його вчинення. Такими фактичними даними при встановленні істини з кримінального провадження відповідно до положень кримінального процесуального закону визнають докази.

У цивілізованому суспільстві фактичні дані, які встановлюють та окреслюють таке явище матеріального світу як злочин, називають доказами.

Порядок визначення доказів, їх фіксації та використання регламентований КПК України.

Відповідно до диспозиції статті 84 КПК України доказами в кримінальному провадженні є фактичні дані, отримані в передбаченому цим Кодексом порядку, на підставі яких слідчий, прокурор, слідчий суддя і суд установлюють наявність чи відсутність фактів та обставин, що мають значення для кримінального провадження та підлягають доказуванню. Процесуальними джерелами доказів є показання, речові докази, документи, висновки експертів. Розкриваючи більш докладно зміст одного з джерел доказів, законодавець у ст. 99 КПК України надає роз'яснення, що речовими доказами можуть бути також і документи, якщо вони містять у собі зафіксовані за допомогою письмових знаків, звуку, зображення тощо відомості, які можуть бути використані як доказ факту чи обставин, що встановлюють під час кримінального провадження [35, с. 61–62].

Необхідно також звернути увагу й на те, що джерелами криміналістично значущої інформації може бути увімкнений комп'ютер, мобільний телефон або інші електронні пристрої. Специфікою здобуття інформації, що має значення в кримінальному провадженні, є те, що така інформація зберігається в увімкнених електронних пристроях, а їхній огляд необхідно проводити у режимі реального часу.

На початковому етапів огляду необхідно насамперед запобігти можливості будь-кому з присутніх заблокувати комп'ютер, вимкнути його з мережі або зашифрувати інформацію, що в ньому зберігається.

Специфікою такої інформації в увімкненій комп'ютерній техніці є її нестійкість та енергозалежність, тобто її самознищення в разі від'єднання від джерела живлення. Тому від працівника правоохоронного органу вимагають її правильне та швидке збереження, адже в іншому випадку інформація буде втрачена [119].

Сучасна комп’ютерна техніка містить у собі значні масиви оперативної пам’яті та може вміщати від 2 до 64 Гб., а в серверній комп’ютерній техніці і того більше.

В останній час значного поширення набуло використання для обробки та зберігання інформації так званих «хмарних» сховищ, специфікою якого є збереження та обробка інформації на значному віддалені від комп’ютера користувача. Доступ до інформації, що зберігається в таких сховищах, регулює законодавство тієї країни, де знаходиться фізичний носій інформації.

В оперативній пам’яті може знаходитися така інформація: інформація про виконувані у комп’ютері процеси; інформація про виконувані сервіси; системна інформація; дані про користувачів, які перебувають в системі; інформація про про відкриті порти; кеш ARP (протоколу визначення адреси); кеш DNS (доменної системи імен); інформація про автоматично завантажені додатки; незбереженні документи; бінарні процеси і сервіси, зокрема й шкідливі програмні засоби, які зберігають тільки в оперативній пам’яті [34, с. 25–26]. Із метою збереження такої «енергозалежної» інформації та недопущення її необережного чи умисного знищення чи пошкодження необхідно: обмежити присутніх осіб від доступу до комп’ютерного обладнання; виявити, описати та сфотографувати кожен пристрій, у якому на момент його огляду міститься «енергозалежна» інформація; за участі спеціаліста вжити заходів щодо унеможливлення її зміни або знищення, провести її фіксацію.

1.4. Характеристика осіб, які створюють, використовують, розповсюджують або збувають шкідливі програмні чи технічні засоби

Закон про кримінальну відповідальність України (КК України) визначає особу, яка вчиняє злочин, зокрема й комп’ютерний, як суб’єкт злочину. Суб’єкт злочину – це один із чотирьох обов’язкових структурних елементів, що утворюють склад злочину.

Суб’єктом злочину визнають фізичну, осудну особу, яка до вчинення злочину досягла віку кримінальної відповідальності [64, с. 74]. Ці положення знайшли своє закріплення в ч. 1 ст. 18 КК України [65, с. 9].

Відповідно до наукового вчення про такий елемент складу злочину, як суб’єкт злочину, останній характеризують за такими ознаками: 1) суб’єктом злочину можуть бути тільки фізичні особи; 2) особа, що вчинила злочин, повинна бути осудною; 3) кримінальна відповідальність настає при досягненні визначеного законом віку.

Частиною 2 ст. 18 КК України визначено поняття спеціального суб’єкта злочину, яким визнають особу, яка, окрім ознак загального суб’єкта, має ще й інші, притаманні лише їй ознаки, що безпосередньо вказані у диспозиції статті.

Аналіз суб’єктивних ознак злочинів у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку, що більшість злочинів XVI передбачає загального суб’єкта, тобто фізичну, осудну особу, яка досягла 16-річного віку, і лише злочини, передбачені статтями 362 та 363 КК України, містять у собі дані, що вказують на спеціального суб’єкта.

У першому випадку це особа, яка має право доступу до інформації, що є предметом злочину, у зв’язку з виконанням нею трудових, службових обов’язків, або наданого власником інформації дозволу, і зловживає цим правом, використовуючи надані їй можливості для вчинення заборонених дій. У другому – особа, яка відповідає за експлуатацію ЕОМ, АС, комп’ютерних мереж чи мереж електрозв’язку [129].

Спираючись на кримінально-правову теорію, кримінологією було розроблено поняття особи злочинця.

Особа злочинця – це сукупність істотних і стійких соціальних властивостей і ознак, соціально значущих біопсихологічних особливостей індивіда, які, об’єктивно реалізуючись у конкретному вчиненому злочині, надають вчиненому діянню характеру суспільної небезпечності, а винній у

ньому особі – властивості суспільної небезпечності, у зв'язку з чим її і притягається до відповідальності, передбаченої кримінальним законом [36, с. 37].

Кримінологічна категорія – особа злочинця, що також містить низку елементів, тобто певну кількість різних ознак, властивостей, рис, особливостей. Назвемо декілька з них: 1) соціально-демографічні ознаки; 2) особистісно-рольові властивості; 3) соціально-психологічні якості; 4) риси правової і моральної свідомості; 5) кримінально-правові ознаки особи злочинця [112].

Із наведених вище ознак цікавою для нашого дослідження є лише перша – соціально-демографічна, оскільки вона містить такі показники особистості, як стать, вік, освіта, соціальний стан, рід занять, фахова приналежність, сімейний стан, рівень матеріальної забезпеченості тощо.

Специфіка комп'ютерної злочинності на сучасному етапі розвитку інформаційно-технічного прогресу все більше засвідчує «фаховість» злочинців, котрі вчиняють подібні злочини. Це передусім пояснюється, з одного боку, загальною доступністю до мереж комп'ютерної інформації, зокрема до програмного забезпечення, а з іншого – наявністю необхідних професійних знань і навичок, які дозволяють користуватися програмним забезпеченням, розроблювати його й змінювати. Саме тому «фаховість» злочинності у комп'ютерній сфері ускладнює процеси розслідування подібних злочинів, протидії їм та профілактики комп'ютерної злочинності.

У літературі таких спеціалістів стали назвати хакерами (злочинці, серед яких існує спеціалізація). Хакерів, які займаються крадіжкою інформації з комп'ютерів, комп'ютерних мереж, називають крекерами, а осіб, які незаконно використовують зі злочинною метою мережі телефонних компаній – фрикерами. Хакерів, які спеціалізуються на крадіжці грошових коштів із використанням комп'ютерних операцій, називають кіберзлодіями, а осіб, що спеціалізуються на збиранні та торгівлі піратськими програмними засобами, – торгашами або піратами [102, с. 14].

Відомо, що особу злочинця досліджують різні науки. Кримінологічні дослідження обмежені передусім тими особливостями людини, які необхідні для використання з метою кримінальної профілактики, попередження злочинів. Характеризуючи особу комп'ютерного злочинця, необхідно виокремити основну ознаку, а саме: в електронну злочинність втягнуто широке коло осіб, від висококваліфікованих фахівців до дилетантів. Правопорушники приходять з усіх сфер життя і мають різний рівень підготовки [7].

Основне місце в криміналістичній характеристиці злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів займає суб'єкт, а також типологія осіб, які вчиняють кримінальні правопорушення. Такому аналізу підлягають стать, вік, приналежність, професія, фізичні, психічні на інші якості правопорушника. Для криміналістики першочерговими є професійні якості такої особи, які проявляються у способах, методах та прийомах, а також дослідження індивідуальних особливостей вчинення кримінального правопорушення та залишення слідів злочинної діяльності.

За своїми особливостями всіх правопорушників такого виду злочинів необхідно розмежовувати на дві категорії суб'єктів, які стосувалися протиправних дій: невстановлені особи та відомі особи.

Невстановлені особи – це ті особи, які вчинили кримінальні правопорушення, однак їхні особи працівниками правоохоронних органів невстановлені. Інформація про таких осіб має лише загальний характер, в основному лише за залишеними на місці скоєння злочину слідами. Так, разом із матеріальними слідами злочинів у деяких випадках залишаються й ідеальні сліди – у пам'яті свідків, потерпілих, інших осіб. За таких обставинах необхідно використовувати статистичні відомості щодо всіх правопорушників цієї категорії злочинів, які раніше стосувалися чи стосуються кіберзлочинності.

Для встановлення таких правопорушників може бути використана інформація у сфері інформаційних технологій уже відомих осіб та інформація, використана у сприянні в установленні невідомих осіб та розслідуванні кримінального провадження.

До відомих осіб, що здійснили протиправну дію, зараховують осіб, установлених працівниками правоохоронними органами. Діяльність таких осіб знаходиться в полі зору з метою встановлення їхніх зв'язків з іншими особами та їхньої поведінки. Або ж якщо протиправна діяльність такої особи припинена, а особа затримана за підозрою в учиненні злочину.

Особлива увага повинна приділятися вивченню портрета суб'єкта такого злочину, установленню психологічного контакту з метою встановлення обставин вчинення злочину, виявлення можливих співучасників та встановлення істини в обставинах, що склалися.

Під час досудового розслідування основне завдання слідчого в такій ситуації – створення сприятливих умов безконфліктного ведення спілкування, а також спонукання такої особи до зізнання в злочині та каяття. На цьому у своїх дослідженнях наголошують Г. М. Бірюков, Ю. М. Кривонос, М. І. Шилан. Автори доводять, що «характеризуючи осіб, які скоюють комп'ютерні злочини, необхідно вказати на їх основну ознаку, а вона полягає в тому, що такі злочини вчиняє широкий діапазон осіб – від висококваліфікованих спеціалістів до дилетантів» [124, с. 39].

Визначаючи інтелектуальний рівень таких осіб, фахівці надають таку інформацію: 77 % злочинців, які вчинили комп'ютерний злочин, мали середній рівень інтелектуального розвитку, 21 % – вищий від середнього, 2 % – нижчий від середнього. Водночас 20 % мали середню освіту, 20 % –середню спеціальну і 40 % – вищу [10, с. 369].

Для протидії цьому новому різновиду злочинів необхідним є вивчення цієї проблеми й дослідження криміналістичних та психологічних рис кіберзлочинців. Вітчизняні та зарубіжні дослідження дають змогу

намалювати портрет типового комп'ютерного злодія, тобто відповідний профіль такого соціального типу [6].

Розглядаючи гендерні особливості осіб, що вчинили такі злочини, слід наголосити, що участь жінок та чоловіків у кіберзлочинах має пропорційну співвіднесеність із переважуванням у бік чоловічої статі. Також за критерієм агресивності у своїх діях перевага залишається на боці чоловічої статі. Жіноча кіберзлочинність чіткіше спланована, більш продумана, складніша у розслідуванні та сприйнятті.

Накопичення інформації про зміст і сутність соціологічної моделі правопорушника, що вчиняє злочини «комп'ютерної» спрямованості, є важливим елементом методики його пошуку, оскільки чим більше характерних рис та інформації про нього буде накопичено, тим більш ефективно можна буде здійснювати розшукових заходи [7]. У цьому контексті важливість надання характеристики портрету такого правопорушника, його соціотипу, основних характерних рис поведінки та інших суттєвих елементів відповідного криміналістичного вчення є недооціненою, а відповідно, на нашу думку, визначення відповідного комплексу соціо-психологічних характеристики є надзвичайно важливим для подальшого розвиту досліджень щодо формування методики досудового розслідування відповідних злочинних діянь.

П. Д. Біленчук акцентує увагу на тому, що соціологічні дослідження надають безцінну інформацію в галузі аналізу особи злочинця, що вчиняє злочини у сфері шкідливих програмних чи технічних засобів. Ці результати насамперед полягають у тому, що лише 7 % таких кримінально караних діянь реально вчиняють професійні програмісти, а загалом, відповідна особа, без приналежності до професійної діяльності, характеризується як активна по житті, нетипова в мисленні та поведінці, обережна молода особистість будь-якої статі [7]. На нашу думку, такі результати суттєво ускладнюють надання характеристики психологічного портрету злочинця, оскільки без приналежності до конкретної соціальної категорії, суспільної верстви

населення, визначення її конкретних стійких рис, охарактеризувати конкретну особу, що має намір вчиняти кримінально карані діяння від традиційного для 21 сторіччя психотипу молодої особи 14–25 років майже неможливо.

Водночас С. О. Прутяний звертає увагу, що так звана «професійна» комп'ютерна злочинність насамперед характеризована конкретністю цілей такого правопорушника, що має на меті здобуття певної вигоди (матеріальної чи будь-якої іншої) [97], що, на нашу думку, за умови набуття таких характеристик складатиме суттєву загрозу для суспільства та потребуватиме оперативного втручання органів охорони правопорядку в їх протиправну діяльність, що буде значно ефективним за умови їх належної професійної підготовленості.

Зазвичай комп'ютерний злочинець – це творча особа з нестандартним мисленням, професіонал у своїй справі, який виявляє інтерес до роботи комп'ютерних програм. Здебільшого це раніше не судимі злочинці-одиночки, хоча вже з'явилися організовані угруповання, учасниками яких можуть бути керівник підприємства з комерційних структур, державні службовці, які беруть участь у фінансових аферах. Група може складатися з осіб, які знаходяться на різних континентах [102, с. 15].

Характеризуючи особу, яка здійснила незаконне втручання необхідно зазначити, що в ці злочинні дії втягнуто широке коло осіб – від професіоналів до дилетантів. Правопорушники мають різний соціальний статус та рівень освіти. Л. П. Паламарчук уважає, що залежно від рівня професійної підготовки і соціального стану комп'ютерних злочинців доцільно розподілити на такі групи: хакери; шпигуни; терористи; корисливі злочинці; вандали; психічно хворі особи, які страждають від нового психічного захворювання – інформаційної хвороби або комп'ютерної фобії. Така класифікація досить повно відображає мотиви здійснення незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж [86, с. 104].

Борисова Л. В. та Волкова О. Г., надаючи психологічну характеристику особі-правопорушнику у сфері комп'ютерних злочинів, надають йому рис, що найбільше притаманні в розрізі психолого-психіатричних особливостей. Так, діяльність такої особи характеризується як протидія інтелектуальних здібностей і знань особи технічним можливостям і алгоритмам роботи електронно-обчислювальної техніки [17, с. 56]. На нашу думку, питання, пов'язані з наданням психологічної характеристики відповідним особам, слід розглядати в криміналістичному аспекті.

Викладена класифікація не є сталою та остаточною. З розвитком інформаційних технологій її можна видозмінювати, доповнювати, розширювати, із чимось погоджуватися, щось може втратити свою актуальність. Так, наприклад, осіб, які вчиняють комп'ютерний злочин, за класифікацією Ю. В. Гавриліна, характеризують за доступом до ЕОТ. Тобто за такою класифікацією більшу увагу приділяють внутрішнім користувачам програмного забезпечення та обслуговуючого персоналу, а також зовнішнім користувачам, які мають стосунок до роботи ЕОТ, іншу класифікацію осіб не розглядають. Тож поза увагою науковця залишаються програмісти-самоучки, хакери-професіонали, психічно-неврівноважені особи тощо. Певною мірою можна погодитися з автором у тому, що на долю саме внутрішніх правопорушників, як свідчить статистика США, припадає близько 80 % всіх кіберзлочинів [55, с. 4].

Такі дослідники, як Л. В. Борисова та О. Г. Волкова, уважають, що сучасне розширення інформаційного простору створює нові можливості для організованої злочинності: стає можливим використання Інтернет не тільки для правопорушень, але й для створення злочинних груп, що може втілитися у перехід наявних груп хакерів і кракерів, які координують свої операції, до формування кримінальних організацій, членам яких не має потреби зустрічатися або знаходитися в одній державі; відбувається поєднання організованої злочинної діяльності із суттєвими елементами неорганізованої злочинності; суб'єктивні дані особи, яка вчиняє злочин

у сфері інформаційних технологій, її психічні та психологічні характеристики визначають спосіб кримінального впливу на інформаційні системи, інформацію та програмне забезпечення, як результат послідовних у просторі та часі дій цієї особи [17, с. 57].

П. Д. Біленчук, Б. В. Романюк та В. С. Цимбалюк звертають увагу на те, що класифікаційні критерії розподілу осіб-злочинців, що вчиняють такі діяння у сфері електронно-обчислювальних машин, у дослідженнях учених різняться. При цьому, автори обґрунтовують власний розподіл, котрий видофікує останніх на три групи: ті, хто порушує правила використання електронно-обчислювальних машин, при цьому завдаючи шкоди їхній стабільній і нормальній діяльності (що може бути вчинене, зокрема, через необережність); підготовлені професіонали, метою яких є здійснення злочинної діяльності у сфері функціонування електронно-обчислювальних машин; психологічно нестійкі програмісти, котрі є належно підготовленими з технічно-інтелектуального боку, проте їхньою метою не є отримання виходи від такої діяльності, оскільки основною характеристикою їх морально-психологічного стану є егоїзм, самовпевненість та бажання самоствердитись, що й рухає ними під час створення, розповсюдження шкідливих програмних засобів [5]. Таким чином, усі зазначені психолого-психіатричні елементи повинні бути досліджені в установленому порядку, оскільки мають значення в доказовому процесі та безпосередньо впливають на кваліфікацію конкретно вчиненого суспільно-небезпечного діяння.

За наявності подібних фактів у процесі розслідування призначають судово-психіатричну експертизу на предмет установлення осудності злочинця на час учинення ним злочинних дій [122].

Н.С. Козак також наголошує на тому, що для вдосконалення характеристики особи комп’ютерного злочинця необхідно також ураховувати дослідження окремих науковців, що розглядають можливі схеми дій певних груп злочинців з урахуванням технології обробки інформації, особливостей

предметної сфери: хакер-одинак; об'єднана хакерська група; підприємство-конкурент; представники різних структур відомчого, міжвідомчого рівня, спецслужби різних держав [51, с. 10–11].

За результатами дослідження кримінальних справ, проведених І. М. Горбаньовим, більшість злочинців матеріально забезпечені; 74% позитивно характеризувалися за місцем проживання, роботи або навчання; 68% мали постійне місце роботи або навчання, 87% мали вищу або незавершену вищу освіту; 97% злочинців раніше не притягувалися до кримінальної відповідальності. Професійна діяльність 64% злочинців пов'язана зі сферою комп'ютерних технологій, 43% були приватними підприємцями. Близько 30% злочинців були посадовцями державних або приватних підприємств, установ, організацій, 9% правопорушників були студентами різних навчальних закладів, 18% складали безробітні чи особи, що працювали без оформлення відповідних документів [32].

Класифікація осіб, що вчиняють кримінальні правопорушення в указаній сфері може значно спростити їх пошук, у випадку активного використання відповідних знань у методиці досудового розслідування відповідної категорії кримінальних правопорушень, однак в умовах стрімкого інформаційно-технічного прогресу та суттєво високого рівня опанування молоддю комп'ютерних технологій це питання потребує більш глибокого вивчення.

Дослідники неодноразово обґрунтовували позицію про криміналістичну характеристику особи, що професійно здійснює кримінальні правопорушення щодо створення, розповсюдження або збуту шкідливих програмних чи технічних засобів і надавали їй такі характеристики: стійкість наявних знань щодо комп'ютерної техніки та інтернет-освіти; замкнутість та небагатослівність, що формує умови для накопичення знань, їх обмірковування та подальшого формування асоціального типу поведінки особи, що, зі свого боку, породжує ігнорування меж індивідуального простору; ігнорування законів і звичаїв суспільства,

надмірна та завзята потреба в демонстрації власної «могутності»; бажання отримати наживу, застосовуючи власні знання тощо. Так, відповідні особи, розраховуючи на свою «всемогутність» в кібер-просторі та користуючись неповним розумінням користувачів інноваційних технологій щодо тонкощів безпеки їх використання, свідомо й цілеспрямовано впливають на нормальний порядок функціонування електронно-обчислювальних машин і пристроїв із власних мотивів корисливого чи некорисливого характеру.

П. Д. Біленчук, аналізуючи комп'ютерну злочинність в Україні на ранньому етапі її становлення, зазначав, що тісний взаємний зв'язок комп'ютерної злочинності та низького соціального рівня в України спричиняє такі обставини й умови, що штовхають на вчинення цих діянь, зокрема й тих представників соціально не захищених верств населення, які в арсеналі здібностей мають знання щодо комп'ютерної техніки [8, с. 16]. Ми вважаємо, що оцінюючи відповідну позицію в ретроспективі, важливим буде підкреслити еволюцію криміналістичної характеристики особи-злочинця, що трансформувався з особи, котра «розуміється» на комп'ютерній техніці, у професійно підготовленого, мотивованого та морально деформованого комп'ютерного злочинця, що використовує інформаційні технології з метою вчинення кримінальних правопорушень та, крім цього, створює з метою розповсюдження таке програмне забезпечення, що може зашкодити нормальній і стабільній діяльності, наприклад, системи інформаційної безпеки банку.

Отже, особа злочинця, що вчинює злочини, пов'язані з використанням шкідливих програмних засобів, являє собою осудну особу, котра має навички володіння комп'ютерними технологіями, свідомо застосовуючи їх з метою замаху на функціональність програмного забезпечення інших комп'ютерних засобів або мереж зв'язку. Тобто, на наш погляд, злочинець вчиняє замах на інформаційні технологічні засоби, а більш конкретно – на інформацію.

Підтримуємо позицію тих учених, які вважають, що мотив і мета вчинення злочину тісно пов'язані із соціально-психологічною та

криміналістичною характеристиками особи злочинця. Вони належать до групи окремих суб'єктивних чинників, що здійснюють вплив на вибір засобів та прийомів досягнення злочинних цілей, визначають характер протиправних дій правопорушника, спосіб учинення злочину, який містить у собі певний комплекс вольових дій людини і є головним аспектом будь-якого злочинного посягання.

У деяких випадках вони є необхідною ознакою суб'єктивної сторони умисних кіберзлочинів. Це такі злочини у сфері інформаційних технологій, за яких правопорушник свідомо здійснював протиправні дії, покладаючи за основу корисний мотив, досягаючи мети викрадення, знищення чи модифікації інформації шляхом несанкціонованого доступу до ЕОТ та впливу на неї за допомогою ЕОТ.

У всіх випадках при розслідуванні злочинів цієї категорії такі елементи необхідно встановлювати у співвідношенні ступеня небезпечності вчиненого протиправного діяння. Аналізуючи вітчизняну та світову практику розкриття та розслідування кіберзлочинів, усі мотиви та мету можна викласти в такій послідовності:

- корисливі – на долю яких припадає близько 66 % злочинів (скоюють переважно професіонали вищого рівня);

- політичні – 17 % шпигування, злочини спрямовані на підрив фінансової та фінансово-кредитної політики, підрив ринкових відносин, учиняють ті самі професіонали;

- зацікавленість – 7 % (студенти та професійні програмісти);

- хуліганські наміри – 5 % (хакери та їх різновиди у поєднанні з професіоналами вищого рівня);

- помста – 5 % (професійні злочинці та психічно неврівноважені особи) [56, с. 5–10].

Звісно, ми підтримуємо думку тих криміналістів, які дотримуються поданої класифікації, однак, хотіли б дещо доповнити та уточнити за окремими аспектами.

Аналізуючи корисливі наміри правопорушників, слід зазначити, що це найбільш розповсюджена і найскладніша категорія. До її числа входять кілька протиправних напрямів.

Так, до сфери інформаційних технологій віднесені діяння, що пов'язані з розповсюдженням шкідливих програмних засобів. Різновид таких злочинів становить близько 20 % від всіх кіберзлочинів, де основою були корисливі наміри. Окрему категорію становлять злочини, які базувалися на безвідплатному користуванні програмним забезпеченням – 7,1 % або подальшому продажі такого програмного забезпечення чи іншої інформації –5,7 %, захист або ліцензійні умови користування яких були подолані за допомогою ШПЗ.

Деяка кількість злочинців мають на меті долучитися до ЕОТ через канали мережі «Інтернет», несанкціоновано та приховано встановивши ШПЗ, із метою добування криптовалюти (майнінг) та уникнення оплати, за користування технічними ресурсами ЕОТ.

Аналіз конкретних кримінальних проваджень та справ, пов'язаних із ШПЗ, та теоретичні обґрунтування науковців цього напряму діяльності дають змогу виокремити найбільш актуальні злочинні цілі, що ставить перед собою криміналітет: фальсифікація платіжних документів; розкрадання як безготівкових, так і готівкових коштів; легалізація злочинних прибутків шляхом переводу викрадених безготівкових коштів у криптовалюту; незаконне отримання кредитів; продаж конфіденційної інформації, закритих баз даних; несанкціоноване використання технічних ресурсів ЕОТ; шифрування інформації на комп'ютері потерпілої особи метою отримання викупу за її розшифрування тощо.

Осіб, які вчинили протиправні діяння такої категорії, на нашу думку, необхідно класифікувати за характером виконуваної ними об'єктивної сторони злочину: особи, що створюють ШПЗ, зокрема їх модифікації наявних програмних засобів, та особи, що використовують або здійснюють їх розповсюдження.

До того ж, таких осіб необхідно розмежувати й за цілями злочинного посягання, а саме: корисливі правопорушники; бешкетники (вандали, особи, що не мають визначеної мети); зломщики (так звані «хакери»); диверсанти (терористи).

Зважаючи на військово-політичну ситуацію в країні, окремо слід вказати на самостійну групу таких правопорушників, як «диверсанти» (терористи). Основною характеризувальною ознакою цієї групи є направленість дій правопорушників на досягнення певних цілей, а саме: підрив економічної безпеки й боєздатності країни, обумовлення дій, направлених на окремі комп'ютерні системи й інформацію, що має низку специфічних властивостей.

Отже, відомості про особу злочинця та предмет безпосереднього замаху у структурі криміналістичної характеристики створення, використання, розповсюдження або збуту шкідливих програмних засобів засвідчують специфічність, нетиповість і вузькопрофільність таких злочинних проявів. У структурі криміналістичної характеристики особою злочинця виступає осудна кваліфікована за інформаційно-програмним фахом або професійно підготовлена особа чи група осіб, яка використовує програмне комп'ютерне забезпечення з метою шкідливого впливу на програмні засоби персональних комп'ютерів, серверів або мережевого зв'язку. У цьому процесі безпосереднім предметом злочинного посягання виступають шкідливі програмні засоби, котрими є системне програмне забезпечення, програмні блоки та окремі програми, створені спеціально 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.

Висновки до розділу 1

Поняття та криміналістична характеристика злочину у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів, розглядані в цьому розділі, засвідчують наявність певних закономірностей, серед яких доцільно узагальнити такі.

На підставі криміналістичного аналізу нормативних джерел та концепцій учених розроблене поняття злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів. Результатом цього аналізу є авторське визначення злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів як винне кримінально каране діяння, учинене одноосібно або групою осіб із метою нанесення негативних наслідків іншому комп'ютерному програмному забезпеченню для отримання матеріальної вигоди чи іншого нематеріального задоволення, яке нанесло матеріальні чи інші нематеріальні збитки охоронюваним законом інтересам шляхом порушення функцій програмного та інформаційно-комунікативного забезпечення комп'ютерного обладнання, а також комунікативних мереж і електронних накопичувальних пристроїв.

Отримало подальший розвиток криміналістичне визначення поняття способу вчинення злочину, яке дещо відмінне від кримінально-правового визначення способу злочину як ознаки об'єктивної сторони складу злочину.

Криміналістична класифікація злочинів у сфері створення, використання, розповсюдження шкідливих програмних засобів базована на міждисциплінарному науково-практичному досвіді не тільки загальноюридичних, але й спеціальноюридичних дисциплін, а також на базі спеціальних технічних знань із галузей інформатики, програмування й інших наук. Тому злочини у сфері створення, використання, розповсюдження шкідливих програмних засобів як комп'ютерні злочини вимагають компаративного структурного аналізу. Структуру криміналістичної характеристики досліджуваного злочину складають спосіб учинення

злочину, слідова картина, особа злочинця та предмет безпосереднього посягання.

На підставі аналізу кримінально-правового поняття суб'єкта злочину та кримінологічного поняття особи злочинця сформовано криміналістичний «портрет» правопорушника, що вчиняє злочини, пов'язані із використанням шкідливих програмних засобів. Установлено, що він являє собою фізичну осудну особу, яка досягла шістнадцятирічного віку, має навички володіння комп'ютерними технологіями, свідомо застосовуючи їх із метою замаху на функціональність програмного забезпечення інших комп'ютерних засобів або мереж зв'язку.

РОЗДІЛ 2. ОРГАНІЗАЦІЯ РОЗСЛІДУВАННЯ СТВОРЕННЯ, ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

2.1. Аналіз первинної інформації та висунення версій на початковому етапі розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Як уже зазначалось у нашому дослідженні, типові слідчі ситуації зумовлюють висування типових слідчих версій та напрямів їх перевірки.

У криміналістичній науці під слідчою версією розуміють обґрунтоване припущення про факт, явище або їх групу, що мають або можуть мати значення для кримінального провадження, пояснюють характер кримінального правопорушення в цілому або його окремі обставини. Версії поділяють на такі види:

– загальні версії – припущення, що охоплюють розслідуване кримінальне правопорушення в цілому;

– окремі версії – припущення, що пояснюють окремі обставини кримінального правопорушення [117, с. 140].

Слідчі версії – це можливі пояснення розслідуваної події та її обставин, які використовують із метою встановлення істини в провадженні. Саме криміналістичне версіювання вможливлює як планування досудового розслідування, так і формування основних методик його здійснення за окремими видами кримінальних правопорушень. Лише чітке, об’єктивно оцінене й змістовно сформульоване уявлення про вчинення кримінального правопорушення – дотримання певного стандарту розуміння протиправної поведінки та вжиття відповідних заходів реагування, використання форм дослідження цих фактів можуть призвести до ефективного вирішення всіх завдань досудового розслідування.

Наведена інформація дає підстави стверджувати, що процес здійснення досудового розслідування створення, розповсюдження та збуту шкідливих програмних засобів полягає в необхідності широкого застосування всього інструментарію слідчого щодо роботи із зібраною доказовою інформацією, що, зі свого боку, є основою для застосування криміналістичного версіювання, висунення гіпотез і припущень не лише щодо факту вчинення протиправної дії, а й щодо способів, засобів, форм і методів провадження такого злочинного умислу, а також розкриття й надання повної характеристики всіх елементів складу кримінального правопорушення.

Спираючись на сучасні криміналістичні вчення, проаналізовані попередньо, варто звернути увагу на те, що версіювання має на меті висунення найбільш вірогідних припущень щодо загального розуміння вчиненого злочинного посягання, а також щодо конкретних елементів цього комплексного явища, що характеризуються окремо, а вже після підтвердження/спростування, узагальнюються в загальному контексті розслідуваного кримінального правопорушення.

Так, А. Ф. Волобуєв на підтвердження обумовленості великої та малої посилок (саме так у його працях сформульовані окреслені нами попередньо «загальний» і «фрагментарний» масштаби версіювання) наводить такий приклад: практичний слідчий досвід говорить, що коли на голові та інших частинах трупа, витягнутого з петлі, виявляються синці та подряпини, то не виключено, що має місце не самогубство, а вбивство, замасковане під самогубство. Такі справи неодноразово бували в минулому, і слідчий знає про них за результатами узагальнення слідчої практики (Велика посилка). Іншим фактом буде наявність на голові та інших частинах трупа, вилученого з петлі, синці та подряпини. Цей факт встановлюється слідчим у результаті огляду місця події і трупа. (Мала посилка) [23, с. 277]. Таким чином, у слідчого наявне загальне уявлення про механізм учинення кримінального правопорушення, основні типовості та стандартизовані попередньо механізми його реалізації, що дає змогу в загальному розумінні версіювати

відповідне кримінальне правопорушення. З іншого ж боку, інформація безпосередньо зібрана з комп'ютерного чи іншого технічного засобу, за допомогою якого було вчинено відповідне кримінальне правопорушення, допит самого ймовірного злочинця та огляд місця вчинення (наприклад, квартири чи домоволодіння) є «фрагментарним» рівнем і дає змогу версіювати злочинну поведінку в межах досудового розслідування конкретно вчиненого діяння.

У цьому контексті, на нашу думку, найбільш логічним є визначення криміналістичного версіювання як одного з найбільш важливих етапів у механізмі методики досудового розслідування відповідної категорії кримінальних правопорушень. На цьому, зокрема, акцентує увагу І. М. Горбаньов, який визначає слідчі версії та процес версіювання загалом як припущення, що ґрунтуються на зібраній у конкретному розслідуванні ситуації та слугують джерелом подальших припущень [33, с. 51], що, на наш погляд, цілком відповідає сучасним реаліям, а також необхідності й потребі формування й розвитку відповідного інституту не лише на загальному рівні, а й у контексті розслідування відповідного кримінального правопорушення.

Слід підкреслити, що ми також дотримуємося цієї позиції, оскільки питання, пов'язані з версіюванням, по-перше, тим чи іншим чином ґрунтуються на вже сформованих уявленнях слідчого про такий тип і вид злочинності, і, по-друге, зумовлюють підстави для накопичення сформованого уявлення на підставі здобутих під час проведення тієї чи іншої слідчої (розшукової) дії доказових фактів (інформації).

Аналогічно, під час аналізу вказаного інституту низка дослідників підкреслює, що з-поміж декількох видів версіювання: слідчого та оперативно-розшукового, слідче версіювання здебільшого є логічним продовженням оперативного версіювання, що, зі свого боку, базується не лише на фактах учиненого правопорушення, а й такого діяння, що готується.

У розрізі досудового розслідування кримінальних правопорушень, пов'язаних зі створенням, розповсюдженням чи збутом шкідливих

програмних засобів, криміналістичне версіювання є комбінацією декількох видів цього інституту, оскільки синергетично поєднуються як версії щодо формату, способів і методів створення самого шкідливого програмного (технічного) засобу, так і класичні формати версіювання, що розуміють під собою ті обставини, події та факти, які спонукали особу до вчинення кримінального правопорушення, обстановку, у якому воно вчинялось, а також інші позакібернетичні елементи.

М. В. Салтевський неодноразово підкреслював, що версіювання як інститут криміналістики є фундаментом планування, що починається з будування загальних версій, спрямованих на максимально повне виявлення обставин, які підлягають доказуванню [102, с. 24].

На думку В. В. Воротнікова, В. В. Умінського, О. І. Пінчука, застосовуючи наукову аналогію в указаному контексті, можна також виокремити форму припущень і версіювання за тяжкістю наслідків. Так, використовувані зловмисниками методи несанкціонованого одержання інформації можна розподілити на безпечні (сканування портів, спроби встановлення з'єднань тощо), потенційно небезпечні (отримання доступу до вмісту підсистем збереження даних, спроби підбору паролів тощо), небезпечні (одержання доступу з високим рівнем повноважень, модифікація відомостей в ІТС, копіювання системної та прикладної інформації, створення власних даних тощо) і надзвичайно небезпечні (знищення інформації, блокування доступу легальних користувачів до ІТС тощо) [25, с. 84–92].

У спеціальній літературі детально аналізують технології виявлення комп'ютерних атак і захисту від комп'ютерних вірусів, ознаки комп'ютерних атак, джерела інформації про комп'ютерні атаки, класифікації комп'ютерних атак, чинники, пов'язані з виявленням комп'ютерних атак, методологія реагування на інциденти, спостереження, детальні схеми дослідження операційних систем тощо. За допомогою фахівця може аналізуватися робота програм, зміст текстових файлів, баз даних, результати роботи антивірусних і тестових програм, комп'ютерне обладнання [52, с. 90–93].

Для виявлення інформаційних слідів (слідів комп'ютерних атак) необхідно вжити таких заходів:

- контроль цілісності програм, файлів даних та інших інформаційних ресурсів, що підлягають захисту. При цьому рекомендують проводити перегляд непередбачених змін каталогів і файлів, порівнювати поточні характеристики файлів і каталогів із збереженими еталонними значеннями. Виявлення підміни чи зміни файлів операційної системи, іншого програмного забезпечення може бути здійснено за допомогою утилітів, що входять до операційної системи;

- аналіз діяльності користувачів і процесів, а також мережного трафіка в комп'ютерній мережі, над якою ведеться контроль. Передбачено аналіз журналів реєстрації операційної системи, систем управління базами даних, прикладних і мережних систем; аналіз механізмів повідомлень від підсистем моніторингу систем (зокрема операційних) та мережі; аналіз виконаних процесів для виявлення непередбаченої поведінки;

- контроль фізичних форм нападу на елементи інформаційної системи. При цьому можливі такі дії: виявлення невідомих і несанкціонованих пристроїв (наприклад, модемів), підключених до системи, перегляд слідів несанкціонованого доступу до фізичних ресурсів. Для виявлення наявності модемів у мережі можливе використання спеціальних програм, що проводять дистанційну перевірку великої кількості вузлів за допомогою різних методів;

- оцінку дій адміністраторів із перевірки попередніх інцидентів. Для цього пропонують проводити аналіз звітів користувачів і даних із зовнішніх джерел про стан системи, процесів, програм, мережних подій.

Під час аналізу інформації у файлах реєстрації фахівці радять відстежувати випадки реєстрації, які за часом і місцем відрізняють від звичайних випадків; спостерігати за невдалими спробами реєстрації; звертати увагу на спроби відкрити файли (чи одержати доступ до ресурсів будь-яким іншим способом) користувачем, який не має відповідних повноважень; стежити за спробами змінити статус при авторизації або загальні привілеї,

рівень файлового захисту визначених ключових файлів (якщо файл має атрибут «тільки для читання» і може бути змінений лише автором або адміністратором системи) [52].

Як уже зазначалося, безпосереднє виявлення ознак злочину слідчим або прокурором можливе при розслідуванні кримінальних проваджень про інші злочини.

Як свідчить слідча практика, оптимальна програма роботи з виявлення комп'ютерних злочинів охоплює такі заходи: 1) огляд місця події з обов'язковим оглядом електронно-обчислювальних машин (далі – ЕОМ), сервера мережі ЕОМ, машинних носіїв інформації і комп'ютерної інформації; 2) опитування персоналу потерпілої організації (особливо фахівців, що мають стосунок до комп'ютерної техніки); 3) попереднє вивчення і дослідження документів та предметів (програмно-технічних засобів); 4) надання доручень фахівцям про проведення в необхідних випадках документальних перевірок і лабораторних досліджень; 5) якщо є підозра щодо конкретного суб'єкта, то в деяких випадках можливе отримання пояснення в нього, а також в інших осіб [5; 20, с. 43].

Специфіка виявлення несанкціонованого втручання в роботу ЕОМ зумовлена застосуванням спеціальних технічних засобів, програмно-технологічних прийомів огляду і фіксації інформації, використанням спеціальних інженерних рішень, обов'язковим залученням фахівця оперативно-технічного підрозділу, тісною взаємодією з операторами зв'язку і провайдерами [5].

З позиції криміналістики потрібно детально розглянути особливості огляду місця події й використання спеціальних знань у формі попередніх досліджень документів і програмно-технічних засобів. Огляд місця події дає змогу встановити низку важливих обставин, а деякі аспекти тактики проведення цієї слідчої дії вже висвітлені в дослідженнях науковців [89].

Огляд місця події вимагає ретельної підготовки й вирішення низки організаційних і технічних питань:

1. Забезпечення участі фахівців. Їх знання потрібні для оперативного аналізу інформації і кваліфікованого її вилучення із засобів комп'ютерної техніки. Профіль потрібного фахівця визначають залежно від завдань огляду з урахуванням первинних даних про характер злочину.

2. Залучення понятих, що розуміються на комп'ютерній техніці хоча б на рівні користувача.

3. Підготовка обладнання, що буде використано для огляду, перевезення й зберігання вилученої інформації. Основні труднощі при проведенні огляду за такою категорією злочинів полягають у тому, що інформаційні сліди можуть бути виявлені й вилучені тільки при використанні спеціального апаратного й програмного забезпечення [53].

З метою отримання доброякісних доказів слідчий комплект апаратного й програмного забезпечення повинен бути надійним, універсальним та з добре налаштованою платформою, що містить достатню кількість компонентів, які дозволяють підключатися до різноманітних зовнішніх пристроїв.

У слідчій практиці прийоми пошуку, аналізу й вилучення комп'ютерної інформації при проведенні огляду місця події групують залежно від етапів його проведення, зокрема: підготовчого, робочого та завершального [101].

На підготовчому етапі важливими є такі дії:

1. У керівника підрозділу, особи, відповідальної за експлуатацію комп'ютерної техніки, або іншого співробітника організації необхідно провести допит, з'ясувати обставини щодо наявності засобів охоронної сигналізації і забезпечення безпеки комп'ютерної інформації, спеціальних засобів у комп'ютері для знищення інформації, пароля для доступу до інформації, мережі комп'ютерів тощо.

2. Вилучити й вивчити документацію, пов'язану із забезпеченням безпеки комп'ютерної інформації в цій організації. Вилучити протоколи й резервні копії вінчестера (якщо такі є).

3. Ознайомити фахівця із зазначеними документами, виробити з ним план проведення огляду [53].

На робочому етапі передбачають такі дії:

1. Швидкими діями запобігти знищенню інформації на ЕОМ.

2. Виключити можливість особам, що беруть участь в огляді, контактувати з устаткуванням, користуватися мобільними телефонами й іншими засобами зв'язку, виставити охорону, а будь-яке увімкнення або вимкнення програм проводити тільки під наглядом фахівця, оскільки цими діями можуть бути внесені зміни у функціонування комп'ютерних програм і зміст інформаційних слідів.

3. Виявити традиційні сліди.

4. При огляді окремого комп'ютера необхідно зафіксувати його розташування і розташування периферійного обладнання, їх опис і робочі параметри, тип і особливості з'єднання між собою всіх пристроїв.

5. Провести аналіз даних про важливі файли й каталоги, аналіз журналів реєстрації, аналіз мережевого трафіка, аналіз повідомлень, аналіз процесів, сервісів і портів, виявлення несанкціонованих пристроїв, інвентаризацію кінцевих пристроїв, контроль модемів, аналіз зовнішніх джерел про поведінку системи.

Під час огляду комп'ютерної інформації і її вилучення необхідно звернути увагу на такі моменти:

1. Після початку огляду потрібно скопіювати всю інформацію, що перебуває у відповідних журналах і каталогах, на жорстких дисках, дискетах тощо.

2. Усі маніпуляції із засобами комп'ютерної техніки повинні бути фіксовані в протоколі. Необхідно відзначати кожну дію, оскільки під час перегляду журналів системи або оцінок часу файлів зафіксовані дані дозволять пізніше ідентифікувати системні зміни, що були викликані діями слідчого.

Для уникнення можливих негативних наслідків вироблено певні правила дій на завершальній стадії огляду: вилучення, упакування, опечатування підконтрольних об’єктів і, за необхідності, транспортування до місця зберігання. На цьому етапі оформляють протокол огляду, до якого додають плани і схеми приміщення, яке оглядають, і розташування комп’ютерного обладнання. Усіх необхідних рекомендацій з огляду вилучення, транспортування комп’ютерної техніки і носіїв комп’ютерної інформації, складання протоколу огляду потрібно дотримуватися для того, щоб вилучена інформація була достовірною, зберегти її доказове значення, щоб у суді не виникло сумнівів щодо недбалості проведених слідчих дій [53].

Отже, розслідування злочинів щодо створення та використання шкідливих програмних засобів повинно бути побудоване на власному уявленні слідчого про події, які містять склад зазначеного злочину. У той же час зазначені версії створюють із метою перевірки достовірності шляхом збору доказів та їх об’єктивного підтвердження. Цей етап початкової стадії розслідування забезпечено особливостями тактики проведення окремих слідчих дій.

Криміналістична характеристика злочинів, пов’язаних із шкідливими програмними засобами є сукупністю найбільш характерної криміналістично значущої взаємопов’язаної інформації про ознаки й властивості такого роду злочинів, здатної слугувати підставою для висування версій про подію злочину і особистість злочинця, що дає змогу правильно оцінити ситуації, що виникають у процесі розкриття й розслідування. Основне цільове призначення криміналістичної характеристики програмно-комп’ютерних злочинів полягає в тому, що вона може слугувати інформаційною базою для висування версій у справах цієї категорії [29, с. 66].

Водночас В. П. Лавров та М. Г. Шурухнов визначають криміналістичну характеристику злочину як віддзеркалення системи криміналістичних рис, властивостей, ознак злочину в об’єктивній дійсності. Зазначена характеристика, на думку вчених, містить дані про типові способи вчинення і

приховання злочинів, механізм злочинного посягання, сліди, обставини, у яких готувалася й відбувалася злочинна подія, предмети злочинного посягання, риси особистостей злочинця і потерпілого, а також про обставини, що сприяли скоєнню злочинів. Роль таких даних полягає в тому, що вони дозволяють побачити зв'язок між різними обставинами вчинення злочину і в умовах браку вихідної інформації висунути обґрунтовані версії, обрати оптимальний шлях щодо встановлення осіб, які скоїли злочин.

Для побудови версій важливу роль відіграє вивчення матеріалів кримінального провадження. Зазначений процес передбачає аналіз даних, що містяться в протоколах слідчих (розшукових) дій, що, зі свого боку, дає змогу виявити суперечності, прогалини в обставинах розслідуваної події або ж навпаки виявити певні спільні риси чи характеристики. Визначальну роль у вивченні матеріалів провадження відіграє аналіз результатів таких слідчих (розшукових) дій, як обшук та огляд місця події. Їх вивчення може мати практичне значення для висування версій про осіб, що його вчинили, та механізм вчиненого злочину.

Побудову версій слідчий проводить безперервно, у мірі надходження до нього інформації. Навіть на початковому етапі розслідування, оглядаючи місце події, члени СОГ зобов'язані обмінюватися інформацією, що дає змогу висувати для тактичного відпрацювання нові версії або ж відмовитися від раніше висунутих.

Важливу роль у побудові версій відведено орієнтувальній інформації отриманій від фахівця. Одержанні дані слідчі використовують для висунення розшукових версій та визначення шляхів пошуку злочинця за гарячими слідами, виявлення носіїв комп'ютерних слідів, які знаходяться поза місцем події, з'ясування механізму та обставин вчиненого злочину тощо [92].

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, які

умовно можна розподілити на дві групи залежно від змісту вихідної інформації [115].

Г. М. Гапотченко звертає увагу на те, що типовий алгоритм проведення слідчих (розшукових) дій у вказаному виді кримінальних правопорушень містить такі елементи: огляд місця події із залученням відповідних спеціалістів; особисті обшуки затриманих, їхніх робочих місць та місць проживання; аудіо-, відеоконтроль особи, накладення арешту на кореспонденцію, огляд і виїмка кореспонденції, зняття інформації з транспортних телекомунікаційних мереж, зняття інформації з електронних інформаційних систем, як таких, що можуть надати істотної допомоги в розкритті зазначеного різновиду злочинів; допит підозрюваних; огляд документів, що засвідчують затриману особу; тимчасове вилучення документів тощо [26].

Отже, на нашу думку, особливу увагу слід звернути на необхідність залучення до проведення всіх необхідних слідчих (розшукових) дій) осіб, що володіють відповідними знаннями, а також порушувати питання про використання спеціальних знань (експертних) навіть щодо питань, у яких слідчий орієнтується особисто в силу свого інтелектуального розвитку.

Під час проведення обшуків, оглядів і затримань (оглядів під час затримань) особливу увагу слід звернути на елементи електронно-обчислювальної техніки, навіть на ті, що, здавалося б, не стосуються досудового розслідування, проте можуть складати об’єкт і предмет експертного дослідження. Також вартим уваги є те, що такі слідчі (розшукові) дії, як зняття інформації з електронних інформаційних систем, є окремими видами й можуть проводитися незалежно від факту проведення обшуку та в поєднанні з іншими діями.

Ключовим у питанні формування належного алгоритму дій слідчого є необхідність щоетапного аналізу всієї зібраної доказової інформації, порівняння більш важливої та менш важливої інформації, узагальнення, групування та долучення до матеріалів кримінального провадження.

Крім цього, дослідники формують уявлення про алгоритм дій слідчого відносно кримінального правопорушення, що було вчинене за незрозумілих обставин, і, на їхню думку, це потребує залучення додаткових ресурсів і використання інших методів, а саме: допиту осіб, указаних у початковій інформації; огляду місця події із залученням відповідних спеціалістів; тимчасового вилучення комп'ютерної техніки, предметів, матеріалів і документів, що мають значення в цьому розслідуванні; 4) порушення клопотань перед слідчим суддею про залучення до кримінального провадження відповідної експертної установи або експерта для проведення комп'ютерно-технічних, бухгалтерських та інших експертиз тощо [48]. Водночас, на наш погляд, відповідний перелік не є повним і потребує доповнення такими класичними елементами, як: опитування потерпілих від правопорушення осіб щодо їх підозри суб'єкта вчинення протиправних дій відносно них; вилучення облікової кадрової документації щодо осіб, яких було нещодавно прийнято/звільнено з роботи у відповідній установі, на підприємстві в організації, стабільний порядок інформаційної системи якого/якої було порушено у спосіб застосування шкідливого програмного (технічного) засобу тощо.

Розгляданий вище матеріал дає змогу узагальнити уявлення про інститут версіювання в досудовому розслідуванні відповідної категорії кримінальних правопорушень, його взаємозв'язок із програмуванням дій слідчого на початковому та подальших етапах здійснення досудового розслідування, оскільки від якості та повноти зібраних попередньо даних залежить подальша обґрунтованість висунутої підозри загалом і результат спроби притягнення до кримінальної відповідальності зокрема.

Отже, аналіз первинної інформації та висунення версій на початковому етапі розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів являє собою результати аналізу складників, які відображають характерні особливості такого злочину,

відмежовуючи його від суміжних злочинів шляхом критеріальних ознак та вимагає компаративного структурного аналізу.

2.2. Типові слідчі ситуації та програми дій слідчого на початковому етапі розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Типові слідчі ситуації та їх фактурний та елементний склад насамперед базований на наявності чи відсутності тих чи інших версій щодо вчинення конкретного кримінального правопорушення, зміст і сутність яких розкрито в попередньому підрозділі. Водночас існування на підставі усталеної практики низки типових слідчих ситуацій, що характеризують вчинення відповідного правопорушення та можуть (теоретично) слугувати основою для розробки найбільш ефективних алгоритмів дій слідчого в разі їх виявлення, є дієвим інструментом досягнення мети кримінального провадження та його завдань.

Така обстановка отримала в криміналістиці загальну назву слідчої ситуації. Іншими словами, це наявна в певний момент реальність, в умовах якої діє слідчий. Слідча ситуація – це визначена на певний проміжок часу реальність, в умовах якої відбувається діяльність із розслідування кримінальних правопорушень [117, с. 132].

Розслідування будь-яких злочинів, учинених умисно або з необережності, базоване на характерних для слідчого процесу етапах, що зумовлені типовими формами вчинення злочинів, їх слідовою картиною та іншими чинниками, які дозволяють узагальнювати за подібністю криміналістичні слідчі ситуації. Це, безумовно, має прямий стосунок і до досліджуваного злочину. Проте в цьому процесі необхідно враховувати особливості вчинення комп’ютерних злочинів, коли новітні технології й технічно-інформаційний прогрес щохвилинно у світі вдосконалюють форми і методи вчинення злочинних посягань за допомогою шкідливих програмних засобів.

На погляд М. І. Скригонюка, слідча ситуація як поєднання певних умов та обставин на тому чи іншому етапі розслідування злочину і слідча версія як аргументований, мотивований здогад суб'єкта криміналістичної діяльності щодо встановлення невідомих чинників, за яких він був учинений, що мають значення для відповідної кримінальної справи, – поняття досить взаємообумовлені. Це означає, що за певних чинників слідчі ситуації й слідчі версії в кримінальній справі про будь-який злочин мають типові форми. Кожній із таких форм відповідає певна конкретна, найбільш вірогідна група слідчих ситуацій і версій [105, с. 6].

Слід підкреслити, що, наприклад, І. В. Європіна наявність та характер орієнтувальної й доказової інформації, що знаходиться в розпорядженні слідчого на початковому етапі розслідування, а також механізму злочину й умов виникнення слідів на місці його вчинення зараховує до об'єктивних чинників, які, зі свого боку, виступають суттєвими елементами в механізмі програмування дій слідчого й однаково важливо розглядаються поруч із інтенсивністю впливу сторонніх сил на ці чинники, а також інших форм організаційно-правового забезпечення досудового розслідування кримінальних правопорушень, що докорінно не впливають на процес самого досудового розслідування, але фундаментально формують певний інструментарій у вказаному контексті [42, с. 162].

Крім цього, рівень знань та практичного досвіду роботи слідчого з комп'ютерними злочинами, уміння оперативно реагувати та приймати рішення в нестандартних і небезпечних для суспільного порядку ситуаціях, а також рівень професійної майстерності щодо спрямування ходу й інтенсивності процесу розслідування без помилок і значних недопрацювань, що призводять до визнання в подальшому доказів недопустимими, зараховують до суб'єктивних чинників [42, с. 162]. Серед суб'єктивних чинників, на нашу думку, чільне місце посідає обізнаність слідчого щодо комп'ютерних технологій загалом і механізму учинення відповідного кримінального правопорушення зокрема. Це зумовить, зі свого боку,

ефективне досудове розслідування, що в поєднанні з психологічною стійкістю та незалежністю від заходів протидії ефективному досудовому розслідуванню уможливить досягнення поставлених КПК України та всім процесуальним законодавством цілей і завдань.

Систематизація типових слідчих ситуацій у розслідуванні злочинів, пов'язаних зі шкідливими комп'ютерними програмами, полягає в тому, що під час розслідування злочинів, що вчинені з використанням комп'ютерів, систем та іншої електронної техніки, слідчий має справу як з традиційними для криміналістики, так і з нетрадиційними слідами злочинної діяльності та речовими доказами. Саме тому за справами цієї категорії під час провадження окремих слідчих дій доводиться шукати, фіксувати й досліджувати специфічні об'єкти криміналістичних досліджень, якими є комп'ютерні об'єкти та комп'ютерна інформація [14].

Надана різноманітність підходів характеризує універсалізацію підходів, які стосуються трактування розуміння типових слідчих ситуацій. Проте сфера створення й використання шкідливих програмних засобів у цьому контексті має свою специфіку.

На підставі викладеного під слідчою ситуацією в криміналістиці слід розуміти визначену на певний проміжок часу реальність, обумовлену чинниками об'єктивного й суб'єктивного характеру, в умовах якої відбувається діяльність із розслідування кримінальних правопорушень. Стосовно злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку можна зауважити, що слідчі ситуації, що виникають при їх розслідуванні, мають свої особливості.

Вивчаючи кримінальні провадження у сфері комп'ютерних злочинів, необхідно зазначити, що саме вони слугують основою для виявлення типових слідчих ситуацій.

При розгляді справ у сфері інформаційних технологій, особливо на початковому етапі розслідування, такий комплекс дає змогу слідчому

більш ефективно розробити ті чи інші рекомендації щодо застосування криміналістичної методики розслідування таких злочинів [75, с. 88]. У цьому контексті характерними виявляються особливості типових слідчих ситуацій при розслідуванні незаконного відтворення та розповсюдження шкідливих комп'ютерних програм.

Матеріали слідчої практики засвідчують систематичні однотипні злочинні посягання, що виявляються у методичних підходах вчинення досліджуваного злочину. За таких умов для кожного з етапів розслідування виділяли типові слідчі ситуації, які є відправним місцем для визначення програми подальшого розслідування. Інформація, яка їх формує, є основою для висунення типових версій, а також для розробки програми їх перевірки. Що стосується повторності (типовості) слідчих ситуацій, то це явище пояснюється проявом типовості в ознаках злочину, якщо розглядати їх у криміналістичному аспекті. Будь-яку ситуацію при штучному звільненні від низки чинників, властивих тільки конкретному кримінальному провадженню, умовно можна охарактеризувати як типову. А отже, для її вирішення може бути розроблений типовий алгоритм слідчих дій та інших заходів. Учені розробили алгоритм, за якого, перше ніж перейти до типових слідчих ситуацій, що складаються на початковому етапі розслідування незаконного відтворення і розповсюдження шкідливих комп'ютерних програм, слід визначити приблизний перелік відомостей, які й формують слідчу ситуацію [33, с. 41].

І. Горбаньов зазначає, що серед плюралізму чинників, що можуть виступати детермінантами тієї чи іншої слідчої ситуації можна виокремити такі специфічні відомості: інформацію про безпосередній момент створення шкідливого програмного забезпечення чи факту початку його розповсюдження; уточнення способів, форм і методів, що були використані під час створення такого програмного забезпечення чи технічного засобу. Такі відомості є єдиним «технологічним» ланцюжком і тому їх слід розглядати в комплексі [33, с. 42]. Саме тому слідчий зобов'язаний постійно тримати

слідчу ситуацію під контролем і бути готовим будь-якої миті належним чином відреагувати на виникнення в ній випадкового чинника без шкоди для загального напряму розслідування. Водночас, на нашу думку, узагальнення відповідних типових слідчих ситуацій і їх складників дають підстави стверджувати, що найбільш характерні риси та особливості досудового розслідування відповідного кола кримінально протиправних посягань мають бути враховані на початковому етапі досудового розслідування й досліджені слідчим першопочатково.

В. О. Куркін акцентує увагу на тому, що під час формування й узагальнення інформації про типові криміналістичні ситуації в розслідуванні організованої злочинності в комп'ютерній сфері важливим є системне й планомірне здійснення контролю за ходом досудового розслідування, оскільки кожна проведена слідча (розшукова) дія може докорінно змінити хід досудового розслідування й вплинути на те, що до його проведення буде залучено додаткових осіб і фігурантів [69, с. 22–24]. Тобто, розслідуючи феномен, пов'язаний зі створенням, розповсюдженням і збутом шкідливих програмних засобів (приладів), одним із найбільш пріоритетних завдань є системне контролювання здобутої інформації від усіх суб'єктів, задіяних до процесу досудового розслідування, оскільки з урахуванням специфіки категорії кримінального правопорушення таких осіб може бути досить багато.

І. В. Європіна зауважує, що зміст усякої слідчої ситуації детермінують здебільшого чинники, які: стосуються розслідуваного злочину та визначають ступінь достовірності й повноту інформаційної моделі діяння на момент оцінки слідчої ситуації; характеризують безпосередньо систему розслідування, його процесуальний, тактичний стан, психологічну налаштованість учасників досудового розслідування тощо; належать до зовнішнього середовища, у якому проводиться розслідування, та визначають так звану слідчу обстановку [42, с. 162–163]. Відповідно, указані елементи типової слідчої ситуації, на нашу думку, суттєво впливають на хід

досудового розслідування та можуть його або загальмувати, або прискорити, розкривши додаткові елементи об'єктивних чи суб'єктивних складників кримінального правопорушення, пов'язаного зі створенням, розповсюдженням чи збутом шкідливих програмних (технічних) засобів.

Отже, формування основних архітектурних ознак певної слідчої ситуації, апелюючи відповідною (достовірною, повною та цілковито доповненою) інформацією, дозволить спрямувати досудове розслідування в правильному напрямі, забезпечити швидкість та його повноту, дотриматись усіх процесуальних процедур і криміналістичних методик.

Змістовною у цьому питанні є позиція В. О. Голубєва, зокрема:

1. Установлено незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, є сліди, є підозрюваний, і він дає правдиві свідчення.

2. Установлено незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, є наявні сліди, що прямо вказують на конкретного підозрюваного, але він заперечує свою причетність до вчинення злочину.

3. Установлено незаконне втручання в роботу ЕОМ (комп'ютерів), систем і комп'ютерних мереж, відомі особи, які за своїм службовим становищем несуть за це відповідальність, але характер їх особистої вини, а також обставини доступу невстановлені.

4. Установлено факт незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж, скоїти який і скористатися результатами якого могли тільки особи з певного кола (за своїм становищем, професійними навичками і знаннями) або відомі особи (фірми, організації), зацікавлені в отриманні цієї інформації [29, с. 126].

Такий підхід автора найбільш науково обґрунтовано відображає сутність порушеної проблематики. В основу типових слідчих ситуацій

покладено знання вихідної інформації про злочин, що, на думку О. І. Мотлях, є основоположним при розслідуванні такої категорії злочинів [75].

Белкін Р. С., аналізуючи питання, пов’язані з формуванням криміналістичних методик, уважає, що найбільш обґрунтовано відображає сутність порушеної проблематики ситуація, за якої в основу криміналістичного планування покладено знання вихідної інформації про злочин, що є основоположним при розслідуванні вказаної категорії злочинів [3, с. 126]. Відповідно, такий підхід у досудовому розслідуванні злочинів, пов’язаних із незаконним створенням, розповсюдженням і збутом шкідливих програмних (технічних) засобів є фундаментальним. Таке уявлення, що базується на певній «типовості» слідчих ситуацій, системно доповнюється нескінченним колом обставин і чинників, що аналізуються слідчим й іншими суб’єктами, залученими до проведення досудового розслідування, а саме тому не лише широта кола здобутої інформації відіграє ключову роль у визначенні ситуаційного підходу до вирішення криміналістичних і процесуальних завдань, а й зміст, і обсяг опрацьованого матеріалу, його практична застосовність в кожному конкретному досудовому розслідуванні.

Таким чином, чим ширшим буде коло отриманої про протиправні діяння особи інформації та більш якісно й масштабно пропрацьовані всі версії й моделі його вчинення, тим швидшим, результативнішим і ефективнішим буде процес притягнення до відповідальності та поновлення порушених прав і свобод людини і громадянина.

Разом із тим дослідники акцентують суттєву увагу не лише на об’єктивних чинниках, що стосуються досудового розслідування відповідної категорії кримінальних правопорушень, а й зосереджуються також на результативних моделях дослідження інформації про особу злочинця. Тож чим ширшим буде коло показів, наданих імовірним зловмисником, тим простішим буде з’ясування (шляхом логіко-семантичного й системно-структурного підходів в аналізі) найбільш сумнівних фрагментів відповідно наданої інформації й пропрацювання відповідних типових версій.

Інші дослідники пропонують класифікацію типових слідчих ситуацій, пов’язаних зі створенням і розповсюдженням шкідливих програмних засобів за іншими підходами.

На наш погляд, така класифікація базована на формах виявлення пошкодженої шкідливими програмами інформації, проте поза увагою вченого залишилися такий аспект, як дані, які надають підстави підозрювати, які допомагають в оперативно-розшуковій діяльності.

У такому контексті важливим моментом є виявлення раніше невідомої інформації шляхом логічного зіставлення з’ясованих на поточній стадії досудового розслідування фактів щодо первинної інформації про вчинене протиправне діяння. Це дозволить установити низку форм і способів учинення кримінального правопорушення, деталізувати окремі обставини його реалізації, а також на підставі зібраної й аналізованої інформації буде можливим проведення додаткових допитів й опитувань як зловмисника, так і потерпілого чи очевидців, що в подальшому шляхом накопичення інформації також указуватиме на правильний напрям досудового розслідування.

У дослідженні О. А. Самойленко наведено класифікацію типових слідчих ситуацій при розслідуванні такого злочину, побудованих за особливостями кримінального провадження щодо особи-злочинця, а саме:

1) відносно працівника фінансово-господарської установи на підставі матеріалів внутрішньої планової або позапланової перевірки;

2) відносно особи, яка безпосередньо не має трудових стосунків із установою-жертвою, на підставі матеріалів оперативно-розшукової перевірки повідомлення про злочин керівництва відповідної установи;

3) відносно особи, затриманої під час вчинення викрадення з використанням комп’ютерних технологій на місці вчинення такого злочину [104, с. 425].

Також типові слідчі ситуації, що стосуються створення, використання, розповсюдження або збуту шкідливих програмних засобів, І. О. Мотлях розглядає в контексті низки прикладів, що свідчать про типові слідчі

обставини, які мають бути досліджені слідчим на початковому етапі. Так, указана як приклад обстановка, що свідчить про факт протиправного втручання в стабільний обіг інформації на банківському підприємстві, проте на початковому етапі досудового розслідування відсутня інформація про коло ймовірно причетних до відповідного діяння осіб, а також форми, способи, методи та засоби, що були застосовані зловмисниками під час такого несанкціонованого проникнення чи пошкодження окремих елементів інформаційних ресурсів [75, с. 93–95]. На нашу думку, незалежно від віднесення цієї ситуації до категорії типових однозначно необхідним є проведення огляду місця події, вилучення серверного обладнання, на яке було здійснено таку протиправну атаку, а також опитування всіх працівників відповідної установи на предмет можливого витоку інформації про уразливі місця в системі безпеки. Не зайвим буде також огляд інформації про новопризначених працівників цієї банківської установи, а також тих, хто звільнився чи кого звільнили за останні півроку. Це забезпечить можливість отримання первинної картини інформації до моменту, поки не буде проведено комп'ютерно-технічну експертизу і не встановлено спосіб зараження того чи іншого інформаційно-аналітичного ланцюга відповідної електронно-інформаційної системи, характер і сутність пошкоджень (що дасть змогу встановити тип і вид шкідливого програмного чи технічного засобу, що був застосований), а також місцезнаходження ймовірного зловмисника чи будь-які його ідентифікувальні дані.

Окрім цього, суттєвим є те, що в одних випадках слідчі ситуації, обумовлюють розшук уже встановленого злочинця, в інших – збирання додаткових фактичних даних, необхідних для затримання вже розшуканого злочинця або для оголошення особі про підозру. На завершальному етапі розслідування вони мають своїм головним призначенням доведення вини підозрюваного в усіх викритих злочинах чи епізодах злочинної діяльності за допомогою якісно й повно зібраних даних доказового характеру. Однією

з таких ситуацій є, наприклад, визнання обвинуваченим своєї вини за наявності переконливих і достатніх доказів [42, с. 168].

Л. П. Паламарчук наголошує, що до проведення огляду місця події необхідно залучати спеціалістів, поняті також повинні мати вичерпні знання з комп'ютерної техніки та програмного забезпечення. Огляду місця події повинен передувати інструктаж слідчо-оперативної групи, консультації спеціалістів, підготовка комп'ютерної техніки та технічних засобів огляду місця події. Особливу увагу необхідно приділяти ретельному процесуальному та криміналістичним способам фіксації ходу і результатів цієї слідчої дії [87, с. 68]. Ми вважаємо, що комп'ютерна обізнаність усіх учасників огляду має критично важливе значення, оскільки, оглядаючи приміщення, де знаходиться комп'ютерна техніка, із якої було вчинено в тій чи іншій формі розповсюдження шкідливого програмного засобу, чи безпосередньо розроблено проєкт шкідливого технічного засобу, або ж виявивши сам шкідливих технічний засіб, усі учасники відповідної слідчої (розшукової) дії мають розуміти, що відбувається, як називаються ті чи інші елементи комп'ютерного обладнання, які дії вчинятиме спеціаліст-криміналісти чи it-фахівець під час проведення огляду ти чи інших елементів предметів, що мають значення для досудового розслідування відповідного кримінального правопорушення.

Зокрема, у ході такої діяльності обов'язковим, на нашу думку, під час виявлення того чи іншого місця, що має причетність до протиправної діяльності у сфері розповсюдження шкідливих програмних (технічних) засобів, їх збуту чи розроблення, є вилучення тих елементів комп'ютерних приладів і засобів, що безпосередньо мають доказове значення: власне комп'ютер (системний блок, суміжне обладнання), елементи мережевого обладнання та різноманітних форм кінцевого обладнання, складників і частин транспортних телекомунікаційних мереж. Також увагу заслуговують механізми вводу інформації (клавіатури, комп'ютерні миші) та все подібне,

що може містити біологічні сліди власника чи користувача того чи іншого технічного пристрою.

Важливим аспектом є попередня підготовка до проведення будь-яких слідчих (розшукових) дій, що має містити залучення спеціалістів із відповідної галузі комп'ютерних (інших спеціальних) знань, підготовку комп'ютерної техніки та різноманітного обладнання, що використовуватимуть у процесі проведення слідчої дії, та інші ймовірно допоміжні чинники й елементи. Уся наведена інформація стає доступною за умови розвинення широкого уявлення про відповідну категорію протиправної діяльності, практику досудового розслідування відповідних кримінальних правопорушень та на основі виведених критеріїв «типовості» тих чи інших слідчих ситуацій у відповідних процесах.

Отже, у **нашому авторському** розумінні слідчі версії при розслідуванні злочинів, пов'язаних зі створенням, використанням, розповсюдженням або збутом шкідливих програмних засобів представляють собою такі характеристики:

- виявлено шкідливе втручання комп'ютерних програм у роботу операційної системи комп'ютера/комп'ютерів або окремих комп'ютерних програм, сліди такого втручання, підозрюваних, які дають правдиві свідчення;

- виявлено шкідливе втручання комп'ютерних програм у роботу операційної системи комп'ютера/комп'ютерів або окремих комп'ютерних програм, сліди такого втручання, підозрюваних, які заперечують свою вину та можливість доказу їх вини ускладнена за умов неможливості перевірити їх свідчення;

- установлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремих комп'ютерних програм, є сліди вчинення злочину, установлено осіб, які можуть бути зацікавлені у здійсненні шкідливого комп'ютерного впливу та відповідальні за комп'ютерну безпеку, але обставини вчинення злочину невстановлено;

- установлено факт шкідливого програмного впливу на операційні системи комп'ютера/комп'ютерів або окремих комп'ютерних програм, сліди відсутні, не встановлено осіб, підозрюваних в учиненні такого злочину.

У процесі розв'язання типових слідчих ситуацій, котрі складаються при розслідуванні досліджуваного злочину, формуються напрями їх розв'язання, які формують тактику першочергових слідчих дій.

Таким чином, розглядані типові слідчі ситуації та напрями їх розв'язання при розслідуванні злочинів, пов'язаних зі створенням, використанням, розповсюдженням або збутом шкідливих програмних засобів зумовлюють висунення типових слідчих версій та напрямів їх розслідування. Окрім цього, у сукупності типові слідчі версії зумовлюють черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування такого злочину, серед яких важливе місце займають такі напрями, як отримання та аналіз доказів, що пов'язані зі створенням та використанням шкідливих програмних заходів подолання протидії слідчим діям, та залучення до слідчих заходів експертів у сфері інформаційних технологій і програмування.

Висновки до розділу 2

Дослідивши особливості початкового етапу розслідування злочинів, пов'язаних зі створенням, використанням, розповсюдженням або збутом шкідливих програмних засобів, необхідно визначити узагальнення, характерні особливості й рекомендації щодо удосконалення цього процесу.

У криміналістиці типовою слідчою ситуацією вважають складну систему взаємозв'язків, яка утворює ту конкретну обстановку, у якій працює слідчий й інші суб'єкти, що беруть участь у доказуванні, і у якій протікає конкретний акт розслідування [106]. Схарактеризовано типові слідчі ситуації та напрями їх розв'язання при розслідуванні злочинів, пов'язаних зі створенням, використанням, розповсюдженням або збутом шкідливих

програмних засобів, та сформульовано закономірні ситуації, які при цьому виникають.

Виокремлені типові слідчі ситуації та напрями їх розв’язання при розслідуванні злочинів зумовлюють відповідну черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування такого злочину. Серед цих заходів найбільш суттєве значення мають такі напрями, як отримання та аналіз доказів, що пов’язані зі створенням та використанням шкідливих програмних заходів, подолання протидії слідчим діям, та залучення до слідчих заходів експертів у сфері інформаційних технологій і програмування.

РОЗДІЛ 3. ПРОВЕДЕННЯ СЛІДЧИХ (РОЗШУКОВИХ) ДІЙ ПІД ЧАС РОЗСЛІДУВАННЯ СТВОРЕННЯ, ВИКОРИСТАННЯ, РОЗПОВСЮДЖЕННЯ АБО ЗБУТУ ШКІДЛИВИХ ПРОГРАМНИХ ЧИ ТЕХНІЧНИХ ЗАСОБІВ

3.1. Організаційно-тактичні особливості проведення слідчих (розшукових) дій під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Варто наголосити, що криміналістична тактика фактично виступає як комплекс знань із галузі науки криміналістики, що формуються на підставі практики застосування норм процесуального й матеріального права, а також окремих елементів методики здійснення досудового розслідування тих чи інших видів кримінальних правопорушень та є важливими при проведенні слідчих (розшукових) дій у досудовому розслідування конкретного кримінального провадження. На підставі узагальненої інформації з указаних сфер існує ймовірність підвищення результативності процесів доказування, збору доказової інформації, її аналізу, що докорінно впливатиме на об’єктивність, неупередженість та швидкість відповідного досудового розслідування.

Справді, це складна система положень, прийомів і рекомендацій, що належать не тільки до проведення окремих процесуальних дій, а й до організації та планування попереднього й судового слідства в цілому, оскільки планування, версіювання та інші інститути науки криміналістики аналогічно важливі в контексті успішності здійснення досудового розслідування конкретного кримінального правопорушення.

Науковці-криміналісти звертають суттєву увагу на те, що галузь предмета криміналістичної науки складають як загальна її теорія, так і техніка, тактика й методика, проте в умовах обмеженості обсягу дисертаційної роботи пропонуємо в межах відповідного підрозділу дослідити

тактичне забезпечення розслідування правопорушень, пов'язаних зі створенням, використанням та розповсюдженням шкідливих програмних засобів.

Слідчі дії складають основний процес відтворення типових слідчих ситуацій і слідчих версій, котрі формуються слідчим у процесі розслідування злочинів, що має безпосередній стосунок і до злочинів із використанням шкідливих програмних засобів. Проведене В. О. Голубєвим дослідження показало, що найпоширенішими приводами порушення кримінальних справ (до 2013 року) за ст. 361-1 КК України визнавали такі:

- повідомлення посадових осіб організацій або їх об'єднань (біля 40 %);
- заяви громадян (біля 35 %);
- безпосереднє виявлення органом дізнання, слідчим або прокурором відомостей, які мають ознаки злочину (біля 20 %);
- повідомлення в засобах масової інформації тощо (біля 5 %).

Узагальнення практики показує, що при відкритті кримінального провадження за ст. 361-1 КК України встановлено такі ситуації:

1. Незаконне втручання виявлене в ході реалізації комп'ютерної інформації незаконним користувачем (наприклад, при розповсюдженні відомостей, що мають конфіденційний характер).

2. Факт незаконного втручання в роботу електронно-обчислювальних машин (комп'ютері), систем і комп'ютерних мереж виявлений законним користувачем, але особа, яка його вчинила, не встановлена.

3. Факт злочину виявлений законним користувачем, який зафіксував на своїй ЕОМ дані про особу, яка здійснює «перекачування» інформації через мережу.

4. Правопорушника застали на місці вчинення незаконного втручання в роботу електронно-обчислювальної машини.

5. Мало місце незаконне втручання в роботу ЕОМ (комп'ютері), систем і комп'ютерних мереж, однак особа, яка його вчинила, не виявлена.

Законодавець відповідно до ст. 214 КПК України дозволяє протягом 24 годин після отримання заяви або повідомлення про вчинений злочин провести перевіряльні дії: отримати пояснення, провести огляд місця події, затребувати необхідні матеріали, здійснити оперативно-розшукові заходи [29, с. 111].

Під час розслідування комп'ютерних та інших злочинів виникає низка питань процесуального характеру. Так, згідно з вимогами кримінального процесуального законодавства України до відкриття кримінального провадження слідчий має право провести огляд місця події [111, с. 65].

Водночас загальні положення криміналістичної тактики визначають підготовчий, дослідний та заключний етапи як самого досудового розслідування, так і окремо взятих слідчих (розшукових) дій, що, на нашу думку, потребує наукової інтерпретації та застосування аналогії в контексті теми дисертації та мети щодо формування загального уявлення про окремі елементи криміналістичної методики досудового розслідування кримінальних правопорушень щодо створення, розповсюдження або збуту шкідливих програмних (технічних) засобів.

Так, наприклад, підготовчий етап до проведення огляду місця події, аналогічно з іншими слідчими (розшуковими) діями, має декілька стадій проведення, що, зі свого боку, мають бути поетапно реалізовані слідчим як основним суб'єктом проведення відповідної дії.

Ураховуючи специфіку розслідування злочинів з інформаційними технологіями, слідчому необхідно до виїзду на місцевість ознайомитися з матеріалами кримінального провадження, які були йому надані як вихідна інформація. Але йому одному досить важко та навіть і неможливо впоратися з таким обсягом робіт щодо опанування масиву криміналістично-значущої інформації за короткий проміжок часу. Тому з метою оперативності та ефективності підготовчої стадії до виїзду на слідчу дію до відкриття кримінального провадження долучається оперативний працівник, одним із завдань якого буде проведення таких заходів:

- установити місцезнаходження засобів електронно-обчислювальної техніки (у подальшому – ЗЕОТ), комп'ютерної інформації та документів, що використовувалися під час підготовки, здійснення й приховування злочину, а також інших можливих предметів, які стосувалися протиправної дії;

- при визначенні місця, де знаходяться ЗЕОТ і комп'ютерна інформація, за допомогою яких було здійснено правопорушення, провести оперативну установку з метою: а) виявлення їх власника чи користувача або осіб, допущених до програмного забезпечення; б) можливості процесуального вилучення комп'ютерної інформації;

- з'ясувати схематичний план місця (приміщення, ділянки місцевості, де буде проводитися слідча дія), місцерозташування технічних засобів та їх кількість;

- установити режим роботи об'єкта, де проводитиметься слідча дія, кількісний та персональний склад працівників та допущених до операційної системи осіб тощо [75].

Оскільки знаряддями вчинення вказаних злочинів є засоби комп'ютерної техніки, зокрема спеціальне програмне забезпечення, огляду насамперед підлягають саме вони.

Слідчий, який збирається виїжджати на огляд місця події, повинен мати при собі 'такі речі:

- відформатовані носії інформації різних форматів, які використовуватимуться для накопичення вилученої з обшукуваного комп'ютера інформації;

- велику кількість липкої стрічки чи інших засобів захисту дисків від запису;

- пакет універсальних програм-утиліт для забезпечення безперешкодного й ефективного вилучення з комп'ютера доказової інформації;

- набори кольорових наклейок для маркування вилучених речей;

- папір для принтера;

- системні носії, тобто ті, із яких можливо ініціювати роботу операційної системи;

- програми виявлення комп'ютерних вірусів для захисту комп'ютерної системи від можливих ушкоджень через обладнання, яке використовує слідчий (це можуть бути як носії, виявлені на місці події, так і програми, отримані через канали зв'язку) [83]. Попередньо ми звертали увагу на необхідності залучення не лише кваліфікованих понятих до проведення того чи іншого огляду чи будь-якої іншої слідчої розшукової дії, а також і спеціалістів відповідного фаху та рівня, що можуть суттєво вплинути на результативність проведення відповідної слідчої (розшукової) дії та сприяти якомога більшому обсягу доказової інформації, здобутої в такий спосіб.

В окремих криміналістичних джерелах існує інша думка, а саме: під час проведення огляду, тимчасового доступу до речей і документів, обшуку, слідчого експерименту, одержання зразків для експертного дослідження, допитів тощо виникає необхідність залучення спеціалістів з інформатики, програмування, електронних мереж, ремонту електронного обладнання [74], водночас подібний підхід ми обґрунтовували крізь усе дослідження, адже встановити характер, зміст, сутність та всі інші об'єктивні обставини, пов'язані зі створенням, розповсюдженням, збутом та іншими видами обігу шкідливих програмних (технічних) засобів неможливо без використання спеціальних знань не лише в їх класичному розумінні, а й у розрізі дотичного їх застосування різними учасниками слідчих (розшукових) дій.

Водночас на певному історичному етапі становлення криміналістичної методики досудового розслідування злочинів у сфері розповсюдження шкідливих програмних засобів обґрунтовувалась позиція про введення поняття «універсальний комп'ютерний експерт» [5], що, на нашу думку, на сучасному етапі революційних перетворень у науці та техніці, становленні новітніх форм комп'ютерно-технічної взаємодії, а також широкого кола різноманітних видів комп'ютерних знань неможливо. Утім важливим є

окреслення переліку спеціалістів у комп'ютерній галузі за видами діяльності для того, щоб слідчий орієнтувався в питаннях суб'єктів, яких необхідно залучати до проведення того чи іншого слідчого заходу чи проведення дослідження.

Розслідуючи злочини, пов'язані зі шкідливими комп'ютерними програмами, органи, які ведуть боротьбу з цим суспільно небезпечним діянням, наштовхуються на такі труднощі:

1. Можливе швидке зникнення слідів учиненого злочину.

2. Відсутність належної взаємодії.

Серед непроцесуальних форм взаємодії слідчого з органами дізнання провідне місце посідають: надання слідчими попередньої правової оцінки матеріалам оперативно-розшукової діяльності, зібраним працівниками оперативних підрозділів та обмін інформацією між слідчим та органом дізнання про хід та результати слідчих дій й оперативно-розшукових заходів.

Матеріали оперативно-розшукової діяльності можна використовувати для отримання фактичних даних, які можуть бути доказами в кримінальному провадженні за наявності певних умов, до яких належить те, що вони повинні знаходитися в причинному зв'язку з предметом доказування, установлювати наявність чи відсутність події злочину і мотиви злочину, характер і розмір шкоди й інші обставини, що мають значення для кримінального провадження. Фактичні дані, що отримані оперативно-розшуковим шляхом, повинні бути введені у кримінальний процес лише в передбачених кримінально-процесуальним законодавством джерелах. Уведення фактичних даних у кримінальний процес повинно відбуватися відповідно до правового режиму для кожного з конкретних видів доказів. Необхідним є виконання вимог щодо перевірки в ході процесуального розслідування отриманих матеріалів із метою всебічного, повного й об'єктивного їх розгляду та оцінки.

Сьогодні перед правоохоронними органами України під час розслідування таких злочинів виникають криміналістичні проблеми, які характеризують специфіку цього процесу, а саме: складність установлення

факту вчинення комп'ютерного злочину; складність кваліфікації злочинних діянь; складність підготовки і проведення певних слідчих дій; відсутність спеціалістів, необхідних для залучення до участі у проведенні слідчих дій; особливість вибору й призначення необхідних судових експертиз; доцільність використання засобів комп'ютерної техніки в розслідуванні злочинів такої категорії; відсутність у значної кількості слідчих та оперативних працівників елементарних знань у галузі комп'ютерної техніки; відсутність узагальнення слідчої й судової практики з розслідування злочинів цієї категорії; відсутність цілісної методики розслідування комп'ютерних злочинів [111, с. 66].

При огляді місця події під час розслідування злочинів, пов'язаних із шкідливим програмним забезпеченням, робота слідчого, крім виявлення, фіксації і вилучення традиційних слідів, полягає й у виявленні, фіксації і вилученні так званих слідів модифікації інформації [83]. Водночас слід підкреслити, що проведення огляду в указаній категорії кримінальних правопорушень пов'язують не лише з необхідністю обізнаності слідчого, а й потребою в залученні осіб зі спеціальним знаннями, оскільки, як свідчить практика, у ході такого огляду вилучають значний обсяг цифрової інформації як на носіях, так і безпосередньо з баз даних і хмарних сховищ, що, зі свого боку, потребує як належного рівня комп'ютерно-технічних знань, так і дотримання відповідних процесуальних тонкощів і особливостей, оскільки важливість відповідної слідчої (розшукової) дії не викликає сумнівів.

Саме ця слідча дія сприяє розв'язанню низки таких важливих питань: на якому об'єкті (на якому конкретно комп'ютері, у якому структурному підрозділі установи) сталася подія; до якого виду можна віднести комп'ютерний злочин, що має місце; яким способом вчинено злочин; які сліди чи інші речові докази вказують на причетність до злочину певної особи; яким є на час огляду стан засобів захисту інформації, охорони приміщень, обладнання тощо [14].

Завданнями слідчого щодо вибору понятих для участі в проведенні огляду місця події є підбір їх із числа тих осіб, котрі мають хоча б

елементарні уявлення про роботу із засобами комп'ютерної техніки. Водночас недоцільно залучати в ролі понятих для участі в проведенні огляду місця події співробітників чи керівників тих структурних підрозділів установи, організації, де було вчинено комп'ютерний злочин [4, с. 91].

На виявлених носіях також можуть міститися дані про інші правопорушення, зокрема, такі злочини: незаконні бухгалтерські та фінансові операції, здійснені в кредитно-фінансовій сфері; програми, які відповідають за проведення електронних платежів мережею «Інтернет» із використанням послуг інтернет-магазинів і суб'єктів господарювання з ознаками фіктивності, а також списки проведених перерахувань із чужих рахунків і кредитних карток на рахунки злочинців та їх співучасників; відомості про рахунки, кредитні картки потерпілих у вітчизняних та закордонних банках, спеціальне програмне забезпечення, яке дає змогу одержувати реквізити таких рахунків і карток; листування учасників злочину, яке стосується організації та вчинення злочину; відомості, які становлять державну, комерційну, банківську таємницю, а також порушують авторські та суміжні права; шкідливі програми; інформація про конфіденційні реквізити доступу до системних ресурсів персональних комп'ютерів і нелегального доступу до мережі «Інтернет» [108, с. 79].

Паралельно з дослідженням технічних комп'ютерних засобів не зайвим буде проведення відповідних пошукових заходів на предмет виявлення можливих витоків інформації з обстежуваного приміщення чи конкретної операційної системи. Для цього необхідно застосувати спеціальне оснащення та перевірити ймовірні місця зняття інформаційних даних. Це можуть бути електроустановлювальна арматура, дверні та віконні отвори, пожежна й вентиляційна системи, сигналізація, телекомунікаційне устаткування, а також усе комп'ютерне обладнання тощо. Доцільно перевірити облікові документи підприємства, де зазначені дані про осіб, що працюють із кібернетичними технологіями та мають до них доступ (журнали обліку робочого часу, проведення ремонтних робіт, регламентних та аварійних), документи

поточної діяльності підприємства (накази, розпорядження, договори) [76]. Слід зазначити, що основною метою проведення обшуку в кримінальному провадженні щодо поширення ШПЗ має бути вилучення саме тих предметів і об'єктів відповідного злочинного механізму, що сприяли його вчиненню.

Такі дані не можуть бути розкриті для їхнього копіювання або вивчення на іншому обладнанні. Для відновлення даних потрібні спеціальні комп'ютерні програми, інколи додаткове обладнання. За певних обставин можна визнати припустимим вилучення даних шляхом їх копіювання на окремі носії інформації, забезпечивши цілісність і збереження вилучених даних. Крім того, використані для копіювання носії не повинні містити ніякої інформації й мають бути в інформаційному розумінні «чистими», що створює умови та гарантії ідентичності копії оригіналу на момент провадження обшуку або виїмки та надійності її зберігання протягом усього часу розслідування і навіть розгляду справи судом [111, с. 68].

Отже, на початковому етапі розслідування основним завданням слідчого є встановлення всіх джерел доказової інформації та осіб, що вчинили такий злочин. Від того, як слідчий вирішить ці завдання, залежить подальший етап розслідування та результати досудового розслідування взагалі. Саме тому на вирішення цих завдань спрямоване правильне проведення огляду місця події, обшуків та виїмок, а також допитів. Недоцільно проводити різке розмежування між особливостями збирання комп'ютерної інформації при проведенні різних слідчих дій. Пояснюється це єдиними об'єктами – комп'ютером та інформаційним масивом, що знаходиться в ньому. Виходячи з цього, очевидно, що в ході будь-якої слідчої дії при виявленні засобів комп'ютерної техніки і наявності достатніх підстав вважати їх потенційними джерелами криміналістично значущої комп'ютерної та іншої інформації повинен проводитися їхній огляд у межах цієї слідчої дії.

Тактичні особливості такого огляду, на думку М. Г. Щербаковського та Д. В. Пашнєва, мають бути такими самими, що й при огляді місця події. Слід зауважити, що тактичні особливості цієї процедури повинні досліджуватись у

нерозривному зв’язку з технічними рекомендаціями, що мають безпосереднє значення для збирання комп’ютерних слідів злочину на носіях комп’ютерної інформації, а також для збереження цих слідів при збиранні традиційних слідів злочину [127, с. 51].

При підготовці до проведення слідчої дії в кримінальних провадженнях про комп’ютерні злочини слідчий обов’язково повинен використати спеціальні знання спеціаліста з комп’ютерних технологій для:

– консультування з питань визначення комп’ютерної специфіки слідчої дії, визначення її окремих цілей, способу і прийомів їх досягнення;

– надання допомоги в підборі понятих, що відповідають певним вимогам [50].

Науковці неодноразово звертали увагу на те, що при здійсненні досудового розслідування будь-яких кримінальних правопорушень, де речовими доказами є спеціальні об’єкти, зокрема комп’ютерна техніка, електронно-обчислювальні пристрої та інші інформаційно-технічні досягнення цивілізованого суспільства, в обов’язковому порядку має бути залучено спеціаліста, тобто особу, яка володіє спеціальними знаннями [30]. На нашу думку, важливим є залучення спеціаліста не лише на початковому етапі, а й під час проведення основних слідчих розшукових дій, оскільки спеціаліст може значно сприяти правильному вилученню того чи іншого предмета (об’єкта), а також запобігти втраті важливої доказової інформації, яка міститься на певному носії.

Це, зокрема, підтверджують також праці інших дослідників, які зазначають, що певна необережність у діях слідчого чи іншої особи, що бере участь у фізичному вилученні того чи іншого потенційного носія доказової інформації, може призвести до незворотної втрати відповідних перспективних доказів, що в подальшому унеможливить доведення винуватості певної особи.

Деякі вчені також укріплюють позицію про те, що розглядати слідчого як носія спеціальних знань під час розслідування комп’ютерних злочинів не

можна, оскільки для повноцінного аналізу доказів не обійтися без залучення спеціаліста чи експерта як процесуальної фігури [100, с. 110]. На нашу думку, важливою є указівка на взаємообумовлювальний характер дії криміналістичної методики здійснення досудового розслідування певної категорії кримінального правопорушення, а також дію норм КПК України, який в такому випадку регулює процесуальні аспекти як залучення того чи іншого учасника слідчої (розшукової) дії, так і порядок вилучення тієї чи іншої інформації, що міститься на матеріальних об’єктах.

Висловлена нами концепція, зокрема й на думку В. М. Бутузова, має бути ключовою в позиціях тих дослідників, котрі формують криміналістичні методики здійснення досудового розслідування кримінальних правопорушень за певними видами. На думку дослідника, використання шпигунського програмного забезпечення та комп’ютерних програм, що призначені для вторгнення в особисте життя особи є неприпустимим, а відповідна галузь потребує системної, злагодженої та спланованої завчасно підготовки фахівців вузькоспеціалізованих підрозділів правоохоронних органів, які здатні застосовувати сучасні методи оперативно-технічного документування та розкриття комп’ютерних злочинів [18]. На нашу думку, це зауваження є досить слушним, проте в умовах формування криміналістичних засад методики здійснення досудового розслідування відповідної категорії кримінальних правопорушень таким, що не відповідає предмету дослідження, хоча й впливає на досягнення результатів у досудовому розслідуванні.

Практика розслідування комп’ютерних злочинів свідчить, що максимальний ефект від проведення окремих слідчих дій досягають у тих випадках, коли їх планують і здійснюють у межах однієї тактичної операції, що має єдність мети і підпорядкована загальним завданням узгодженої системи слідчих, пошукових, оперативно-розшукових та організаційних заходів. Заставлення, доповнення, оцінка та використання інформації, яка отримана при виконанні слідчих дій і проведенні оперативно-розшукових

заходів, сприяють швидкому встановленню осіб, які вчинили комп'ютерний злочин, та збиранню доказів у кримінальному провадженні. Направляючи оперативному підрозділу доручення та деякі доручення про проведення слідчих (розшукових) чи негласних слідчих (розшукових) дій у кримінальних провадженнях про шкідливі комп'ютерні програми, слідчий безпосередньо у тексті згаданих вище документів має вказувати на необхідність участі у зазначених діях спеціаліста в галузі інформатики та обчислювальної техніки. Участь понятих із-поміж осіб, що мають фахові знання у галузі комп'ютерної техніки, під час провадження слідчих дій практично унеможливлює випадки звернень зацікавлених осіб із скаргами на спотворення органами розслідування інформації, яка зберігалася в комп'ютерах чи на магнітних носіях і була виявлена та вилучена під час проведення слідчої дії. Розслідування злочинів здійснюється в ситуації конфлікту інтересів, протидії зацікавлених осіб.

Розроблення методів розкриття злочинів, дослідження прийомів провадження окремих слідчих дій під час досудового розслідування в кримінальних провадженнях про комп'ютерні злочини потребує поглибленого дослідження. Тактико-криміналістичне забезпечення розслідування комп'ютерних злочинів повинно враховувати всі аспекти проведення слідчих дій із метою швидкого й повного розкриття злочинів, викриття винних та недопущення притягнення до кримінальної відповідальності невинних [111, с. 68].

Виходячи з вищенаведеного, необхідно резюмувати, що особливості тактики проведення окремих слідчих дій полягають у специфічності комп'ютерних устаткувань інструментів вчинення злочинів – шкідливих комп'ютерних програм. Тактика проведення окремих слідчих дій на початковому етапі розслідування даних злочинів зумовлена слідчими ситуаціями і слідчими версіями, котрі перевіряють у процесі таких слідчих дій, як виїмка, огляд, обшук, допит, експертиза та інших слідчих заходів. Саме на цьому етапі виявлення об'єктивних ознак злочину залежатиме

від професіоналізму слідчого та допоміжних фахівців-експертів у сфері комп'ютерних технологій. Тому важливим науковим завданням постає характеристика типових тактичних операцій при розслідуванні створення, використання, розповсюдження або збуту шкідливих програмних засобів.

Першочерговими діями слідчого на місці події мають бути ужиття заходів щодо збереження ситуації такою, якою вона була до моменту прибуття, з метою запобігання знищенню інформації, а саме: вивести всіх осіб із зони доступу до обладнання, запобігти втручанню в систему через лінії зв'язку (зокрема через модеми), а також внесення змін у роботу системи. Якщо в приміщенні знаходяться декілька комп'ютерів, об'єднаних між собою в мережу, слідчий повинен попросити осіб, які за ними працюють, залишити місця роботи й відійти від цих комп'ютерів. Необхідним є проведення відеозапису місця події для фіксації поточного стану операційної системи комп'ютера та порядку розташування його обладнання, проведення фотозйомки серійних номерів та номерів моделей комп'ютерного обладнання, а також нумерація комп'ютерного обладнання відповідно до його розташування на місці події [83].

Після успішного проведення відповідних заходів підготовчої стадії до здійснення огляду місця події слідчо-оперативна група має приступити до не менш складного завдання – робочого (дослідного) етапу зазначеної слідчої дії, обов'язковою умовою якого є чітке дотримання норм КПК України. Цю стадію доцільно, як і попередню, також поділити на умовні підетапи: загальний огляд (статична дія), детальний (динамічна дія) [75, с. 104].

Наступною тактичною стадією є обшук і виїмка об'єктів, котрі можуть відображати шкідливі програмні засоби. Слід зауважити, що під час проведення обшуку та виїмки об'єктів, що мають доказове значення в досудовому розслідуванні кримінальних правопорушень у сфері електронно-обчислювальної техніки, важливим є віднайдення та вилучення не лише фізичних носіїв (банки даних, комп'ютерна техніка, серверне обладнання тощо), а й фактичної інформації, що на них міститься, оскільки

в подальшому безпосереднє доказове значення в суді матиме лише інформація, що містить доводи кримінальної протиправності дій особи, а не той фізичний носій, який її зберігав. Водночас такий носій може свідчити про те, який саме спосіб було застосовано зловмисником для досягнення відповідно поставленої злочинної мети.

Водночас дослідники неодноразово звертали увагу на те, що способи вилучення відповідних матеріальних носіїв різняться, оскільки вилучення інформації з деяких можливе лише в спеціальних умовах (наприклад, під час проведення експертизи), саме тому першочергово, під час проведення відповідної слідчої (розшукової) дії обшуку, має бути вилучено відповідні матеріальні об’єкти, а вже згодом вилучено інформацію з них у процесі призначеного експертного дослідження. Утім слід звернути увагу, що в процесі проведення обшуку також можливе вилучення та/або копіювання доказової інформації за добровільною згодою власника такого пристрою, що суттєво спростить процес здійснення досудового розслідування.

А. С. Белоусов наголошує, що існують слідчі ситуації, за основних умов яких неможливим і в подальшому процесуально необґрунтованим є вилучення матеріальних об’єктів із місця проведення обшуку в кримінальному провадженні щодо незаконного використання електронно-обчислювальних машин у злочинних цілях. Наприклад, на думку автора, не доцільно здійснювати копіювання вилученої інформації на носії, що містять навіть таку інформацію, яка стосується цього кримінального провадження, навіть якщо ця інформація ідентична повністю або містить фрагменти тієї, котра підлягає вилученню [4, с. 93]. Така позиція цілком відображає позицію суду з відповідного питання, оскільки носій, на який здійснюється вилучення чи/або копіювання відповідної доказової інформації, має бути спеціально підготовлений та цілісний, тобто не ушкоджений і не заповнений іншою, навіть тією, що стосується здійснення цього досудового розслідування, інформацією, оскільки в подальшому такий доказ, зібраний у неналежний спосіб можна буде визнати недопустимим.

Як свідчить аналіз слідчої і судової практики, найбільш типовими слідчими (розшуковими) діями, що виступають засобами збирання доказів при розслідуванні злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж є огляд, обшук, допит, експертиза.

Огляд і обшук. Такі слідчі (розшукові) дії є одними з найбільш розповсюджених і потребують найбільш детального аналізу, оскільки огляд і обшук у досудовому розслідуванні використання, розповсюдження або збуту шкідливих програмних чи технічних засобів має свою специфікацію й вимоги як до кваліфікації працівника, що його проводить (слідчого), так і до осіб, яких необхідно задіяти під час його проведення. Це питання потребує розгорнутого наукового тлумачення й саме тому складатиме значну частину в межах відповідного підрозділу.

Так, огляд є найбільш розповсюдженою слідчою (розшуковою) дією відносно потерпілої від використання, розповсюдження або збуту шкідливих програмних чи технічних засобів особи, оскільки така дія може (і як показує аналіз матеріалів слідчої практики) проводиться за добровільною згодою потерпілої особи, оскільки остання є зацікавленою в якнайшвидшому зборі доказової інформації та встановленні причетних до вчинення протиправних діянь. У той же час, слід указати, що обшук є примусовою слідчою (розшуковою) дією, і його проведення не завжди узгоджується з інтересами особи, у якої його проводять, оскільки крім цього, така дія має характеристику раптовості, що зобов'язує слідчого перед її проведенням звернути увагу на технічну, процесуальну та морально-психологічну підготовленість до його проведення.

Обшук приміщення, де відбувалось використання, розповсюдження або збут шкідливих програмних чи технічних засобів також має певні особливості не лише з криміналістичного, а й із кримінального процесуального погляду. Так, наприклад, розпочати його варто з відшукування слідів пальців рук на слідосприймальних поверхнях, які і є

основними об’єктами при відшукуванні такого типу інформації. У той же час, вилученню під час обшуку такого приміщення підлягають будь-які технічні пристрої, які мають відповідні характеристики й могли бути використані для вчинення відповідного протиправного діяння.

При огляді та обшуку треба встановити та описати в протоколі слідчої дії тип апаратури, найменування фірми виробника, серійний номер, рік випуску і номери, інші індивідуальні ознаки та місце виявлення [46], оскільки ці індивідуалізовані параметри та характеристики дають змогу забезпечити точність та змістовність отримуваної доказової інформації у процесі призначення експертних досліджень, а також при використанні методів криміналістичного версіювання та плануванні відповідного досудового розслідування.

В. П. Диденко звертає увагу на те, що треба в обов’язковому порядку застосовувати під час такого огляду/обшуку відеофіксацію, оскільки це значно спростить проведення відповідної слідчої (розшукової) дії, а також убезпечить зібрані докази від визнання їх недопустимими в умовах неможливості повторного проведення обшуку/огляду [37, с. 91–97]. На нашу думку, крім застосування відеофіксації під час проведення огляду/обшуку, важливим є також схематичне відтворення обстановки й умов, що є об’єктами огляду, оскільки цей спосіб є найбільш доступним і зрозумілим. У випадку конструктивного взаємодоповнення тексту протоколу, відеоматеріалу й відповідної схеми це зумовить неможливість визнання такої слідчої (розшукової) дії недопустимою.

І. М. Горбаньов зауважує, що особливу увагу слід звернути на засоби вчинення злочину й вилучити з місця події апаратуру, котра використовувалась для незаконного тиражування комп’ютерних програм [33, с. 70]. Водночас, на нашу думку, не лише місце події може стати об’єктом огляду в контексті досудового розслідування відповідного кримінального правопорушення. Це насамперед місце, де воно було безпосередньо вчинене, а також місце, де було завдано злочинного

шкідливого наслідку – здебільшого в досудовому розслідуванні відповідних правопорушень ці місця не є одними й тими самими.

Не варто обмежуватися пошуком інформації тільки в комп'ютері або на певному магнітному носієві, який виявлено в приміщенні. Слід ретельно вивчити наявну документацію, різноманітні записи, які можуть містити програми, паролі, відомості щодо змін в конфігурації системи, особливостей побудови інформаційної бази комп'ютера тощо.

При розслідуванні комп'ютерних злочинів огляд (обшук) проводять на місці:

- збереження й оброблення комп'ютерної інформації, яка зазнала злочинного впливу (наприклад, у разі незаконного втручання у роботу ЕОМ (комп'ютерів), їх систем чи комп'ютерних мереж);

- знаходження комп'ютерного обладнання, яке використовувалося при вчиненні злочину (у разі поширення комп'ютерного вірусу після незаконного проникнення в комп'ютерну мережу);

- збереження інформації, отриманої злочинним шляхом (у разі заволодіння комп'ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем);

- порушення правил експлуатації ЕОМ, комп'ютерної системи або мережі;

- настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп'ютерної інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі) [111].

Будь-яка слідча (розшукова) дія результативна лише за умов її попередньої підготовки. Підготовка до огляду (обшуку) під час розслідування зазначених злочинів містить дві стадії.

1. До виїзду на місце слідчому необхідно:

- з урахуванням слідчої ситуації, що склалася, намітити коло осіб, які візьмуть участь у слідчій (розшуковій) дії. Окрім учасників СОГ (слідчого, співробітника Департаменту кіберполіції, спеціаліста експерта-криміналіста),

залучити спеціалістів із комп'ютерних технологій, представників юридичних осіб або потерпілих;

- запросити понятих. Бажано запрошувати таких осіб, які мають достатній рівень знань у галузі комп'ютерних технологій. Якщо не має можливості залучити кваліфікованих понятих, то дії слідчого (спеціаліста) з дослідження ЕОМ чи з комп'ютерної інформації повинні пояснюватися. Зазначене необхідне на випадок допиту понятих у суді як свідків;

- підготувати відповідну комп'ютерну техніку, програмне забезпечення, що буде використовуватися для зчитування і збереження вилученої інформації. Традиційно відповідні технічні засоби застосовують ІТ-спеціалісти, але це не знімає відповідальності зі слідчого за їх наявність і комплектність;

- пояснити мету проведення слідчої (розшукової) дії та завдання, що стоять перед її учасниками, їхні права та обов'язки, а також необхідні заходи обережності під час пересування на місці огляду (обшуку) або роботи зі слідами тощо.

2. Після прибуття на місце проведення огляду слідчий повинен:

- видалити з місця проведення слідчої (розшукової) дії сторонніх осіб та забезпечити його охорону, якщо це не було зроблено раніше. Обов'язковій охороні підлягають: територія місця події, затриманий, ЕОМ, у якій було виявлено сліди злочину, сервер, пункти вимкнення живлення, якщо техніка знаходиться в увімкнутому стані тощо;

- виключити можливість стороннім особам чинити будь-які дії з комп'ютерною технікою. Позбавити їх можливості користуватися іншими технічними засобами, що можуть за допомогою бездротових технологій внести зміни (видалити) інформацію. Практиці відомий випадок, коли під виглядом кур'єра, який доставив замовлення, на місце обшуку проник співробітник ІТ-компанії, за допомогою смартфону та WI-FI з'єднався з сервером і видалив всю інформацію;

- опитати потерпілого (заявника), свідків про те, що відбулося, зміни, які були внесені в обстановку, дії осіб до прибуття СОГ, види та технологічні операції, у ході яких було виявлено ознаки злочину тощо;

- дати доручення учасникам СОГ на встановлення свідків, виявлення слідів, їх фіксацію тощо.

Найбільш доцільним шляхом подолання захисту комп'ютерної інформації від несанкціонованого доступу є призначення комп'ютерно-технічної експертизи, під час якої експерт вирішить питання щодо наявності захисту, його виду, способу подолання, професійності користувача комп'ютера тощо. Для вирішення питання про необхідність зняття даних, що знаходяться в ОЗП, слід виходити з обставин кримінального провадження та слідчої ситуації. У протоколі слідчої (розшукової) дії описують основні фізичні характеристики приладів, магнітних та інших постійних носіїв інформації, що вилучають, серійні номери апаратури, їх видимі індивідуальні ознаки, вид упакування тощо.

Допит свідків (потерпілих). Приймаючи рішення про допит конкретної особи як свідка, слідчий повинен заздалегідь спрогнозувати, яку саме інформацію (насамперед технічного характеру) він може одержати від допитуваного. Орієнтуючись на це, і необхідно підготувати комплекс запитань. Скласти орієнтовний перелік запитань може допомогти спеціаліст із комп'ютерних технологій. За можливості бажано, щоб він взяв безпосередню участь у проведенні допиту. Відповідно до ч. 4 ст. 71 КПК України спеціаліст має право ставити запитання, звертати увагу на певні обставини тощо. Зазначене дозволить слідчому отримати повну інформацію про обставини злочину та осіб до нього причетних. Ураховуючи специфіку злочинів, що розглядають, слідчому під час допиту доцільно використовувати ілюстративний матеріал та словники спеціальних термінів, це надасть можливість оперувати правильними термінами та однозначно інтерпретувати показання свідків і потерпілих.

При розслідуванні неправомірного доступу до комп'ютерної інформації на початку кримінального провадження виникає необхідність допитувати як свідків громадян різних категорій, для кожної із який існує своя специфіка [99].

Допит підозрюваного. Указана слідча (розшукова) дія є достатньо складною з погляду її підготовки та проведення. Слідчому перед допитом підозрюваного доцільно вивчити його особистість (характер, темперамент, зв'язки, освіта, інтереси, хобі, авторитетні для підозрюваного особи тощо), рівень навичок володіння комп'ютерними технологіями, урахувати дані криміналістичної характеристики цього виду злочинів тощо. Така інформація надасть можливість сформувати лінію поведінки слідчому, визначитись із тактичними прийомами. Не менш важливим є аналіз спеціальної літератури з питань, які входять до предмета доказування та обставин, що підлягають встановленню під час допиту.

Основними тактичними завданнями допиту є: виявлення елементів складу злочину, установлення обставин, місця й часу значущих для слідства дій, способу й мотивів їх учинення, зовнішній вигляд осіб, що брали участь, визначення предмета злочинного посягання, розміру заподіяних збитків, установлення інших свідків та осіб, причетних до скоєння злочину. Допит можна визначити як слідчу дію, змістом якої є особисте спілкування слідчого з допитуваним із метою отримання в нього даних про обставини, які підлягають доказуванню в кримінальному провадженні [58, с. 314].

У чинному Кримінальному процесуальному кодексі досить чітко регламентовано порядок підготовки та проведення допиту, права й обов'язки особи, яка проводить цю дію, а також особи, котра підлягає допитові. У юридичній літературі зазначеному аспекту слідчих дій приділено чільне місце, ми сконцентруємо свою увагу на окремих особливостях допиту осіб у злочинах, пов'язаних з інформаційними технологіями.

Слідчий повинен визначити коло обставин предмета допита, а саме:

- обставини, пов’язані із самою подією злочину (час, місце, спосіб, наслідки тощо);

- обставини, які встановлюють чи спростовують винність конкретних осіб та мотиви їх дій, що впливають на ступінь та характер відповідальності обвинуваченого;

- обставини, які відносяться до характеру та розміру шкоди, нанесеної злочином тощо.

На думку О. І. Мотляха, формування підготовчого етапу до планування допиту слідчим має містити більш конструктивні аспекти, які повинні зацікавити слідство, а саме: з’ясувати специфіку кримінального провадження, особливо питання, що стосуються технічних аспектів підготовки та реалізації злочинних замислів; визначити обставини, які потребують уточнення інформації: а) відомості про потерпілу сторону; б) технічні та конструктивні особливості комп’ютерної системи, що піддавалася впливу; в) засоби комп’ютерної техніки, що використовувалися злочинцем при вчинення злочину; підготувати доказові або інші матеріали для пред’явлення в разі фіксації ходу слідчої дії. Згідно з нормами Кримінального процесуального кодексу України розрізняють такі види допиту: допит свідка, допит потерпілого, допит підозрюваного, допит обвинуваченого, допит експерта [75].

До тактичних прийомів допиту підозрюваних при розслідуванні «комп’ютерних» злочинів можна віднести:

1. Детальний допит із наступним зіставленням із матеріалами кримінального провадження.

2. Пред’явлення під час допиту доказів (висновки експертів, показання свідків, співучасників злочинну; вилучені під час огляду місця події та обшуку речові докази).

3. Аналіз отриманих від підозрюваного показань спеціалістом у галузі комп’ютерних технологій.

4. Постановка контрольних та деталізованих питань, що можуть свідчити про поінформованість слідчого про обставини, за яких вчинено злочин.

5. Повторний допит за тими обставинами, за якими підозрюваний раніше вже допитувався. Деталізація показань при повторному допиті може виявити невідповідність із першим, а протиріччя свідчити про їх неправду [99].

Варто мати на увазі, що на першому допиті підозрюваний може спробувати пояснити факт неправомірного доступу до комп'ютерної інформації некримінальними причинами (випадковістю, збігом визначених обставин, стороннім впливом тощо).

Для викриття таких осіб позитивні результати дає правильна реалізація інформації про злочинну діяльність цієї особи, отримана при проведенні негласних слідчих (розшукових) дій, а також участь під час його допиту спеціаліста, який своїми запитаннями може присікти неправдиві показання підозрюваного і дати зрозуміти, що подальше заперечення своєї участі в учинені злочину не буде мати якоїсь користі для нього. Перевірити показання підозрюваного, окрім зіставлення з тими даними, що містяться в матеріалах кримінального провадження, можна шляхом проведення слідчого експерименту.

3.2. Використання спеціальних знань під час розслідування створення, використання, розповсюдження або збуту шкідливих програмних чи технічних засобів

Результати аналізу наукових джерел та слідчої практики свідчать, що типові тактичні операції при розслідуванні створення, використання, розповсюдження або збуту шкідливих програмних засобів здебільшого

проходять у своєму розвитку такі етапи: слідчий огляд із метою виявлення ознак злочину; обшук та виїмка комп'ютерних об'єктів та носіїв комп'ютерної інформації; допит осіб у кримінальних провадженнях у процесі розслідування комп'ютерних злочинів; експертні заходи щодо виявлення та характеристики ознак створення, використання або збуту шкідливих програмних засобів.

Саме останньому з окреслених етапів ми плануємо приділити найбільшу увагу для того, щоб особливо підкреслити істотну роль спеціальних знань при виявленні, розслідуванні та судовому розгляді випадків створення, розповсюдження або збуту шкідливих програмних засобів. Застосування спеціальних знань у розкритті та розслідуванні злочинів, зокрема під час досудового слідства, є найбільш суттєвою, уже традиційною реалією для криміналістики [22].

Спеціальні знання – це сукупність теоретичних знань та практичних навичок із різних наук (крім права), техніки, мистецтва, ремесла, що здобуті шляхом спеціальної підготовки або професійного досвіду [71, с. 327].

Сабадаш Р. В., досліджуючи значення спеціальних знань при розслідуванні, справедливо зауважує, що метою застосування спеціальних знань при розслідуванні комп'ютерних злочинів є: збирання доказової інформації при розслідуванні комп'ютерних злочинів; дослідження комп'ютерної інформації в її первинному вигляді; дослідження електронних носіїв інформації та інформації, що знаходиться на них; розшифрування даних; установлення параметрів і можливостей комп'ютерних пристроїв; дослідження програмного забезпечення [100, с. 112].

Практика досудового розслідування свідчить, що у більшості слідчих випадків добути необхідну інформацію без використання спеціальних знань практично неможливо. Необхідність у співпраці зі спеціалістами інших профілів постає тоді, коли власні можливості і знання виявляються недостатніми для ефективної роботи зі встановлення фактів у процесі

розслідування, виявлення характерних ознак досліджуваних об’єктів тощо [21].

Стаття 71 КПК України дає законодавче визначення поняття спеціаліста як особи, яка володіє спеціальними знаннями та навичками застосування технічних або інших засобів і може надавати консультації під час досудового розслідування і судового розгляду з питань, що потребують відповідних спеціальних знань та навичок [67, с. 54–55].

Вказана кримінально процесуальна норма також регламентує випадки, у яких залучають спеціаліста, а також його права та обов’язки. Слідчий, яким би кваліфікованим та високоосвіченим він не був, завжди залишається спеціалістом вузького профілю. За межами його фахового кругозору здебільшого залишається чимало знань, які є надбанням людської цивілізації. Тому в разі потреби слідчий мусить звертатися по допомогу до спеціалістів – осіб, які компетентні в тій чи іншій галузі знань [21].

Спеціаліст, якого слідчий запрошує для участі в проведенні слідчих дій за справами про комп’ютерні злочини, повинен мати доскональні знання операційних систем, під керуванням яких функціонує конкретна обчислювальна система, та іншого програмного забезпечення, що задіяне в цій системі. За певних ситуацій він додатково повинен добре орієнтуватися в різних специфічних питаннях, зокрема в особливостях експлуатації мережного обладнання, у процедурах шифрування, надання доступу і збереження інформації тощо [110].

Слід звернути увагу на те, що залучення до проведення слідчих (розшукових) дій спеціаліста є необхідною умовою й запорукою її успішності, оскільки саме цей фах дає змогу найбільш якісно та детально розглянути всю необхідну доказову інформацію, указати на ті спеціалізовані складники об’єктивної та суб’єктивної сторони вчиненого кримінального правопорушення, які дозволять в подальшому довести винуватість особи, яка вчинила такі дії.

Завдання спеціаліста полягає в тому, щоб на підставі своїх знань він надавав сприяння слідчому у виявленні й вилученні слідів злочину, предметів та документів, що можуть бути речовими доказами в кримінальному провадженні [13, с. 121].

Завдання спеціаліста безпосередньо на місці проведення конкретної слідчої (розшукової) дії в досудовому розслідуванні кримінального правопорушення пов'язаного з використанням, розповсюдженням або збутом шкідливих програмних чи технічних засобів полягає у віднайденні ключових речових доказів, що становлять суто технічне значення для реалізації злочинного замислу в указаній сфері, що в подальшому дозволить конвертувати відповідну інформацію в доказову та долучити її до матеріалів досудового розслідування.

Отже, спеціаліст – це фізична особа, що досконало володіє певною спеціальністю, має знання й практичні навички в конкретній сфері людської діяльності [1].

При розслідуванні кримінальних правопорушень використання спеціальних знань здебільшого здійснюється у вигляді:

- залучення спеціалістів для участі в процесуальній та іншій діяльності;
- проведенні судових експертиз;
- проведення перевірок, обстежень, консультацій;
- допит спеціалістів як свідків, або експертів, якщо вони брали участь у проведенні перевірок, досліджень або експертиз.

На стадії судового розгляду, при дослідженні доказів, суд може користуватися усними або письмовими роз'ясненнями спеціаліста, наданими на підставі спеціальних знань відповідно до положень частини 1 статті 360 КПК України [60, с. 412].

У криміналістиці розрізняють дві форми застосування спеціальних знань – процесуальну та непроцесуальну.

До процесуальних форм використання спеціальних знань зараховують: залучення слідчим власних спеціальних знань; участь фахівця у слідчих діях;

проведення експертизи. Непроцесуальні форми використання спеціальних знань полягають у консультативний та довідковий діяльності свідуючих осіб, проведенні ревізійних й аудиторських дій, попередньому дослідженні матеріальних об'єктів, наданні технічної допомоги слідчому тощо [27].

Процесуальна форма застосування спеціальних знань порівняно з непроцесуальною є більш важливою та ефективною, оскільки вона передбачена законом і має юридичну силу. Слід зауважити, що вся діяльність спеціаліста із застосуванням спеціальних знань у непроцесуальній формі не має юридичної сили, оскільки вона не передбачена законодавством. Практикою однозначно встановлено, що участь спеціалістів підвищує ефективність слідчих дій, робить їх більш цілеспрямованими й підвищує якість фактично отриманих даних [57].

Сучасний науково-технічний прогрес створює сприятливі умови для застосування новітніх досягнень науки і техніки в боротьбі зі злочинністю, а це відкриває нові додаткові можливості реалізації спеціальних знань у судових експертизах. Призначення і проведення судових експертиз – це найважливіша процесуальна форма застосування спеціальних знань [1].

Судова експертиза – це процесуальна дія, що полягає у фаховому розгляді й дослідженні об'єктів, пов'язаних із розслідуванням справи, із метою отримання об'єктивних висновків та встановлення істини [71, с. 331].

Закон України від 25 лютого 1994 року «Про судову експертизу» (далі – Закон) визначає, що судова експертиза – це дослідження на основі спеціальних знань у галузі науки, техніки, мистецтва, ремесла тощо об'єктів, явищ і процесів із метою надання висновку з питань, що є або будуть предметом судового розгляду [97].

Статтею 7–1 Закону встановлені підстави проведення судової експертизи. Відповідно до цих законодавчих положень підставами для проведення судової експертизи є відповідне судове рішення чи рішення органу досудового розслідування, або договір з експертом чи експертною установою – якщо експертизу проводять на замовлення інших осіб.

Щодо тематики нашого дослідження стосовно кримінальної відповідальності за незаконні дії з шкідливими програмними засобами порядок призначення й проведення відповідних експертиз встановлено Кримінальним процесуальним кодексом України.

Стаття 69 КПК України визначає поняття експерта в кримінальному провадженні як «особи, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України «Про судову експертизу» на проведення експертизи і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та надати висновок із питань, які виникають під час кримінального провадження і стосуються сфери її знань» [67, с. 53].

Така сама кримінально процесуальна норма регламентує права та обов'язки експерта при проведенні експертиз і визначає категорію осіб, які не можуть бути експертами.

Судовими експертами можуть бути особи, які мають необхідні знання для надання висновку з досліджуваних питань. Судовими експертами державних спеціалізованих установ можуть бути фахівці, які мають відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста, пройшли відповідну підготовку та отримали кваліфікацію судового експерта з певної спеціальності. Також закон установлює, що судові експерти, які не є працівниками державних спеціалізованих установ, можуть залучатися до проведення судових експертиз за умови, що вони мають відповідну вищу освіту, освітньо-кваліфікаційний рівень не нижче спеціаліста, пройшли відповідну підготовку в державних спеціалізованих установах Міністерства юстиції України, атестовані та отримали кваліфікацію судового експерта з певної спеціальності [95].

Атестовані судові експерти занесені до державного реєстру атестованих судових експертів, ведення якого покладається на Міністерство юстиції України відповідно до ст. 1 Закону України «Про наукову і науково-технічну експертизу» від 10 лютого 1995 року [94].

Аналіз наведених положень дає підстави зробити висновок, що до статті 69 КПК України своєчасно не було включене й не увійшло положення, яке визначає одну з найважливіших ознак поняття «експерт», а саме вказівка на те, що експерт має бути включеним до державного реєстру атестованих судових експертів. Саме це робить підготовлені ним висновки легітимними.

У зв'язку з викладеним, пропонуємо доповнити статтю 69 КПК України вказівкою щодо встановлення такої вимоги до статусу судового експерта як його приналежність до державного реєстру атестованих судових експертів. Кримінально процесуальними нормами (статтями 242–244 КПК) регламентовані підстави проведення експертизи, а також порядок залучення експерта й інші, пов'язані з цим питання.

Положення щодо висновку експерта та його змісту врегульовані статтями 101, 102 КПК. Водночас чинний КПК України не визначає такого важливого для кримінального судочинства положення, як поняття судової експертизи. У теорії кримінального процесу судову експертизу визначають як процесуальну дію, яка полягає в дослідженні експертом за дорученням сторін кримінального провадження або суду речових доказів та інших матеріалів із метою встановлення фактичних даних та обставин, які мають значення для правильного прийняття рішення за матеріалами кримінального провадження [117, с. 203].

Зазначена процесуальна дія полягає в проведенні досліджень різних об'єктів за дорученням слідчого або суду відповідними фахівцями й надання висновку про результати цих досліджень. Метою такого **дослідженні є встановлення фактичних даних та обставин, що мають значення для правильного вирішення кримінального провадження.**

Використовуючи отримані відомості, ми спробували сформулювати власне визначення поняття судової експертизи. На наш погляд, для більш докладного визначення кримінально процесуальних понять було б доцільним

доповнити КПК України статтею 242–1 «Судова експертиза» з вище визначеним змістом.

Експертне дослідження оформлюють мотивованим висновком експерта, у якому описано хід дослідження й надано відповіді на поставлені запитання. Отриманий висновок є доказом, що свідчить про наявність чи відсутність фактичних даних, необхідних для вирішення того чи іншого питання або стає підставою для судового розгляду [130].

Розглядані положення більшою мірою висвітлюють загальні питання щодо використання спеціальних знань у процесі кримінальних проваджень. Ці самі питання, у ситуаціях, коли йдеться про розслідування правопорушень, пов’язаних зі створенням із метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, мають свої особливості, на дослідженні яких слід зосередитися.

При розслідуванні комп’ютерних злочинів слідчий огляд зазвичай повинен проводитися на місці: збереження й обробки комп’ютерної інформації, підданої злочинному впливу (наприклад, у разі незаконного втручання в роботу ЕОМ (комп’ютерів), їх систем чи комп’ютерних мереж); знаходження комп’ютерного обладнання, яке використовувалося при вчиненні злочину (наприклад, у разі шкідливого програмного засобу після незаконного проникнення в комп’ютерну мережу); збереження інформації, отриманої злочинним шляхом (наприклад, у разі заволодіння комп’ютерною інформацією шляхом викрадення, привласнення, вимагання, шахрайства чи зловживання службовим становищем); порушення правил експлуатації ЕОМ, комп’ютерної системи або мережі; настання шкідливих наслідків (знищення, блокування, модифікації, копіювання комп’ютерної інформації, порушення роботи комп’ютера, комп’ютерної системи або мережі [108, с. 77–78].

Окремі вимоги варто висувати щодо складу слідчо-оперативної групи, яку повинен очолювати слідчий, що спеціалізується на проведенні досудового розслідування в кримінальних провадженнях цієї категорії. До складу групи має входити оперативний працівник підрозділу боротьби зі злочинами у сфері

комп'ютерних технологій та оперативний працівник, якому ввірена територія або об'єкт, який є місцем події. З огляду на специфіку об'єктів, що мають бути оглянуті в ході слідчої дії, кількість спеціалістів не повинна обмежуватися лише спеціалістом-криміналістом, до завдань якого входитиме надання допомоги у виявленні та фіксації слідів. Слідчо-оперативну групу може бути підсилено спеціалістом у сфері інформаційних технологій, допомога якого полягатиме в роботі з комп'ютерними об'єктами. У разі складного і багатооб'єктного місця події, де відбуваються динамічні зміни в обстановці, обов'язки з відеодокументування чи фотозйомки варто покласти на спеціально залученого для цього криміналіста. До специфічних завдань огляду місця події можна віднести огляд і вилучення документів та інформації з автоматизованих охоронних систем відеоспостереження й контролю доступу до місця події та до електронно-обчислювальних машин, а також пошук, виявлення, огляд, фіксацію й вилучення в разі наявності такої потреби спеціальних технічних пристроїв, що призначені або пристосовані й запрограмовані для негласного отримання, знищення, копіювання чи модифікації або блокування комп'ютерної інформації [4, с. 92].

На підготовчому етапі слідчої дії слідчий повинен поінструктувати спеціаліста щодо сутності слідчої дії, яка готується, його окремих завдань, правил поведінки на місці проведення слідчої дії та доручити йому перевірити готовність спеціальних засобів, що будуть застосовуватись при збиранні слідів. Оскільки при проведенні більшості слідчих дій слідчий отримує доступ до інформації, яка часто належить до відомостей з обмеженим доступом, зокрема персональних, слід попередити спеціаліста про недопустимість розголошення відомостей, що стали йому відомі в ході участі в досудовому слідстві.

Перед тим, як безпосередньо розпочати огляд, слідчий ознайомлює спеціаліста з поясненнями або протоколами допитів, вилученою документацією і її копіями. Складають та обговорюють план проведення огляду (як безпечно для збереження комп'ютерної інформації ввійти

до приміщення, відключити комп'ютери від мережі, припинити їхню роботу тощо) [84, с. 6].

Необхідність проведення судових експертиз у досудовому розслідуванні відповідної категорії кримінальних проваджень зумовлена насамперед тим, що предмети й об'єкти, які використовувались для реалізації злочинного умислу, потребують в дослідженні застосування спеціальних знань, котрими не може володіти суб'єкт здійснення досудового розслідування (наприклад, слідчий чи прокурор, котрий також має право на проведення окремих слідчих (розшукових) дій), водночас необхідно підкреслити, що інформаційно-трасологічні експертизи, наприклад, здебільшого можуть надати широке коло відомостей про картину вчинення несанкціонованого проникнення до програмного забезпечення тієї чи іншої інформаційної системи чи обладнання, що забезпечує її функціонування.

М. П. Климчук звертає увагу на те, що судова комп'ютерно-технічна експертиза є однією з найбільш розповсюджених під час здійснення досудового розслідування кримінальних правопорушень відповідної категорії, оскільки її проведення дозволить визначити статус об'єкта посягання (конкретний комп'ютерний пристрій), детально дослідити цей об'єкт не лише з технічного погляду, а й крізь призму його функцій і призначення, що дозволить отримати доступ до інформації, яку він зберігає або якою оперує. За такої умови дослідник пропонує об'єкти відповідного виду експертизи класифікувати на такі: апаратні; програмні; інформаційні (дані) [47]. На нашу думку, така класифікація більш детально дозволить слідчому ознайомитись із технічними та експертними можливостями вилучення доказової інформації в установленому законодавством України порядку,

оскільки без наявності такої інформації неможливим буде притягнення до кримінальної відповідальності відповідних осіб.

Проведення (чи то призначення) будь-якого експертного дослідження характеризоване тим, що для здійснення цієї дії в особи, яка володіє певним видом спеціальних знань, має бути не лише розуміння системи процесу, а й формальний дозвіл на проведення відповідного типу (виду) експертного дослідження.

Крім цього, як звертає увагу А. Білоусов, необхідність та потреба в дослідженні комп'ютерної техніки та іншого інформаційно-телекомунікаційного обладнання зумовлена потребою в дослідженні всіх обставин і деталей злочинної поведінки, що притаманна конкретному кримінальному правопорушенню. Мета в такому випадку є однозначним критерієм, від повноти встановлення якої (і, власне, її меж) залежить кінцевий результат досудового розслідування, тоді як поточні факти й обставини є її складниками (як от: місце зберігання ШПЗ, спосіб його створення, спосіб розповсюдження, міра й обсяг шкоди який було завдано) [15, с. 177]. Практика правозастосування вказує на те, що постановлені судами України вироки за вчинення кримінальних правопорушень, передбачених статтею 361–1 КК України, свідчать, що за всіма без винятку провадженнями призначали судову телекомунікаційну або судово-комп'ютерно-технічну експертизи. Висновки цих експертиз визнані судами як основні докази винності засуджених осіб, і судді посилались на них у своїх вироках. У деяких випадках судді не обмежувалися оголошенням висновків експертиз, а й викликали експертів на судові засідання для надання пояснень за раніше складеними висновками.

У цьому контексті слід зазначити, що суб'єктами використання спеціальних знань можуть бути слідчий, спеціаліст, експерт. Учені наголошують на тому, що при проведенні розслідувань у кримінальних

провадженнях про комп’ютерні злочини необхідним є залучення фахівців експертної служби, які мають повний набір технічного й унікального службового програмного забезпечення для організації успішного розслідування та призначення особливого роду експертиз, які отримали назву комп’ютерно-технічних [118].

Таким чином, типові тактичні операції при розслідуванні створення, використання, розповсюдження або збуту шкідливих програмних засобів утворюють комплекс слідчих заходів, які призначені для з’ясування дійсності злочинного посягання, обставинах його вчинення й осіб, які стосуються злочину, що розслідують. Відповідно, узагальнення наукової теорії і слідчої практики формує найбільш характерні тактичні операції, які, окрім загальних для розслідування злочинів, зокрема таких, як огляд, обшук, виїмка, також характеризуються обов’язковим залученням фахових комп’ютерно-технічних експертів, яких залучають із метою використання вузькоспеціалізованих знань для виявлення об’єктивної сторони злочину й слідової характеристики особливостей його вчинення.

Висновки до розділу 3

У розділі проаналізовано основні засади проведення слідчих (розшукових) дій і використання спеціальних знань у процесі здійснення досудового розслідування відповідного кола кримінальних правопорушень. Доведено, що залежно від поставлених перед слідством завдань, змісту, сутності, а також форми й мети кримінально караного діяння, залежить тип і вид слідчих (розшукових) дій, що обирають до проведення, а також їх порядок і черговість. Проведення слідчих (розшукових) дій слідчим має здійснювались виключно в порядку черговості, а також з урахуванням слідчої обстановки й необхідності, що, зі свого боку, базується не лише на формальних вимогах законодавства України до проведення конкретної дії, а й на професійному рівні відповідного суб'єкта.

Тактика проведення слідчих (розшукових) дій залежить від конкретних обставин вчинення злочину, запланованих слідчим заходів щодо 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 дій, спрямованих на збирання й дослідження доказів, установлення об'єктивної істини по справі та прийняття у кримінальному провадженні обґрунтованого рішення.

Для більшої деталізації кримінально-процесуальних понять доцільно доповнити КПК України новою ст. 242-1 «Судова експертиза» такого змісту: судова експертиза – процесуальна дія, що складається з проведення досліджень експертом, який відповідає вимогам, визначеним Законом України «Про судову експертизу», та зарахований до державного реєстру атестованих судових експертів із питань, вирішення яких потребує спеціальних знань в галузі науки, техніки, мистецтва, і які поставлені перед експертом судом, суддею, слідчим або прокурором із метою встановлення

обставин, що підлягають доказуванню за конкретним провадженням і наданням висновку за результатами дослідження.

ВИСНОВКИ

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

2. Обґрунтування криміналістичної класифікації кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів полягає в тому, що на нашу думку, кримінальним правопорушенням у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів у авторському розумінні слід вважати винне кримінально каране діяння, учинене одноосібно чи групою осіб із метою нанесення негативних наслідків іншому комп'ютерному програмному забезпеченню для отримання матеріальної вигоди чи іншого нематеріального задоволення, яке нанесло матеріальні чи інші нематеріальні збитки охоронюваним законом інтересам шляхом порушення функцій програмного чи інформаційно-комунікативного забезпечення комп'ютерного обладнання, а також комунікативних мереж і електронних накопичувальних пристроїв.

3. Визначення основних джерел криміналістично значущої інформації під час досудового розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів дало підстави обґрунтувати низку тез щодо відповідного питання.

Ґрунтовний аналіз елементів обстановки вчинення таких злочинів дав змогу ранжувати шкідливі програмні засоби на такі видів: комп'ютерні віруси, що являють 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, що 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 в диспозиції статті міститься безпосередня вказівка на шкідливі програмні засоби. Безпосереднє дослідження та 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.

4. Під поняттям способу вчинення злочинів у сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів слід розуміти інформаційно-технічний захід, учинений шляхом застосування програмних розробок шкідливого програмного забезпечення у вигляді створення, копіювання, оптимізації самовідтворення та інкорпорації в програмне забезпечення або його розповсюдження з використанням можливостей програмних комп'ютерних мереж.

Спосіб учинення кримінального правопорушення, слідові картина, особа злочинця та предмет безпосереднього посягання складають структуру криміналістичної характеристики. Криміналістична класифікація таких злочинів базована на міждисциплінарному науково-практичному досвіді не тільки загальноюридичних, але й спеціальноюридичних 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 як комп'ютерні злочині потребують компаративного структурного аналізу.

Спосіб учинення кримінального правопорушення, що досліджується, пов'язаний із технологічними особливостями створення, використання, розповсюдження шкідливих програмних засобів та може бути класифікований за різними підставами, які в подальшому будуть мати значення для криміналістичної характеристики. Основна класифікація ґрунтована на розподілі всіх способів на дві основні групи: активні і пасивні.

5. Існування кореляційної залежності у зв'язках між способом учинення й особою, що вчинила кримінальне правопорушення, між місцем, часом учинення й особою правопорушника, а також механізмом слідоутворення та іншими структурними елементами криміналістичної характеристики кримінального правопорушення дають підстави для визначення предмета безпосереднього посягання, яким виступають шкідливі програмні засоби, системне програмне забезпечення, програмні блоки та окремі програми, створені спеціально 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.

6. Сформовано криміналістичний «портрет» правопорушника, який учиняє злочини, пов'язані з використанням шкідливих програмних засобів. Установлено, що він являє собою фізичну осудну особу, яка досягла шістнадцятирічного 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.

7. Типові слідчі ситуації та напрямки їх розв'язання при розслідуванні злочинів зумовлюють відповідну черговість проведення слідчих дій та інших тактико-криміналістичних заходів розслідування такого виду злочинів. Серед цих заходів найбільш суттєве значення мають такі напрями, як отримання та аналіз доказів, що пов'язані зі 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 в тому, що під час розслідування злочинів, що вчинені з використанням комп'ютерів, їхніх систем та іншої електронної техніки слідчий має справу як з 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 дає змогу конкретизувати процес збирання доказів, визначивши найбільш доцільне в окремій слідчій ситуації проведення слідчих (розшукових) дій, негласних слідчих (розшукових) дій та інших заходів у певній послідовності.

8. Проаналізувавши засади криміналістичного версіювання в досудовому розслідуванні кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, автор обґрунтовує позицію про те, що криміналістична характеристика злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів являє собою результати аналізу складників, які відображають характерні особливості такого злочину, відмежовуючи його

від суміжних злочинів шляхом критеріальних ознак та вимагає компаративного структурного аналізу. Такі ознаки й формують структуру криміналістичної характеристики досліджуваного злочину, зокрема, до них зараховують: 1) спосіб вчинення злочину; 2) слідова картина; 3) особа злочинця; 4) предмет безпосереднього посягання. Така структура може слугувати інформаційною базою для висування версій у кримінальних провадженнях про зазначені види злочинів. Усі ці складники 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 створюватися різноманітні слідчі ситуації. Обґрунтовано позицію про те, що побудова версій проводиться слідчим безперервно, у мірі надходження до нього інформації. Навіть на початковому етапі розслідування, оглядаючи місце події, члени СОГ зобов'язані обмінюватися інформацією, що дає змогу висувати для тактичного відпрацювання нові версії або відмовитися від раніше висунутих.

9. Тактика проведення слідчих (розшукових) дій залежить від конкретних обставин учинення злочину, зумовлених слідчими ситуаціями, висунутих слідчих версій, запланованих слідчих заходів щодо встановлення осіб (особи), що вчинили (вчинила) 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 й дослідження доказів, установлення об'єктивної істини по справі та прийняття в кримінальному провадженні обґрунтованого рішення.

Здійснюючи досудове розслідування злочинів зазначеної категорії, слідчому необхідно проводити низку слідчих (розшукових) дій (призначення експертиз, проведення оглядів, обшуків), 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).

10. Досягнуто висновку, що застосування спеціальних знань у процесі досудового розслідування відповідної категорії кримінальних правопорушень є вкрай 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 при дослідженні 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). Розглядані положення здебільшого висвітлюють загальні питання щодо використання спеціальних знань у процесі кримінальних проваджень. Ці самі питання в ситуаціях, коли йдеться про розслідування правопорушень, пов'язаних зі створенням із метою використання, розповсюдження або збуту, а також розповсюдження або збут шкідливих програмних чи технічних засобів, мають свої особливості, на дослідженні яких слід зосередитися.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Артеменко О.В. URL: http://dspace.nubip.edu.ua:8080/jspui/bitstream/123456789/2223/1/Artemenko_problemi.pdf.

2. Архіпова К. С. Загальна характеристика окремих видів комп'ютерних злочинів. *Нові технології : Науковий вісник КУЕІТУ*. № 1 (35). 2012. С. 78–81.

3. Березняк В. С., Павлова Н. В., Чаплинський К. О. Концептуальні засади методики розслідування кримінальних правопорушень{ у сфері нерухомості: теорія та практика: монографія / Київ. Одеса: Видавничий дім «Гельветика», 2022. 352с.

4. Белоусов А. С. Особенности производства отдельных следственных действий по преступлениям, связанным с нарушением авторских и смежных прав. *Сборник научных работ. Компьютерная преступность и кибертерроризм. Исследование. Аналитика*. Выпуск 1. Запорожье, 2004. С. 88–95.

5. Біленчук П. Д., Романюк Б. В., Цимбалюк В. С. Комп'ютерна злочинність: навчальний посібник. Київ : Атіка, 2002. 240 с.

6. Біленчук П. Д. Комп'ютерні злочини. Київ, 1994. С. 15.

7. Біленчук П. Д. Питання соціальної та криміналістичної характеристики комп'ютерного злочинця. URL: http://www.crime-research.org/library/Bilen3.htm.

8. Біленчук П. Д. Портрет комп'ютерного злочинця. Київ, 1997. 48 с.

9. Біленчук П. Д., Гель А. П., Салтевський М. В., Семаков Г. С. Криміналістика (криміналістична техніка) : курс лекцій. Київ : МАУП, 2001. 216 с.

10. Біленчук П. Д., Дубовий О. П., Салтевський М. В., Тимошенко П. Ю. Криміналістика. Підручник. Київ : Атіка, 1998. 416 с.

11. Біленчук П. Д., Лисиченко В. К, Клименко Н. І. Криміналістика : підручник. 2-ге вид., випр. і доп. Київ, 2001. 544 с.

12. Біленчук П., Котляревський О. Основи комп'ютерної криміналістики. Криміналістика. Київ, 1998. С. 364–372.

13. Білоусов А. С. Використання спеціальних знань при розкритті й розслідуванні комп’ютерних злочинів. *Вісник Луганського державного університету внутрішніх справ*. Спеціальний випуск. 2007. № 2. Частина 3. С. 119–126.

14. Білоусов А. С. Криміналістичний аналіз об’єктів комп’ютерних злочинів : автореф. дис... канд. юрид. наук : 12.00.09. Київ, 2008. 19 с.

15. Білоусов А. С. Поняття й сутність спеціальних знань в галузі ком’пютерно-технічної експертизи. *Південноукраїнський правничий часопис*. 2006. № 4. С. 176–178.

16. Борисова Л. В. Поняття і класифікація вихідної інформації про комп’ютерні злочини. *Право і безпека*. Харків, 2002. Вип. 4. С. 45–49.

17. Борисова Л. В., Волкова О. Г. Соціально-психологічна характеристика комп’ютерних злочинців. *Вісник ХДПУ ім. Г. С. Сковороди. Психологія*. Вип. 9, 2002 С. 55–60.

18. Бутузов В. М. До питання специфіки протидії комп’ютерній злочинності URL: http://nbuv.gov.ua/portal/soc_gum/bozk/ Шех^ 18_ 29.htm.

19. Бутузов В. М., Остапець С. Л., Шоломенцев В. П. Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку. Науково-практичний коментар. Київ, 2005.

20. Використання електронних (цифрових) доказів у кримінальних провадженнях: метод. реком. / [М. В. Гуцалюк, В. Д. Гавловський, В. Г. Хахановський та ін.]; за заг. ред. О. В. Корнейка. Вид. 2-ге, доп. Київ : Вид-во Нац. акад. внутр. справ, 2020. 104 с.

21. Використання спеціальних знань у розслідуванні та попередженні злочинів. URL: http://4ua.co.ua/pravo/kriminalistika/vikoristannya-spetsialnih-znan-rozsliduvanni-poperedzhenni-zlochiniv.html.

22. Вірусна активність в Україні : Троянці збавляють темп. URL: http://zillya.ua/virusna-aktivnist-v-ukra-ni-troyantsi-zbavlyayut-temp.

23. Волобуєв А. Ф. Криміналістика : навчальний посібник. КНТ. 2011. 504 с.

24. Волобуєв А.Ф. Проблеми розслідування «комп'ютерних» злочинів. *Вісник Університету внутрішніх справ.* 1996. № 1. С. 63–70.

25. Воротніков В. В., Умінський В. В., Пінчук О. І. Способи несанкціонованого доступу до інформаційно-телекомунікаційних систем. *Збірник наукових праць ЖВІНАУ*. 2009. Випуск 2. С. 84–92.

26. Гапотченко Г. М. Удосконалення кримінально-процесуальної діяльності щодо отримання та перевірки інформації про злочини. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* Спеціальний випуск у 2-х частинах. Ч. 2. 2008. № 1. С. 140.

27. Глава 23. Використання спеціальних знань в діяльності органів слідства та дізнання. URL: http://www.um.co.ua/4/4-5/4-53133.html.

28. Голубев В. О., Гавловський В. Д., Цимбалюк В. С. Інформаційна безпека: проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій. Запоріжжя : Просвіта, 2001. 252 с.

29. Голубєв В. О. Розслідування комп'ютерних злочинів. Монографія. Запоріжжя : Гуманітарний університет «ЗІДМУ», 2003. 296 с.

30. Голубєв В. О. Кримінолого-криміналістичні питання розслідування злочинів, що вчиняються за допомогою комп'ютерних технологій. URL: http://www.bezpeka.com/ru/lib/spec/crim/art72.html.

31. Гора В. К., Колесник В. А. Вчинення злочинів у сфері інформаційних технологій та їх криміналістичний аналіз. *Інформаційна безпека людини, суспільства, держави.* № 2 (9). 2012. С. 129–136.

32. Горбаньов І. М. Кримінологічна характеристика особи, що вчиняє порушення авторського права щодо незаконного відтворення та розповсюдження комп'ютерних програм. URL:

http://www.ukrainianpravo.narod.ru/krimnalstika_ta_krimnologya/krimnologchna_harakteristiki_osobi_scho_.

33. Горбаньов І. М. Особливості методики розслідування порушень авторського права щодо незаконного відтворення та розповсюдження комп'ютерних програм : дис... канд. юрид. наук: 12.00.09. Академія адвокатури України. Київ, 2007. 240 с.

34. Гребенюк М. В., Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. Використання електронних (цифрових) доказів у кримінальних провадженнях : В 43 метод. рек. Київ : МНДЦ при РНБО України, 2017. 76 с.

35. Гуцалюк М. В., Гавловський В. Д., Хахановський В. Г. Використання електронних (цифрових) доказів у кримінальних провадженнях : методичні рекомендації. Київ : Вид-во Національної академії внутрішніх справ, 2020. 104 с.

36. Даньшин І.М, Голіна В. В., Валуйська М. Ю. Кримінологія : Загальна та Особлива частини : підручник. Харків : Право, 2009. 288 с.

37. Диденко В. П. Тактические приемы применения киносъемки на предварительном следствии. *Криминалистика и судебная экспертиза*. 1975. № 11. С. 91–97.

38. Документ A/CONF.17/20 // Доповідь Другого конгресу ООН із запобігання злочинності й поводженню з правопорушниками (Лондон, 8–19 серп. 1960 р.).

39. Доповнення до Кримінального кодексу України від 23.12.2004 р. № 286-IV. URL: http://zakon2.rada.gov.ua/laws/show/2341-14.

40. Духов В. Е. Экономическая разведка и безопасность бизнеса. Киев : ИМСО МО Украины, 2000. 96 с.

41. Європіна І. В. **Види протиправних діянь у сфері новітніх інформаційних технологій.** ***Вісник Академії адвокатури України*****. № 3(19) 2010. С. 129–136.**

42. Європіна І. В. Слідча ситуація та її роль у розслідуванні злочинів, які вчинюються з використанням комп’ютерів. *Вісник Академії адвокатури України*. 2 (21). 2011. С. 159–171.

43. Карчевський В. М. Злочини у сфері використання комп’ютерної техніки: навчальний. посібник. Луганський державний університет внутрішніх справ. Луганськ, 2006. 192 с.

44. Карчевський М. В. Кримінальна відповідальність за незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (аналіз складу злочину) : Дис... канд. юрид. наук: 12.00.08. Національна юридична академія України ім. Я. Мудрого. Харків, 2003. 175 с.

45. Кіберзлочинність в Україні зростає : дані звіту Price Waterhouse Coopers. URL: http://ladynews.com.ua/newsline/kiberprestupnost-v-ukraine-nabiraet-oboroty-96603.html.

46. Клименко Н. І., Колонюк В. П. Роль експертизи в захисті об’єктів інтелектуальної власності. *Теорія та практика судової експертизи і криміналістики*. Збірник науково-практичних матеріалів (до 80-річчя заснування Харківського НДІ судових експертиз) Випуск № 3. Харків : Право, 2003. С. 554–559.

47. Климчук М. П., Коміссарчук Ю. А., Марко С. І., Стецик Б. В. Судова комп’ютерно-технічна експертиза у кримінальному провадженні : навчальний посібник. Львів : Львівський державний університет внутрішніх справ, 2022. 112 с.

48. Коваленко В. В., Анапольська А. І. Розслідування шахрайств та пов’язаних із ними злочинів, вчинених у сфері функціонування електронних розрахунків: монографія. МВС України, ЛДУВС ім. Е. О. Дідоренка. Луганськ : РВВ ЛДУВС ім. Е.О. Дідоренка, 2013. С. 85.

49. Коваленко М. М. Комп’ютерні віруси і захист інформації. Київ : Наукова думка, 1999. С. 138–143.

50. Кожевников Г., Бабенко В., Громыко Т. Участие специальных понятых при расследовании преступлений, связанных с компьютерами. *Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні* : науково-технічний збірник. Київ, 2004. Вип. 8. 165 с.

51. Козак Н. С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : автореф. дис. ... канд. юрид. наук : 12.00.09. Національний університет державної податкової служби України. Ірпінь, 2011. 18 с.

52. Козак Н. С. Техніко-криміналістичні засоби та прийоми виявлення і розслідування комп'ютерних злочинів. *Підприємництво, господарство і право.* 2012/2. № 12. С. 90–93.

53. Козак Н. С., Цимбал П. В., Данкович Н. О., Криміналістичні аспекти виявлення комп'ютерних злочинів. *Науковий вісник Національного університету ДПС України (економіка, право)*. 2010. № 4 (51). С. 252–258.

54. Колесник В. А., Гора І. В., Костін М. І. Розслідування комп'ютерних злочинів : науково-методичний посібник. К. : Вид-во НА СБ України, 2003. 124 с.

55. Компьютерная преступность в США. *Проблемы преступности в капиталистических странах*. 1990. № 9. С. 3–5.

56. Компьютерная преступность в Швейцарии : формы проявления и характеристика преступников. *Проблемы преступности в капиталистических странах*. 1987. № 9. С. 5– 10.

57. Копча В. В., Човганин М. І., Правове використання спеціальних знань у кримінальному судочинстві. юридичні підстави щодо проведення судових експертиз. URL: https://dspace.uzhnu.edu.ua/jspui/bitstream/lib/41326/1/%D0%9F%D0%A0%D0%90%D0%92%D0%9E%D0%92%D0%95%20%D0%92%D0%98%D0%9A%D0%9E%D0%A0%D0%98%D0%A1%D0%A2%D0%90%D0%9D%D0%9D%D0%AF%20%D0%A1%D0%9F%D0%95%D0%A6%D0%86%D0%90%D0%9B%D0%AC%D0%9D%D0%98%D0%A5.pdf.

58. Криміналістика: навчальний посібник / за заг. ред. Є.В. Пряхіна. Львів: ЛьвДУВС, 2010. 540 с.

59. Криминалистика : Специализированный курс. Под ред. М. В. Салтевского. Киев, 1987. 307 с.

60. Криміналістика. Підручник. Київ : Центр учбової літератури. 2015. 543 с.

61. Кримінальне право України. Загальна частина. Київ : Атіка. 2008. 104 с.

62. Кримінальне право України. Загальна частина. Підручник. Київ : «Правові джерела». 2002. 425 с.

63. Кримінальне право України. Особлива частина. Київ : Атіка. 2008. 711 с.

64. Кримінальне право України. Практикум. Навчальний посібник. К. КНТ. 2006. 431 с.

65. Кримінальний кодекс України : Закон України від 5 квіт. 2001 р. № 2341-III (розділ 1). URL: https://zakon.rada.gov.ua/laws/card/2341-14.

66. Кримінальний кодекс України. Кримінально-процесуальний кодекс України. Постанови Пленуму Верховного Суду України із загальних питань судової діяльності та в кримінальних справах. Київ : Юрінком Інтер, 1999. 318 с.

67. Кримінальний процесуальний кодекс України. Київ : Паливода. 2017. 402 с.

68. Кузнецов В. В. Кримінальна відповідальність за крадіжки : монографія. Київ, 2005. С. 79–105.

69. Куркін В. О, Мотлях О. І. Типові криміналістичні ситуації у розслідуванні організованої злочинної діяльності. *Вісник Академії праці і соціальних відносин ФП України*, 2004. № 2 (26). С. 22–24.

70. Лісовий В. В. Комп'ютерні злочини : питання кваліфікації. *Право України*. 2002. № 2. С. 86–88.

71. Марусь В. О. Криміналістика : навчальний посібник. Київ : Кондор, 2007. 558 с.

72. Мельник М. І., Хавронюк М. І. Науково-практичний коментар кримінального кодексу України. Київ : А.С.К., 2003. 976 с.

73. Міхайліна Т. В. Особливості кваліфікації злочинів, передбачених ст.361–1 кримінального кодексу України. *Вісник Донецького національного університету*. Серія В. Економіка і право. 2008. № 2. С. 459–464.

74. Моїсеєв О. М. Залучення спеціаліста до розслідування комп'ютерних злочинів. *Правові основи захисту комп'ютерної інформації від протиправних посягань* : Матеріали міжвузівської науково-практичної конференції. Донецьк, 2001, С. 81.

75. Мотлях О. І. Питання методики розслідування злочинів у сфері інформаційних комп'ютерних технологій : дис... канд. юрид. наук: 12.00.09. Академія адвокатури України. Київ, 2005. 221 с.

76. Мотлях О. І. Проведення огляду місця події у злочинах, що скоюються за допомогою комп'ютерних технологій. URL: https://www.socosvita.kiev.ua/sites/default/files/Visnyk_2006_2-p3_100.pdf.

77. Науково-практичний коментар Кримінального кодексу України. За ред. М. І. Мельника, М. І. Хавронюка. Київ : Наукова думка, 2007. 1184 с.

78. Науково-практичний коментар кримінального кодексу України. Київ : Юридична думка. 2007. 1181 с.

79. Научно-практический комментарий Уголовного кодекса Украины от 5 апреля 2001 года. Под ред. Н. И. Мельника, Н. И. Хавронюка. Киев : Изд-во А.С.К., 2004. 1216 с.

80. НБУ повідомив про незаконні операції з платіжними картками. URL: https://finpost.com.ua/news/6909.

81. Новий тлумачний словник української мови. Видавництво «АКОНІТ» Київ. 2001. Т. 3 С. 862.

82. Обнорський В. І. Комп'ютерні злочини – способи та види. *Інформаційний бюлетень*. 2000. № 2. С.14–20.

83. Огляд місця події при розслідуванні «комп'ютерних» злочинів. URL: http://expertprava.ucoz.ru/index/0-34.

84. Осмотр компьютерных средств на месте происшествия : метод. рекомендации / Отв. ред. М. В. Салтевский. Харьков, 1999. С. 6.

85. Офіційний веб-сайт Генеральної прокуратури України. URL: https://www.gp.gov.ua/ua/statinfo.html.

86. Паламарчук Л. П. Криміналістична характеристика осіб, які скоюють злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Бюлетень Міністерства юстиції України*. 2004. № 8. С. 100–106.

87. Паламарчук Л. П. Криміналістичні заходи запобігання незаконному втручанню в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. *Часопис Київського університету права.* 2004. № 2. С. 66–71.

88. Пархоменко І. І., Молодан Б. О. Сучасні вірусні загрози для комп'ютерних систем сімейства операційних систем windows. *Наукоємні технології*, 2009. № 3–4 (7–8). С. 73–76.

89. Пашнєв Д. В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : автореф. дис. на здобуття наук. ступеня канд. юрид. наук : спец. 12.00.09. Кримін. процес та криміна л.; судова експ. Харків, 2007. 20 с.

90. Пашнєв Д. В. Криміналістична класифікація комп'ютерних злочинів URL: http://archive.nbuv.gov.ua/portal/soc_gum/Kyuv/2009_1/1-5/13.pdf.

91. Пашнєв Д. В. Особливості виявлення і фіксації криміналістично значимої комп'ютерної інформації при розслідуванні злочинів. *Право і безпека*. 2003. № 1. С. 108–111.

92. Пашнєв Д. В., Рудик М. В. Особливості виявлення та кримінально-правова кваліфікація злочинів, що посягають на комп'ютерну інформацію з обмеженим доступом. *Ученые записки Таврического*

национального университета им. В. И. Вернадского Серия «Юридические науки». Т. 22 (61). № 1. 2009. С. 232.

93. Про внесення змін до Закону України «Про авторське право та суміжні права»: Закон України від 11 липня 2001р. *ВВРУ*. 2001. № 43. Ст. 214.

94. Про наукову і науково-технічну експертизу: Закону України від 10 лютого 1995 року. Відомості Верховної Ради України (ВВР), 1995, № 9. Ст. 56. Від 10 лютого 1995 року. № 51/95.

95. Про судову експертизу : Закон України від 25 лют. 1994 р. № 4038-XII. URL: http://zakon5.rada.gov.ua/laws/show/4038-12.

96. Про судову експертизу: Закон України від 25 лютого 1994 року № 4038-XII. Відомості Верховної Ради України (ВВР), 1994. № 28. Ст. 232.

97. Прутяний С. О. Класифікація комп'ютерних злочинів, які вчиняються кримінальними професіоналами. URL: http://www.lex-line.com.ua/?go=full_article&id=827.

98. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : дис... канд. юрид. наук : 12.00.08. НАН України; Інститут держави і права ім. В. М. Корецького. Київ, 2003. 222 с.

99. Романюк Б. В., Гавловський В. Д., Гуцалюк М. В. Виявлення та розслідування злочинів, що вчиняються у сфері інформаційних технологій : науково-практичний посібник. Київ, 2001. С. 95–96.

100. Сабадаш Р. В. Застосування спеціальних знань при розслідуванні злочинів у сфері комп'ютерної інформації: поняття, суб'єкти та цілі. *Науковий вісник Чернівецького університету*. *Правознавство*. 2011. Випуск 578. С.109 –113.

101. Салтевский М. В., Щербаковский М. Г., Губанов В. А. Осмотр компьютерных средств на месте происшествия : методическое пособие. Харьков : Академия правовых наук Украины, НИИ изучения проблем преступности, 1999. 11 с.

102. Салтевський М. В. Основи методики розслідування злочинів, скоєних з використанням ЕОМ : навчальний посібник. Харків : Національна юридична академія України. 2000. 35 с.

103. Салтевський М. В. Криміналістика (у сучасному викладі) : підручник. Київ : Кондор, 2005. С. 419.

104. Самойленко О. А. Особливості початкового етапу розслідування викрадень майна, вчинених із використанням комп'ютерних технологій. *Держава і право : Збірник наукових праць. Юридичні і політичні науки*. Київ : Ін-т держави і права ім. В. М. Корецького НАН України, 2006. Вип. 31. С. 423–428.

105. Скригонюк М. І. Криміналістика : підручник. Київ : Атіка, 2005. 496 с.

106. Следственная ситуация и тактическое решение. URL: https://bstudy.net/909161/pravo/sledstvennaya_situatsiya_takticheskoe_reshenie.

107. Снігерьов О. П., Голубєв В. О. Проблеми класифікації злочинів у сфері комп'ютерної інформації. *Вісник Університету внутрішніх справ*. 1999. № 5. С. 25–29.

108. Старушкевич А. Організація огляду місця події. Аналіз криміналістично- значимої інформації при розслідуванні злочинів у сфері комп'ютерної інформації. *Вісник прокуратури*. 2003. № 12. С. 77–86.

109. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку. URL: http://www.scourt.gov.ua/clients/vsu/vsu.nsf/(print)/AFB1E90622E4446FC2257B7C00499C02.

110. Тарасенко О. С. Застосування спеціальних знань під час розслідування кримінальних правопорушень, пов'язаних з обігом протиправного контенту в мережі інтернет. URL: https://journal-nam.com.ua/index.php/journal/article/download/560/524.

111. Тарасюк А. В. Актуальні питання тактики проведення окремих слідчих дій при розслідуванні комп'ютерних злочинів. *Інформаційна безпека людини, суспільства, держави*. № 3 (7). 2011. С. 64–70.

112. Тема 5. Особа злочинця. URL: https://mix.sumdu.edu.ua/textbooks/11059/728093/index.html.

113. Тенденції розповсюдження шкідливих програм. URL : http://licasoft.com.ua/index.php/-eset/-esetnews/21008--tendenc-rozpovsudjennia-shkdlivih-program-jovten-2012-.html.

114. Тест на проникновение (Пентест) URL: http:// pentest.com.ua/

115. Типові слідчі ситуації, версії та відповідний їм алгоритм слідчих (розшукових) дій початкового етапу розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютері), систем та комп'ютерних мереж і мереж електрозв'язку. URL: http://4ua.co.ua/pravo/kriminalne/tipovi-slidchi-situatsiyi-versiyi-vidpovidniy-yim-algoritm-slidchih-rozshukovih-diy.html.

116. Уголовный кодекс Украины : научно-практический комментарий. Отв. ред. Е. Л. Стрельцов. Харьков : ООО «Одиссей», 2007. 872 с.

117. Удовенко Ж. В. Криміналістика : конспект лекцій. Київ : «Центр учбової літератури». 2016. 320 с.

118. Усов А. И. Применение специальных познаний при раскрытии и расследовании преступлений, сопряженных с использованием компьютерных средств URL: http://jurfak.sp.ua/conference/1810200Zusov.htm.

119. Фарима М. М. Розслідування торгівлі дітьми або іншої незаконної угоди щодо дитини : автореф. дис. ... канд. юрид. наук : 12.00.09. Національна академія внутрішніх справ. Київ, 2021. 20 с.

120. Федотов О. А. Щодо поняття злочинів у сфері комп'ютерних технологій. *Економіка, фінанси, право*. Вип. 10. № 10. 2010. С. 37–39.

121. Хахановський В. Г. Теорія і практика криміналістичної інформатики : автореф. дис. ... д-ра юрид. наук : 12.00.09. Національна академія внутрішніх справ. Київ, 2011. 28 с.

122. Хахановський В. Г. Особливості криміналістичної характеристики кіберзлочинців. *Юридичний часопис НАВС*. № 1. 2011. URL: http://www.naiau.kiev.ua/chasopis/materials/24.

123. Шадхін В. Ю., Дель Д. Г., Піддубна Я. Ю., Рогальський І. Ю. Дослідження моделей поширення шкідливого коду в комп'ютерно-інтегрованих системах управління. *Технології та дизайн*. № 2 (3). 2012. URL: http://archive.nbuv.gov.ua/e-journals/td/2012_2/12svyisu.pdf.

124. Шилан Н. Н., Кривонос Ю. М., Бирюков Г. М. Компьютерные преступления и проблемы защиты информации : монография. Луганск: РИО ЛИВД, 1999. 60 с.

125. Школьний Б. В. Питання загальної теорії слідоутворення у контексті боротьби з кіберзлочинністю. *Юридична психологія та педагогіка*. 2011 №1 (9). С. 284–287.

126. Шмонин А. В. Современное представление о криминалистической характеристике преступлений. *Следователь*. 2005. № 2. С. 43–49.

127. Щербаковський М. Г., Пашнєв Д. В. Розслідування комп'ютерних злочинів : посібник. МВС України, Харківський національний університет внутрішніх справ. Харків : ХНУВС, 2010. 112 с.

128. Щодобове зведення про вчиненні на території держави кримінальні правопорушення за період з 01.01.2013 по 04.07.2013. Ст. 361-1 КК України.

129. Юридична відповідальність як охоронний засіб. URL: http://obt.inf.ua/page16.html.

130. Юдін О. М., Макарова М. В., Лавренюк Р. М. Системи електронної комерції: створення, просунення і розвиток: монографія. Полтава: РВВ ПУЕТ, 2011. 201 с.

ДОДАТКИ

Додаток А

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ ТА ВІДОМОСТІ ПРО АПРОБАЦІЮ

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.

Додаток Б

АКТИ ВПРОВАДЖЕННЯ МАТЕРІАЛІВ ДИСЕРТАЦІЙНОГО ДОСЛІДЖЕННЯ В ОСВІТНІЙ ПРОЦЕС, НАУКОВУ ДІЯЛЬНІСТЬ ТА ПРАВОЗАСТОСОВЧУ ПРАКТИКУ

ВЕРХОВНА РАДА УКРАЇНИ
ІНСТИТУТ ЗАКОНОДАВСТВА
04053, Київ, пров. Несторівський, 4, тел. 235 96 01, факс. 235 96 05, e-mail:zak_norm@rada.gov.ua

№ 22/108-1-15 „16" 05 2019 р.

АКТ
впровадження у практичну діяльність Інституту законодавства Верховної Ради України результатів дисертаційного дослідження здобувача наукового ступеня кандидата юридичних наук Волкова Олександра Олександровича на тему «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів»

Повідомляємо, що наукові положення, розроблені здобувачем наукового ступеня кандидата юридичних наук Волковим Олександром Олександровичем на тему «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів», можуть бути використані Інститутом законодавства Верховної Ради України при підготовці відповідних законопроектів.

Заслуговують на увагу розроблені Волковим Олександром Олександровичем зміни та доповнення до чинного національного законодавства, зокрема, що потребує доповнень та коригувань стаття 69 (Експерт) Кримінального процесуального кодексу України та доповнення новою статтею 242^{-1}, відповідний кодекс, наступного змісту:

«**Стаття 242-1.** Судова експертиза

Судова експертиза - процесуальна дія, що складається з проведення досліджень експертом, який відповідає вимогам, визначеним Законом України «Про судову експертизу» та зарахований до державного реєстру атестованих судових експертів, з питань, вирішення яких потребує спеціальних знань в галузі науки, техніки, мистецтва, і які поставлені перед експертом судом, суддею, слідчим або прокурором, з метою встановлення обставин, що підлягають доказуванню по конкретному кримінальному провадженню і дачі висновку по результатам дослідження.

Експертне дослідження оформлюється мотивованим висновком експерта, в якому описується хід дослідження і даються відповіді на поставлені питання. Отриманий висновок є доказом, що свідчить про наявність чи відсутність фактичних даних, необхідних для вирішення того чи іншого питання або стає підставою для судового розгляду».

Крім цього автором у дисертаційному дослідженні обґрунтовано необхідність доповнення (викладу в новій редакції) чинної статті 361-1 (Створення з метою протиправного використання, розповсюдження або збуту

шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут) Кримінального кодексу України, а саме:

«**Стаття 361-1.** Створення з метою використання, розповсюдження або збуту шкідливих програмних матеріалів чи технічного обладнання, а також їх використання, розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також використання, розповсюдження або збут шкідливих програмних матеріалів чи технічного обладнання, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до п'яти років».

Наведені вище висновки та рекомендації Волкова Олександра Олександровича взяті до уваги Інститутом законодавства Верховної Ради України і будуть враховуватись при підготовці експертно-аналітичних матеріалів для відповідних Комітетів Верховної Ради України, з метою удосконалення кримінальних і кримінальних процесуальних основ здійснення досудового розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів.

Директор,
академік НАН України **О. Р. Копиленко**

ЗАТВЕРДЖУЮ
Заступник Голови Національної поліції України – начальник Головного слідчого управління, доктор юридичних наук, доцент, заслужений юрист України, генерал поліції третього рангу

Максим ЦУЦКІРІДЗЕ

10 листопада 2022 року

АКТ № 30085

Про впровадження у практичну діяльність Головного слідчого управління Національної поліції України результатів дисертаційного дослідження

Уклала комісія у складі:

Голови: заступника начальника Головного слідчого управління Національної поліції України – начальника управління організації роботи та методичного забезпечення, полковника поліції Сергія Гайду

членів комісії: начальника відділу методичної роботи та правового забезпечення Головного слідчого управління Національної поліції України, кандидата юридичних наук, полковника поліції Владислава Бурлаки

старшого слідчого в особливо важливих справах відділу методичної роботи та правового забезпечення Головного слідчого управління Національної поліції України, доктора філософії з права, майора поліції Максима Романова

комісія відповідно до Положення про організацію проведення НДР і ДКР у системі МВС України, затвердженого наказом МВС України «Про організацію наукової діяльності в системі МВС України» від 15.05.2007 № 154 склала цей акт, щодо розгляду результатів дисертаційного дослідження Волкова Олександра Олександровича на тему: «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» зі

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

Матеріали дисертаційного дослідження, висновки, пропозиції та рекомендації, що запропоновано автором в ньому можуть застосовуватися у практичній діяльності слідчих підрозділів Національної поліції України під час проведення занять в системі службової підготовки, а також при проведенні семінарів, нарад.

У дисертації здійснено комплексне дослідження правових, теоретичних та організаційно-тактичних засад кримінального провадження на початковому етапі розслідування кримінальних правопорушень у сфері створення, використання та розповсюдження шкідливих програмних засобів з огляду на нормативні положення чинного кримінального та кримінального процесуального законодавства України. Сформульовано поняття та сутність злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів. Зважаючи на кримінально-правові положення розроблено і сформульовано поняття шкідливого програмного засобу. 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.

Відповідні матеріали було використано під час підготовки листів-роз'яснень до органів досудового розслідування територіальних органів поліції Національної поліції України, оскільки вони мають як необхідний теоретичний та методологічний рівень, так і практичну цінність, що сприяють вдосконаленню процесуальної діяльності органів досудового розслідування Національної поліції України.

Голова комісії: **Сергій ГАЙДУ**

Члени комісії: **Владислав БУРЛАКА**

Максим РОМАНОВ

ЗАТВЕРДЖУЮ
Перший проректор
Національної академії
внутрішніх справ
д.ю.н., професор
С.Д. Гусарєв

18 05 2018 р.

АКТ
впровадження результатів дисертаційного дослідження здобувача кафедри криміналістики та судової медицини Волкова Олександра Олександровича на тему «Початковий етап розслідування злочинів у сфері створення, використання та розповсюдження шкідливих програмних засобів», підготовленого на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.09 – кримінальний процес та криміналістика; судова експертиза; оперативно-розшукова діяльність до освітнього процесу Національної академії внутрішніх справ

Комісія у складі: начальника відділу організації та координації освітнього процесу, кандидата юридичних наук, лейтенанта поліції Дубівки І.В., завідувача кафедри криміналістики та судової медицини, кандидата юридичних наук, доцента, підполковника поліції Самодіна А.В. та завідувача кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2, кандидата юридичних наук, майора поліції Атаманчука В.М. склала цей акт про те, що наукові роботи, підготовлені Волковим О.О., використовуються у освітньому процесі Національної академії внутрішніх справ.

Результати наукового дослідження знайшли своє відображення у навчально-методичних матеріалах, де як джерела рекомендовані наступні публікації:

1. Волков О. О. Тактичні особливості проведення огляду місця події при розслідуванні розповсюдження, збуту та створення з метою використання, розповсюдження або збуту шкідливих програмних засобів. *Збірник наукових праць*. Херсон: Херсонський юридичний інститут Харківського національного університету внутрішніх справ. 2005. С. 79–83.
2. 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.
3. Волков О. О. До проблеми підготовки фахівців правоохоронних органів по боротьбі з кіберзлочинністю. *Правова інформатика*. 2008. № 1(17). С. 67–77.
4. Волков О. О. Виявлення доказової інформації при розслідуванні створення, використання, розповсюдження і збуту шкідливих програмних засобів. *Інформаційне забезпечення розкриття та розслідування злочинів*. у 3 т. Луганськ: РВВ ЛДУВС. 2008. Спец.вип. № 5. Т.3. С. 158–165.

питань антимонопольної політики. Антимонопольний комітет України, 2018. С. 121–123.

16. Волков О. О. Особливості документування злочинів при організації розслідування кримінальних справ пов'язаних зі створенням, використанням та поширенням шкідливих програмних засобів: (ст.361-1 Кримінального кодексу України): метод. рек. Київ, ГСУ МВС України, 2011. 48 с.

17. Розслідування злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: метод. рек. / М. В Карчевський., М. Ю. Літвінов, А. І. Анапольська , М. О. Яковенко, А. Б. Марченко О. О. Волков та ін.]. / за заг. ред. Ю. Ю. Орлова. Київ: ЛДУВС, 2013. 135 с.

18. Розслідування злочинів, учинених з використанням шкідливих програмних чи технічних засобів: метод. рек. / О. Ф. Вакуленко, О. М. Стрільців, О. С. Тарасенко, О. О. Волков та ін.]. Київ, 2016. 56 с.

19. Особливості розслідування кримінальних правопорушень, пов'язаних із розповсюдженням у мережі Інтернет забороненого контенту: метод. рек. / О. М. Стрільців , В. В. Крижна, О. В. Максименко, О. О. Волков та ін.; за заг. ред. Ю. Ю. Орлова. Київ: ГСУ, Нац. акад. внутр. справ, 2016. 78 с.

Члени комісії дійшли спільного висновку, що представлені матеріали мають належний науковий та практичний рівень розробки проблематики теми дисертаційного дослідження і відображені у науково-методичних матеріалах з навчальних дисциплін: «Криміналістика», «Розслідування окремих видів злочинів» та «Особливості розслідування окремих видів злочинів» для здобувачів вищої освіти бакалавра і магістра, а також можуть використовуватися у системі підвищення кваліфікації слідчих, оперативних працівників та інших категорій практичних співробітників Національної поліції України.

Члени комісії:
Начальник відділу організації та координації освітнього процесу НАВС кандидат юридичних наук лейтенант поліції **І.В. Дубівка**
18 05 2018 р.

Завідувач кафедри криміналістики та судової медицини НАВС кандидат юридичних наук, доцент підполковник поліції **А.В. Самодін**
18 05 2018 р.

Завідувач кафедри криміналістичного забезпечення та судових експертиз навчально-наукового інституту № 2 НАВС кандидат юридичних наук майор поліції **В.М. Атаманчук**
18 05 2018 р.

ЗАТВЕРДЖУЮ
В.о. Президента Науково-дослідного
інституту публічного права,
доктор юридичних наук, професор
Сергій КОРОЄД
11.11.2022 р.

А К Т
впровадження у наукову діяльність результатів дисертаційного дослідження здобувача Науково-дослідного інституту публічного права Волкова Олександра Олександровича на тему: «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів» у науково-дослідну роботу Науково-дослідного інституту публічного права

Комісія в складі: в.о. президента Науково-дослідного інституту публічного права, доктора юридичних наук, професора Короєда Сергія Олексійовича (голова комісії), завідувача аспірантури, доктора юридичних наук, професора Сороки Лариси Володимирівни, завідувача відділу науково-правових експертиз та законопроектних робіт, доктора юридичних наук, старшого дослідника Куркової Ксенії Миколаївни, склала цей акт про те, що матеріали дисертації Волкова Олександра Олександровича на тему: «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів», мають необхідний теоретичний, методологічний рівень, практичну значущість і використовуються в науково-дослідній роботі наукових відділів Наукового дослідного інституту публічного права, зокрема для подальшого розроблення наукових питань щодо правових засад діяльності суб'єктів, що здійснюють заходи в сфері здійснення досудового розслідування Національною поліцією України, а також у межах реалізації Інститутом теми науково-дослідницької роботи «Правове забезпечення прав, свобод та законних інтересів суб'єктів публічно-правових відносин» (номер державної реєстрації 0115U005495).

Використання результатів дисертації сприятиме активізації та підвищенню ефективності наукової роботи працівників відділів та аспірантів Науково-дослідного інституту публічного права.

ВИСНОВОК

Результати дисертації здобувача Науково-дослідного інституту публічного права Волкова Олександра Олександровича на тему: «Початковий етап розслідування кримінальних правопорушень у сфері створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних

засобів» вважати впровадженими у науково-дослідну роботу Науково-дослідного інституту публічного права, під час проведення загальнотеоретичних і галузевих досліджень, спрямованих на вирішення теоретико-методологічних проблем науки кримінального процесу.

Голова комісії: **Сергій КОРОЄД**

Члени комісії: **Лариса СОРОКА**

Ксенія КУРКОВА

Додаток В

Зведені дані анкетування 275 слідчих, що стану обізнаності в методиці розслідування кримінальних справ у злочинах пов'язаних з створенням, використанням, розповсюдженням та збутом шкідливих програмних засобів

Таблиця 1.

Стаж служби в правоохоронних органах

Назва альтернативи	шифр	кількість	%
До 5 років	001	33	12,0
Понад 5 років	002	242	88,0

Таблиця 2.

Стаж практичної роботи

Назва альтернативи	шифр	кількість	%
До 3 років	003	65	23,6
Більше 5 років	004	210	76,4

Таблиця 3.

Наявність досвіду в розкритті та розслідуванні злочинів пов'язаних з виготовленням, розробкою поширенням або збуто шкідливих програмних засобів

Назва альтернативи	шифр	кількість	%
Так	005	21	7,6
Ні	006	254	92,4

Таблиця 4.

По якій причині інформація про створення, використання, розповсюдження або збут шкідливих програмних засобів не повідомляються в правоохоронні органи

Назва альтернативи	шифр	кількість	%
Наявність в своїй діяльності конфіденційної інформації	007	100	36,4

Думка про некомпетентність правоохоронців	008	76	27,6
Наявність в діяльності потерпілого ознак інших протиправних діянь	009	55	20,0
Наявність власних сил і засобів до встановлення осіб і відшкодування завданих збитків	010	11	4,0
Інші причини	011	33	12,0

Таблиця 5.

Які фактори зумовлюють низьку ефективність діяльності правоохоронних органів в цій сфері?

Назва альтернативи	шифр	кількість	%
Новизна таких злочинів, недостатня обізнаність про способи їх вчинення;	012	167	60,7
Відсутність необхідних знань, розуміння технологічного процесу роботи ЕОМ;	013	53	19,3
Відсутність розроблених сучасних методик виявлення та розслідування створення, використання, розповсюдження або збуту шкідливих програмних засобів;	014	0	0
Недостатній рівень використання ОРЗ та оперативного супроводження роботи мереж;	015	6	2,2
Недосконаліть правової бази, регламентує діяльність правоохоронних органів в цій сфері;	016	12	4,4
Недостатній рівень інформаційного забезпечення;	017	0	0
Неефективна взаємодія різних служб та відомств у тому числі на міжнародному рівні;	018	23	8,4
Недостатня професійнакомпетентність та неукомплектованість оперативних працівників;	019	0	0
Необ’єктивна система обліку результатів правоохоронної діяльності та оцінки її результатів;	020	14	5,0

Таблиця 6.

Що на Вашу думку, може сприяти підвищенню професійної майстерності і розслідуванні злочинів пов’язаних з створенням, використанням, розповсюдженням або збутом шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Покращення рівня спеціальної підготовки на базі вищих навчальних закладів;	021	155	56,4

Перепідготовка за різними формами підвищення кваліфікації;	022	54	19,6
Систематичне проведення на базі підрозділу нарад з аналізом недоліків та спільним розглядом окремих проблемних ситуацій, у тому числі за участю прицівників інших відомоств;	023	33	12,0
Видання спеціальної літератури з окремих питань виявлення та розслідування злочинів зазначеної групи;	024	33	12,0

Таблиця 7.

Чи необхідно вивчення цього виду злочинності на рівні злочинної діяльності (подібно слідчої, оперативно-розшукової, судової діяльності)?

Назва альтернативи	шифр	кількість	%
Так	025	222	80,7
Ні	026	53	19,3

Таблиця 8.

Які аспекти такої діяльності слід вивчати:

Назва альтернативи	шифр	кількість	%
Тактичні аспекти: - при підготовці до вчинення злочину; - при протидії розслідуванню;	027	110	40,0
Напрямок і форми функціонування злочинної діяльності;	028	110	40,0
Способу злочинної діяльності:	029	45	16,4
Особу злочинця;	030	0	0
зв’язки і координацію діяльності з зарубіжними злочинними угруповуваннями;	031	10	3,6
Характер матеріально-технічного і фінансового забезпечення злочинної діяльності;	032	0	0

Таблиця 9.

Якими джерелами інформації стосовно таких злочинів ви користуєтесь?

Назва альтернативи	шифр	кількість	%
Обмін досвідом і знаннями з колегами;	033	108	39,3
Особистий досвід;	034	0	0

Літературні джерела;	035	123	44,7
Службова підготовка і підвищення кваліфікації;	036	44	16,0

Таблиця 10.

По яких аспектах такої злочинної діяльності необхідна додаткова інформація?

Назва альтернативи	шифр	кількість	%
Напрями і форми здійснення злочинної діяльності;	037	145	52,7
Тактичні аспекти злочинної діяльності;	038	75	27,3
Зв’язки злочинця;	039	0	0
Особа злочинця;	040	11	4,0
Способи злочинної діяльності;	041	0	0
Міжнародне співрпобітництво і зв’язки злочинця;	042	11	4,0
Характер матеріально-технічного і фінансового забезпечення своєї діяльності;	043	33	12,0

Таблиця 11.

Чи є необхідність спеціального вичення тактики злочинців щодо створення, використання, розповсюдження або збуту шкідливих програмних засобів:

Назва альтернативи	шифр	кількість	%
Так	041	232	84,4
Ні	042	43	15,6

Таблиця 12.

Що включає в себе тактику злочинної діяльності, що потребує наукової розробки

Назва альтернативи	шифр	кількість	%
Приховування слідів цього злочину;	043	123	44,7
Поведінка в процесі проведення розслідування;	044	20	7,3
Маскування злочинної діяльності;	045	44	16,0

Вибір засобів і способів вчинення злочинів;	046	55	20,0
Поводження за межами підготовки, вчинення і розслідування злочину (вивчення особистості, його побут);	047	33	12,0

Таблиця 13.

По яких питаннях тактики злочинців інформація відсутня?

Назва альтернативи	шифр	кількість	%
Приховування слідів злочину;	048	156	56,7
Поведінка в процесі проведення розслідування;	049	42	15,3
Маскування злочинної діяльності;	050	22	8,0
Вибір засобів і способів вчинення злочинів;	051	55	20,0
Поводження за межами підготовки, вчинення і розслідування злочину (вивчення особистості, його побуту);	052	0	0

Таблиця 14.

По яких джерелах необхідно вивчати тактику злочинної діяльності:

Назва альтернативи	шифр	кількість	%
Опитування практичних працівників;	053	42	15,3
Опитування злочинців;	054	90	32,7
Вивчення кримінальних справ;	055	110	40,0
Вивчення оперативних матеріалів;	056	11	4,0
Вивчення зарубіжних літературних джерел;	057	0	0
Аналіз літератури, що випускається «для злочинців»;	058	22	8,0

Таблиця 15.

Чи необхідно і чи доцільно спеціальне вивчення помилок, що допускаються практичними працівниками в своїй діяльності?

Назва альтернативи	шифр	кількість	%
Обумовлених неправильністю власних рішень і дій;	059	221	80,4

Пов’язаних з протидією з боку злочинців;	060	43	15,6
Така необхідність відсутня;	061	11	4,0

Таблиця 16.

Чи необхідно і допустимо виділення цього виду злочину пріоритетним у боротьбі зі злочинністю?

Назва альтернативи	шифр	кількість	%
Так	062	65	23,6
Ні	063	210	76,4

Таблиця 17.

Чи слід розширити систему покарання і посилити відповідальність?

Назва альтернативи	шифр	кількість	%
Так	064	222	80,7
Ні	065	53	19,3

Таблиця 18.

Чи вважаєте ви допустимим висвітлення в ЗМІ відомостей про способи вчинення злочину і методах боротьби з цими видами правопорушень?

Назва альтернативи	шифр	кількість	%
Так	066	98	35,6
Ні	067	177	64,4

Таблиця 19.

Чи достатньо методичних рекомендацій, оглядів, літератури стосовно боротьби з цим видом злочинної діяльності:

Назва альтернативи	шифр	кількість	%
Так	068	31	11,3

Ні	069	244	88,7

Таблиця 20.

Якщо так, то чи потрібна, на Вашу думку, окрема спеціальна методика розслідування злочинів в сфері створення, використання, розповсюдження або збуту шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Так, оскільки розслідування цих злочинів відзначається суттевою специфікою;	070	254	92,4
Ні, я вважаю, що в мене достатньо знань для розслідування злочинів даної категорії;	071	10	3,6
Важко відповісти;	072	11	4,0

Таблиця 21.

Дефіцит яких відомостей Ви при цьому відчуваєте?

Назва альтернативи	шифр	кількість	%
Про характеристику технологічного процесу створення, використання, розповсюдження або збуту шкідливих програмних засобів;	073	221	80,4
Про основні способи вчинення злочинів, механізми та схеми окремих кримінальних операцій іх властивими їм ознаками;	074	43	15,6
Про джерела та процесуальні механізми одержання необхідної для встановлення істини інформації;	075	0	0
Про перелік обставин, що підлягають встановленню до відкриття кримінального провадження та ефективного розслідування;	076	11	4,0
Про типові ситуації, що складаються при отриманні первинної інформації, документуванні злочинних дій та реалізації оперативних матеріалів, можливі навпрями їх вирішення;	077	0	0
Про умови та порядок використання спеціальних технічних та криміналістичних знань (експертиз, допомоги спеціалістів тощо);	078	0	0
Про особливості юридичної оцінки та кваліфікації злочинів;	079	0	0

Таблиця 22.

В якій формі, на Вашу думку, мають бути розроблені методичні рекомендації?

Назва альтернативи	шифр	кількість	%
Практичні посібники або довідники;	080	88	32
Методичні листи;	081	88	32
Огляди оперативно-розхшукової, слідчої та судової практики;	082	43	15,6
Підручники та учбові посібники розгорнуті плани слідчо-оперативних заходів по кримінальним провадженням;	083	56	20,4

Таблиця 23.

Яке місце, на Вашу думку, в розслідуванні злочинів займають оперативні відомості?

Назва альтернативи	шифр	кількість	%
Визначальне;	084	133	48,4
Допоміжне;	085	120	43,6
В процесуальному розслідуванні не використовуються, мають значення тільки для ОРС;	086	22	8,0

Таблиця 24.

Яким чином в процесуальному розслідуванні використовується оперативно розшукова робота?

Назва альтернативи	шифр	кількість	%
Проведення за дорученням слідчого окремих слідчих та процесуальних дій;	087	98	35,6
Особиста участь оперативного працівника у проведенні окремих слідчих та процесуальних дій, виконуваних слідчим;	088	78	28,4
Проведення в ході слідства оперативно-розшукових заходів;	089	89	32,4
Взаємні консультації та обмін інформацією, матеріалами, досвідом;	090	10	3,6

Таблиця 25.

Хто найчастіше виступає ініціатором використання матеріалів ОРС при розслідуванні?

Назва альтернативи	шифр	кількість	%

Оперативний працівник, керівництво оперативного підрозділу;	091	65	23,6
Слідчий;	092	11	4,0
Керівництво слідчого підрозділу;	093	177	64,4
Керівник органу розслідування;	094	22	8,0

Таблиця 26.

Як взагалі Ви оцінюєте стан використання матеріалів ОРС та взаємодії слідчих та оперативних працівників в процесуальному доказуванні?

Назва альтернативи	шифр	кількість	%
Як оптимальний;	095	21	7,6
Як задовільний, але такий, що потребує вдосконалення;	096	199	72,4
Як незадовільний, оскільки не відповідає цілям та задачам боротьби зі злочинністю	097	55	20,0

Таблиця 27.

Які фактори, на Вашу думку, сприятимуть підвищенню ефективності оперативно розшукового супроводження розслідування?

Назва альтернативи	шифр	кількість	%
Вдосконалення кримінально-процесуального законодавства та нормативних актів з метою надання ОРС відповідного процесуального статусу та забезпечення реальної взаємодії слідчих та оперативних працівників;	098	232	84,4
Вдосконалення системи обліку результатів оперативних та слідчих підрозділів та критеріїв їх оцінки;	099	32	11,6
Важко відповісти;	100	11	4,0

Зведені дані опитування 258 учасників кримінальних проваджень які брали участь в опитуванні у ході здійснення досудового розслідування про кіберзлочини

Таблиця 1.

Ваш вік

Назва альтернативи	шифр	кількість	%
До 18 років	001	0	0

До 30 років	002	234	90,7
До 40 років	003	24	9,3
Понад 5 років	004	0	0

Таблиця 2.

Освіта

Назва альтернативи	шифр	кількість	%
Вища	005	51	19,8
Неповна вища	006	105	40,7
Середня-спціальна	007	102	39,5
Немає	008	0	0

Таблиця 3.

Чи знайомі ви з заходами які необхідно проводити на ЕОМ (комп'ютері) по недопущенню проникнення шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Так	009	110	42,6
Ні	010	148	57,4

Таблиця 4.

Чи застосовуєте Ви на своєму комп'ютері заходи безпеки щодо недопущення проникнення шкідливих програмних засобів? (фаерволи, антивірусні програми)

Назва альтернативи	шифр	кількість	%
Так	011	137	53,1
Ні	012	121	46,9

Таблиця 5.

Чи зустрічались ви з впливом на роботу ЕОМ (комп'ютерів) шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Так	013	118	45,7
Ні	014	140	54,3

Таблиця 6.

Якщо зустрічались то чи звертались ви за допомогою до правоохоронних органів?

Назва альтернативи	шифр	кількість	%
Так	015	19	7,4
Ні	016	239	92,6

Таблиця 7.

Як часто ви зустрічаєтесь спробою впливу, впливом на роботу Вашого ЕОМ (комп'ютера) шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Часто	017	12	4,7
Нечасто	018	154	59,7
Важко відповісти	019	92	35,7

Таблиця 8.

Чи відомі вам джерела поширення таких шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Так	020	64	24,8
Ні	021	194	75,2

Таблиця 9.

Чи бували при роботі на Вашому ЕОМ (комп'ютері) випадки проникнення шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Так	022	45	17,4
Ні	023	213	82,6

Таблиця 10.

Якщо так, то це було пов’язане з:

Назва альтернативи	шифр	кількість	%
Неспроможність систем захисту, їх недосконалість;	024	38	14,7
Недотримання самим користувачем правил безпеки;	025	44	17,1
Важко відповісти;	026	176	68,2

Таблиця 11.

Які операції є найбільш криміногенними?

Назва альтернативи	шифр	кількість	%
Активна робота в мережі;	027	135	52,3
Пасивна робота в мережі;	028	34	13,2
Саме підключення, без будь-якої діяльності в мережі;	029	89	34,5

Таблиця 12.

Які фактори визначають активізацію створення, використання, розповсюдження або збут шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Недосконалість нормативної бази в суспільстві;	030	67	26,0

Відсутність комплексної програми протидії;	031	137	53,1
Відсутність взаємодії з іншими правоохоронними органами, комерційними і громадськими організаціями;	032	54	20,9

Таблиця 13.

Які фактори, крім вищевказаних визначають кримінальну активність та зумовлюють можливість створення, використання, розповсюдження або збуту шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Можливість ефективного приховування;	033	58	22,5
Злочинці розуміють, що інформація про вчинений злочин все рівно не «дійде» до правоохоронних органів;	034	72	27,9
Недосконаліть програмного та технічного забезпечення захисту;	035	84	32,6
Низький професійний рівень адміністраторів комп. мережі;	036	18	7,0
Недостатній профілактичний моніторинг або його відсутність;	037	8	3,1
Низька ефективність роботи правоохоронців;	038	18	7,0

Таблиця 14.

Які фактори ускладнюють процес взаємодії організацій, підприємств, установ, що розробляють антивірусні програмні засоби та правоохоронних органів, що здійснюють оперативне супроводження та розслідують злочини в цій сфері?

Назва альтернативи	шифр	кількість	%
Некомпетентність працівників правоохоронних органів та відсутність перспектив розслідування;	039	96	37,2
Збитки від офіційного розслідування можуть бути вищими ніж сума заподіяної злочином шкоди;	040	72	27,9
Страх підірвати свою репутацію;	041	24	9,3
Викриття в ході розслідування професійної некомпетентності;	042	28	10,9
Правова неосвіченість;	043	20	7,8
Недовіра до того що завдані збитки будуть відшкодовані;	044	18	7,0

Таблиця 15.

Які фактори будуть сприяти ефективній протидії таким злочинам?

Назва альтернативи	шифр	кількість	%
Активізація законодавчого регулювання;	045	55	21,3
Підвищення свідомості працівників (адміністраторів);	046	62	24,0
Розробка новітніх систем захисту' як на програмному так і апаратному рівні;	047	141	54,7

Таблиця 16.

Чи реальна за теперішніх умов безпечна робота в мережі, Інтернеті?

Назва альтернативи	шифр	кількість	%
Цілком реальна;	048	80	31,0
Абсолютно нереальна;	049	56	21,7
Важко відповісти;	050	122	47,3

Таблиця 17.

Якими мотивами керується особа то займаються розробкою, поширенням шкідливих програмних засобів?

Назва альтернативи	шифр	кількість	%
Корисні;	051	71	27,5
Самосгвердження;	052	56	21,7
Ідеологічні;	053	60	23,3
Важко сказати;	054	71	27,5

Таблиця 18.

По якій причині інформація про злочини в цій сфері не повідомляються в правоохоронні органи?

Назва альтернативи	шифр	кількість	%
Наявність в своїй діяльності конфіденційної інформації;	055	59	22,9
Думка про некомпетентність правоохоронців;	055	91	35,3
Наявність в діяльності потерпілого ознак інших протиправних діянь;	057	28	10,9
Наявність власних сил і засобів до встановлення осіб і відшкодування збитків;	058	24	9,3
Інші причини;	059	56	21,7

Таблиця 19.

Які фактори зумовлюють низьку ефективність діяльності правоохоронних органів в цій сфері?

Назва альтернативи	шифр	кількість	%
Новизна таких злочинів, недостатня обізнаність про способи їх вчинення;	060	82	31,8
Відсутність необхідних знань, розуміння технологічного процесу роботи ЕОМ;	061	86	33,8
Відсутність розроблених сучасних методик виявлення та розслідування банківських злочинів;	062	34	13,2
Недостатній рівень використання оперативно-розшукових заходів та оперативного супроводження роботи мереж;	063	14	5,4
Недосконаліть правової бази, що регламентує діяльність правоохоронних органів в цій сфері;	064	10	3,9
Недостатній рівень інформаційного забезпечення;	065	12	4,7
неефективна взаємодія різних служб та відомств в тому числі на міжнародному рівні;	066	0	0
Недостатня професійна компетентність та неукомплектованість оперативних працівників;	067	0	0
Необ’єктивна система обліку результатів правоохоронної діяльності та оцінки її результатів;	068	20	7,8

Таблиця 20.

Чи необхідно і допустимо виділення цього виду злочину пріоритетним в боротьбі зі злочинністю:

Назва альтернативи	шифр	кількість	%

Так	069	161	62,4
Ні	070	97	37,6

Таблиця 21.

Чи слід розширити систему покарання і посилити відповідальність?

Назва альтернативи	шифр	кількість	%
Так	071	175	67,8
Ні	072	83	32,2

Таблиця 22.

Чи вважаєте Ви допустимим висвітлення в ЗМІ даних про способи скоєння злочину і методах боротьби з цими видами правопорушень:

Назва альтернативи	шифр	кількість	%
Так	073	149	57,8
Ні	074	109	42,2

Таблиця 23.

Чим обумовлені основні недоліки в протидії виготовленню, розробки поширенню або збут шкідливих програмних засобів:

Назва альтернативи	шифр	кількість	%
Високий рівень професіоналізму злочинця;	075	106	41,1
Низький рівень матеріально технічного і фінансового забезпечення підрозділів;	076	86	33,3
Відсутність методичних і практичних посібників, методик;	077	14	5,4
Низький рівень підготовки і професіоналізму співробітників;	078	22	8,5
Відсутність зацікавленості в результатах своєї роботи;	079	0	0
Недостатня нормативно-правова забезпеченість;	080	20	7,8

Недостатня увага держави і суспільства до таких правопорушень;	081	10	3,9
Відсутність систематичності, планомірності, цілеспрямованості діяльності в державній політиці;	082	10	3,9

Таблиця 24.

Джерела інформації про такі види злочинів?

Назва альтернативи	шифр	кількість	%
Обмін досвідом і знаннями з колегами;	083	107	41,5
Особистий досвід;	084	59	22,9
Літературні джерела;	085	30	11,6
Професійна підготовка, підвищення кваліфікації;	086	62	24,0

Додаток Г

У додатку надані пропозиції щодо внесення змін і доповнень до окремих норм Кримінального процесуального кодексу України та Кримінального кодексу України, виділені курсивом.

Кримінальний процесуальний кодекс України:

Стаття 69. Експерт

1. Експертом у кримінальному провадженні є особа, яка володіє науковими, технічними або іншими спеціальними знаннями, має право відповідно до Закону України "Про судову експертизу" на проведення експертизи, *відомості про яку, внесені до Державного реєстру атестованих судових експертів* і якій доручено провести дослідження об'єктів, явищ і процесів, що містять відомості про обставини вчинення кримінального правопорушення, та дати висновок з питань, які виникають під час кримінального провадження і стосуються сфери її знань.

2. Не можуть бути експертами особи, які перебувають у службовій або іншій залежності від сторін кримінального провадження або потерпілого.

3. Експерт має право:

1) знайомитися з матеріалами кримінального провадження, що стосуються предмета дослідження;

2) заявляти клопотання про надання додаткових матеріалів і зразків та вчинення інших дій, пов'язаних із проведенням експертизи;

3) бути присутнім під час вчинення процесуальних дій, що стосуються предметів та об'єктів дослідження;

4) викладати у висновку експертизи виявлені в ході її проведення відомості, які мають значення для кримінального провадження і з приводу яких йому не були поставлені запитання;

5) ставити запитання, що стосуються предмета та об'єктів дослідження, особам, які беруть участь у кримінальному провадженні;

6) одержати винагороду за виконану роботу та відшкодування витрат, пов'язаних із проведенням експертизи і викликом для надання пояснень чи показань, у разі, якщо проведення експертизи не є службовим обов'язком особи, яка залучена як експерт;

7) заявляти клопотання про забезпечення безпеки у випадках, передбачених законом;

8) користуватися іншими правами, передбаченими Законом України "Про судову експертизу".

4. Експерт не має права за власною ініціативою збирати матеріали для проведення експертизи. Експерт може відмовитися від давання висновку, якщо

поданих йому матеріалів недостатньо для виконання покладених на нього обов'язків. Заява про відмову має бути вмотивованою.

5. Експерт зобов'язаний:

1) особисто провести повне дослідження і дати обґрунтований та об'єктивний письмовий висновок на поставлені йому запитання, а в разі необхідності - роз'яснити його;

2) прибути до слідчого, прокурора, суду і дати відповіді на запитання під час допиту;

3) забезпечити збереження об'єкта експертизи. Якщо дослідження пов'язане з повним або частковим знищенням об'єкта експертизи або зміною його властивостей, експерт повинен одержати на це дозвіл від особи, яка залучила експерта;

4) не розголошувати без дозволу сторони кримінального провадження, яка його залучила, чи суду відомості, що стали йому відомі у зв'язку з виконанням обов'язків, або не повідомляти будь-кому, крім особи, яка його залучила, чи суду про хід проведення експертизи та її результати;

5) заявити самовідвід за наявності обставин, передбачених цим Кодексом.

6. Експерт невідкладно повинен повідомити особу, яка його залучила, чи суд, що доручив проведення експертизи, про неможливість проведення експертизи через відсутність у нього необхідних знань або без залучення інших експертів.

7. У разі виникнення сумніву щодо змісту та обсягу доручення експерт невідкладно заявляє клопотання особі, яка призначила експертизу, чи суду, що доручив її проведення, щодо його уточнення або повідомляє про неможливість проведення експертизи за поставленим запитанням або без залучення інших осіб.

Стаття 242-1. Судова експертиза

Судова експертиза - процесуальна дія, що складається з проведення досліджень експертом, який відповідає вимогам, визначеним Законом України «Про судову експертизу» та зарахований до державного реєстру атестованих судових експертів, з питань, вирішення яких потребує спеціальних знань в галузі науки, техніки, мистецтва, і які поставлені перед експертом судом, суддею, слідчим або прокурором, з метою встановлення обставин, що підлягають доказуванню по конкретному кримінальному провадженню і дачі висновку по результатам дослідження.

Експертне дослідження оформлюється мотивованим висновком експерта, в якому описується хід дослідження і даються відповіді на поставлені питання. Отриманий висновок є доказом, що свідчить про наявність чи відсутність

фактичних даних, необхідних для вирішення того чи іншого питання або стає підставою для судового розгляду.

Кримінальний кодекс України:

Стаття 361-1. Створення з метою використання, розповсюдження або збуту шкідливих програмних *матеріалів* чи технічного *обладнання*, а також їх *використання,* розповсюдження або збут

1. Створення з метою використання, розповсюдження або збуту, а також *використання***,** розповсюдження або збут шкідливих програмних *матеріалів* чи *технічного обладнання*, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, -

караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років, або позбавленням волі на той самий строк.

2. Ті самі дії, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, -

караються позбавленням волі на строк до п'яти років.