УДК: 343.98

КРИМІНАЛІСТИЧНИЙ АСПЕКТ СПОСОБІВ ВЧИНЕННЯ КІБЕРЗЛОЧИНІВ

Ярослав Неділько

CRIMINALISTIC ASPECT OF METHODS TO COMMIT CYBERCRIMES

Yaroslav Nedilko

Анотація. *У статті досліджено особливості способів вчинення кіберзлочинів як елементу криміналістичної характеристики.*

Визначено, що в юридичній науці спосіб вчинення злочину досліджується в кримінально-правовому, кримінально-процесуальному, криміналістичному напрямах та вкладає у дане визначення своє особливе значення.

Розглянуто основні підходи вчених до визначення поняття «спосіб вчинення злочину», які, своєю чергою, дали можливість навести сучасне визначення способу вчинення кіберзлочину. Проаналізовано генезу способів вчинення комп'ютерних злочинів та їх трансформацію у кіберзлочини. За результатами проведеного дослідження надано класифікацію способів вчинення кіберзлочинів.

Ключові слова: *способи вчинення злочину, способи вчинення кіберзлочину, криміналістична характеристика способів вчинення кіберзлочину.*

Summary. *This article studies the peculiarities of ways of committing cybercrime as an element of forensic characteristics.*

It was considered, that in forensic science committing crime actions was started to study by scientists in the mid-20s. The author analyzes opinions of researchers of the XX-XXI centuries concerning the understanding of the crime in criminal science.

There are considered the basic approaches of scientists to the definition of the concept of "crime mode". The researcher analyzes genesis of crimes with the help of computer technologies and its transformation into cybercrime. According to the results of the research, it is provided a classification of ways of committing cybercrime: 1) illegal access to information technologies; 2) illegal data interception; 3) possession, producing, sale, update of malware, passwords, encodings or other; 4) counterfeiting and fraud related to the use of information technology; 5) possession, producing, offering or providing, distributing, acquiring child pornography using information technology; 6) infringement of copyright or related rights; 7) a complex of ways. The author describes each of the following ways of committing cybercrime. It is separated in the research a set of methods – consists of two or more methods of different groups, one of them is always used as the main, and the other perform auxiliary functions, such as the production of malware (3) to distribute child pornography (5).

The researcher emphasizes that the intensive development of the latest technologies causes the abusers to adapt and invent new ways of illegal use of information technologies in their crime of intent. Therefore, knowledge of typical ways of committing crimes using information technology, as one of the elements of the forensic characteristic of cybercrime, contributes to a more efficient organization of crime investigation. First of all, determining the method of committing a cybercrime in combination with other elements of the criminalistic characteristic of the crime allows the investigator to obtain information about the circumstances of the perpetrator, to make a realistic plan of investigation and to determine the specific directions of search for traces of a crime.

Key words: *methods of committing a crime, crime mode, methods of committing a cybercrime, forensic characteristics of ways of committing a cybercrime.*

Актуальність теми дослідження. Під час розслідування будь-якого злочину особливу увагу приділяють способу його вчинення. Як на практиці, так і на сторінках теоретичних праць тривають дискусії з цього питання.

Спосіб вчинення злочину в різний час досліджували такі вчені, як: Р.С. Бєлкін, П.Д. Біленчук, О.М. Дуфенюк, С.М. Зав'ялов, Г.Г. Зуйков, О.Н. Колесниченко, Г.А. Матусовський, М.В. Салтевський, М.П. Яблоков та інші.

Одним із важливих і визначальних елементів у структурі криміналістичної характеристики кіберзлочинів є спосіб їх вчинення. Метою цього дослідження є виявлення особливостей способів вчинення кіберзлочинів як елементу криміналістичної характеристики та визначення цього поняття.

Основний текст. Термін «спосіб» тлумачать як певну дію, прийом або систему прийомів, що дає можливість зробити, здійснити що-небудь, досягти чогось [1, p. 1179].

У юридичній науці спосіб вчинення злочину вивчають у кримінально-правовому, кримінально-процесуальному, криміналістичному аспектах та вкладають у це визначення значення з урахуванням напряму дослідження. В.Є. Корноухов слушно наголошує, що в кримінальному праві спосіб вчинення пов'язаний з іншими елементами об'єктивної сторони злочину, він визначає караність діяння, а також виступає як кваліфікуюча ознака. У кримінально-процесуальному праві значення способу вчинення злочину належить до обставин, що підлягають доказуванню. У криміналістиці з огляду на спосіб вчинення злочину розшукують осіб, які вчинили злочин, з'ясовують закономірності механізму слідоутворення, а також місцезнаходження інших слідів, що стосуються вчиненого злочину [2, Kornoukhov, 2000, p. 172-173].

Враховуючи відсутність єдиної думки з цього питання, В.О. Коновалова зазначає, що проблема способу вчинення злочину як одна з ключових у криміналістиці залишається дискусійною. Це спричинено наявністю різних підходів вчених до інтерпретації понятійного апарату, зокрема до змісту понять «спосіб вчинення» і «спосіб приховання» [3, Konovalova, 2001, p. 7].

У криміналістичній науці спосіб вчинення злочину вчені почали досліджувати в середині XX століття. Вважається, що найпершими визначення поняття способу вчинення умисного злочину надали А.І. Вінберг та Б.М. Шавер, які розглядали його як складову предмета криміналістики та стверджували, що використання знань про спосіб вчинення злочину застосовується для виявлення його слідів, встановлення злочинців і розкриття вчинених ними злочинів. Це поняття вони трактували так: це дії, безпосередньо спрямовані на досягнення злочинних наслідків, включаючи дії щодо проникнення злочинця на місце вчинення злочину, прийоми, які злочинець використовував, особливо стосовно предмета замаху, місце, час, знаряддя злочину [4, Shawer and Winberg, 1950, p. 199; 5, Shawer, 1952, p. 34].

Уперше структуру способу вчинення умисного злочину розкриває Е.Д. Куранова, стверджуючи, що це комплекс дій з підготовки, вчинення і приховання злочину, вибраних злочинцями з наміченою метою і з урахуванням тих умов, за яких реалізується злочинний намір [6, Kuranova, 1962, p. 165-167].

Власну криміналістичну концепцію способу вчинення злочину сформулював О.Н. Колесниченко, який пропонує розуміти спосіб дій злочинця, що виявляється у певній послідовності, поєднанні окремих дій, прийомів, які застосовує суб'єкт. Цікавим є те, що вчений запропонував розглядати окремо спосіб готування до вчинення злочину, спосіб власне вчинення злочину і спосіб приховання злочину [7, Kolesnichenko, 1965, p. 18].

Такого погляду дотримується і О.М. Дуфенюк, яка розділяє окремо спосіб готування, вчинення і приховання злочину як елементів криміналістичної характеристики злочинів та зауважує, що не кожний вид злочину має всі три стадії, адже вагому частку злочинів вчиняють взагалі без підготовчого етапу або маскування слідів злочинного діяння [8, Dufeniuk, 2012, p. 237].

Г.Г. Зуйков, проте, вважає, що спосіб вчинення злочину – це система дій з готування, вчинення і приховання злочину, детермінованих умовами зовнішнього світу і психофізіологічними якостями особистості, що можуть бути пов'язані з вибірковим

використанням відповідних знарядь або засобів і умов місця й часу та об'єднані загальним злочинним задумом [9, Zuikov, 1970, p. 205].

Однак Р.С. Бєлкін зауважує, що твердження Г.Г. Зуйкова є правильним для тих випадків, коли готування, вчинення і приховання злочину відбувається за єдиним задумом, коли всі ці дії тісно пов'язані між собою в єдину систему і, ще не вчинивши злочину, суб'єкт має чітку програму дій щодо його приховання. Але так буває не завжди. Дії щодо вчинення і приховання злочину можуть бути розірвані за суб'єктом, коли приховує не той, хто його вчинив, а інша особа без відома суб'єкта злочину, який і не скоював дій з приховання злочину. Ці дії можуть відрізнятися за задумом, коли цілі приховання спочатку не переслідувалися, а виникли вже після вчинення злочину через непередбачені обставини або такі, що змінилися. Формулюючи висновок, вчений стверджує, що приховання може існувати самостійно, як система дій зі знищення, маскування або фальсифікації слідів злочину і злочинця – і матеріальних, і ідеальних [10, Belkin, 2001, p. 735].

Разом з тим, на думку П.Д. Біленчука, В.К. Лисиченка та Н.І. Клименко, не доцільно до криміналістичної характеристики способу вчинення злочину відносити сукупність відомостей про дії злочинця, направлені на маскування (приховання) злочину і його слідів, оскільки це є частиною способу вчинення злочину [11, Bilenchuk, Lisichenko and Klimenko, 2001, p. 365].

Своєю чергою, способи вчинення злочину М.С. Уткін пропонує поділяти на: 1) повноструктурні, або найкваліфікованіші (готування, вчинення і приховання злочину); 2) менш кваліфіковані, або усічені першого типу (вчинення і приховання злочину); 3) менш кваліфіковані, або усічені другого типу (готування і вчинення злочину); 4) некваліфіковані, або спрощені, що складаються лише з дій власне вчинення злочинів [12, Utkin, 1975, p. 6].

Натомість, М.А. Погорецький, Д.Б. Сергєєва, З.М. Топорецька переконані, що спосіб вчинення злочину – це послідовність дій суб'єкта, спрямована на досягнення поставленої мети (певного злочинного результату), тобто усе те, що характеризує дії злочинця під час підготовки (підшукання місця, вибір предмета посягання, готування знарядь і засобів, необхідних для здійснення злочинної цілі тощо), вчинення злочину й приховання його слідів [13, Pogoretskiy, Sergeyeva and Toporetska, 2015, p. 27].

Враховуючи відсутність єдності поглядів щодо трактування способу вчинення злочину та наведені позиції науковців, на нашу думку, для кіберзлочинів характерні дії, що передбачають готування, вчинення та приховання злочину.

Варто зауважити, що в науковій літературі впродовж тривалого часу домінувало поняття «комп'ютерний злочин». Це пов'язано з тлумаченням у XIX столітті слова «комп'ютер» («той, що вираховує») [14] як механічного, а пізніше цифрового, аналогового і електронного, обчислюваного пристрою, який злочинці використовують для досягнення своїх злочинних намірів. Проте науково-технічний прогрес зумовлює подальший стрімкий розвиток і широке використання в усіх сферах суспільного життя новітніх інформаційних технологій (комп'ютерної техніки, глобальних інформаційних мереж та їх ресурсів, мобільних засобів комунікації та інших технічних засобів).

У цьому аспекті обґрунтованою є позиція науковців, які стверджують, що разом із розвитком новітніх технологій поняття «комп'ютерні злочини» трансформувалось у поняття «злочини, що вчиняються з використанням інформаційних технологій (кіберзлочини)» [11, Bilenchuk et al., 2001, p. 434]. Дефініція «кіберзлочинність» відповідає і міжнародним стандартам.

Відповідно, окрім визначення поняття «комп'ютерний злочин», вивчалися і способи його вчинення.

Так, свого часу Ю.М. Батурін, узагальнюючи конкретні дії злочинців щодо доступу до засобів комп'ютерної техніки, запропонував класифікувати способи вчинення комп'ютерних злочинів, поділяючи їх на п'ять груп:

1) вилучення засобів комп'ютерної техніки;

2) перехоплення інформації;

3) несанкціонований доступ до засобів комп'ютерної техніки;

4) маніпуляція даними і керуючими командами;

5) комплексні методи [15, Baturin, 1991, p. 18-34].

На противагу цьому, О.Х. Волинський поділяє такі злочини на дві великі групи. До першої вчений відносить злочинні діяння, що здійснюються без використання комп'ютерних пристроїв як інструментів для проникнення в інформаційні системи чи вплив на них. Зокрема, викрадення електронних носіїв інформації у формі блоку чи елементів ЕОМ тощо. До другої групи належать діяння з використанням комп'ютерних та комунікаційних пристроїв як інструментів для проникнення в інформаційні системи чи вплив на них [16, Volinskiy, 1999, p. 585-586].

Л.П. Паламарчук, розмірковуючи про способи вчинення злочинів зазначеної категорії, цілком слушно зауважує, що спосіб вилучення засобів комп'ютерної техніки передбачає фізичне вилучення, а тому його доцільно відносити до злочинів проти власності. На переконання науковця, слід виділити п'ять груп способів вчинення злочинів зазначеної категорії:

1) незаконне втручання в роботу ЕОМ (комп'ютера), системи та комп'ютерної мережі;

2) незаконне перехоплення комп'ютерної інформації;

3) маніпуляції з комп'ютерною інформацією;

4) використання шкідливих програм;

5) комплексні методи, тобто використання одночасно кількох методів [17, Palamarchuk, 2004, p. 50].

Резонно зазначає В.Б. Вєхов, що майже всі способи вчинення цих злочинів мають індивідуальні ознаки, за якими їх можна розпізнати та класифікувати в окремі групи. Зазвичай їх основу становлять дії злочинця, направлені на отримання різного роду доступу до засобів комп'ютерної техніки. Всі ці дії здійснюються з використанням кваліфікованих і хитрих способів маскування, що ускладнює їх виявлення, розслідування та розкриття [18, Vehov, 1996].

У загальному значенні спосіб вчинення кіберзлочинів – це сукупність послідовних умисних протиправних дій суб'єкта (суб'єктів) у кіберпросторі, що передбачають дії з готування, вчинення та приховування і спрямовані на досягнення певного злочинного результату з використанням інформаційних технологій.

Однак із розвитком сучасних інформаційних технологій почали змінюватися і форми злочинної діяльності. Це зумовило виникнення нового поняття «злочини, що вчиняються з використанням інформаційних технологій (кіберзлочини)».

З урахуванням визначених у Конвенції про кіберзлочинність [19] та положеннях ст.ст. 361-363[1] КК України [20] видів кіберзлочинів, можемо виокремити наступні, притаманні цій категорії злочинів, способи їх вчинення:

1) незаконний доступ до інформаційних технологій;

2) незаконне перехоплення даних;

3) володіння, виготовлення, продаж, придбання шкідливих програм, паролів, кодів доступу або подібних даних;

4) підробка та шахрайство, пов'язане з використанням інформаційних технологій;

5) володіння, вироблення, пропонування або надання, розповсюдження, здобуття дитячої порнографії з допомогою інформаційних технологій;

6) порушення авторських чи суміжних прав;

7) комплекс способів.

Стисло охарактеризуємо кожну із наведених груп.

Так, до першої групи слід віднести дії, спрямовані на отримання незаконного доступу до інформаційних технологій. Доступ означає проникнення в усю систему (ст. 4

Конвенції) або її частину, до програм і даних (ст. 5 Конвенції), які там містяться. Це може бути прямий фізичний доступ до інформаційних технологій або входження з віддаленого місця, наприклад із застосуванням супутникового зв'язку або інших інформаційних технологій [11, Bilenchuk et al., 2001, p. 438-439]. В юридичній літературі цей вид називають «хакінг» – протиправний доступ до інформаційних технологій з порушенням засобів захисту [11, Bilenchuk et al., 2001, p. 439].

Другу групу становлять дії, спрямовані на одержання даних шляхом використання аудіовізуального та електромагнітного перехоплення. До них належать: безпосереднє перехоплення; електромагнітне перехоплення; відеоперехоплення. [17, Palamarchuk, 2004, p. 55]. Л.П. Паламарчук слушно зазначає, що безпосереднє перехоплення – найпростіший спосіб незаконного втручання в роботу інформаційних технологій, що здійснюється через зовнішні комунікаційні канали системи або шляхом прямого підключення до ліній периферійних пристроїв та мереж. Зазначений спосіб мало поширений з причини децентралізації обробки інформації, оскільки дані простіше перехопити під час їх передачі телекомунікаційними каналами і мережами, ніж проникнути безпосередньо до приміщення [17, Palamarchuk, 2004, p. 55-56]. Електромагнітне перехоплення дає можливість одержати дані шляхом не прямого підключення до інформаційної техніки, а перехоплення випромінювань центрального процесора, дисплея, комунікаційних трактів, принтера тощо [21, Fedorov, 1994, p. 45-46]. У науковій літературі як підвиди електромагнітного перехоплення розглядають аудіоперехоплення та відеоперехоплення. Аудіоперехоплення полягає у застосуванні в інформаційних технологіях чуттєвих мікрофонів, так званих жучків, з метою перехоплення розмов для отримання інформації про роботу комп'ютерної системи, персоналу, засобів безпеки тощо [17, Palamarchuk, 2004, p. 57]. Відеоперехоплення – це дії, спрямовані на незаконне отримання необхідної інформації з певної відстані під час спостереження за об'єктом шляхом використання різної оптичної техніки (бінокля, мисливського пристрою нічного бачення тощо) [17, Palamarchuk, 2004, p. 57].

До третьої групи належить будь-яке спеціально створене програмне забезпечення, яким володіє, виготовив, придбав чи продав злочинець для того, щоб завдавати шкоди інформаційним технологіям [22]. Прикладами таких програм є: «Троянський кінь» – прихована програма, яку використовують злочинці для отримання доступу до інформаційних технологій, обійшовши систему захисту [11, Bilenchuk et al., p. 440-441]; «WannaCry» – комп'ютерний вірус, що вражає операційну систему Microsoft Windows шляхом шифрування файлів, атакує комп'ютери шляхом шифрування файлів користувача, після чого виводить повідомлення про перетворення файлів з пропозицією протягом трьох днів здійснити оплату ключа дешифрування для розблокування даних у біткойнах в еквіваленті суми $300, у разі ненадходження коштів сума автоматично збільшується вдвічі, на сьомий день вірус знищує дані [23]; інші.

До четвертої групи віднесено дії, направлені на приховання, зміну, знищення, введення даних, а також втручання у функціонування системи інформаційних технологій, з шахрайською метою набуття економічних переваг для себе чи іншої особи (ст.ст. 7, 8 Конвенції) [20]. Зазвичай цей спосіб застосовують в економічних злочинах, наприклад при зміні вхідних (вихідних) даних бухгалтерського обліку в процесі автоматизованої обробки документів [24, Vehov, Golubev, 2004, p. 159-160].

П'яту групу становлять дії з вироблення, володіння, пропонування або надання, розповсюдження, здобуття дитячої порнографії за допомогою інформаційних технологій та здійснення цих дій у кіберпросторі. Слід зазначити, що згідно з Законом України «Про захист суспільної моралі» під дитячою порнографією слід розуміти зображення у будь-який спосіб дитини чи особи, що виглядає, як дитина, задіяної у реальній чи змодельованій відверто сексуальній поведінці, або будь-яке зображення статевих органів дитини в сексуальних цілях [25].

До шостої групи способів вчинення кіберзлочинів належить незаконне копіювання,

розповсюдження або публікація програмного забезпечення, ігор та всього, що захищено авторським чи суміжним правом, через кіберпростір чи за допомогою інформаційних технологій.

І, відповідно, комплекс способів, що складається з двох чи більше способів різних груп, причому один із них завжди використовується як основний, а інші виконують допоміжні функції, наприклад виготовлення шкідливих програм (3) з метою розповсюдження дитячої порнографії (5).

Висновок. Безперечно, інтенсивний розвиток новітніх технологій спонукає зловмисників прилаштовуватись і вигадувати нові способи незаконного використання інформаційних технологій у своїх злочинних намірах. Тому знання способів вчинення злочинів з використанням інформаційних технологій як елементів криміналістичної характеристики кіберзлочинів сприяють більш ефективній організації розслідування злочинів. Визначення способу вчинення кіберзлочину в поєднанні з іншими елементами криміналістичної характеристики злочину дає можливість слідчому отримати інформацію про обставини вчиненого, скласти реальний план розслідування і визначити конкретні напрями пошуку слідів злочину.

Список використаних джерел:

[1] Великий тлумачний словник сучасної української мови. Уклад. і голов. ред. В.Т. Бусел. Київ, Ірпінь: Перун, 2001. 1440 с.

[2] Курс криминалистики. Общая часть. За ред. В.Е. Корноухова. Москва: Юристъ, 2000. 784 с.

[3] Коновалова В.О. Вбивство: мистецтво розслідування: монографія. Харків: Факт, 2001. 311 с.

[4] Шавер Б.М., Винберг А.И. Криминалистика. Москва: Юриздат, 1950. 324 с.

[5] Шавер Б.М. Криминалистика. Москва: Юриздат, 1952. 412 с.

[6] Куранова Э.Д. Об основных положениях методики расследования отдельных видов преступлений. *Вопросы криминалистики.* 1962. № 6–7. С. 152–167.

[7] Колесниченко А.Н. Общие положения методики расследования отдельных видов преступлений. Харьков: Изд-во Харьков. юрид. ин-та, 1965. 28 с.

[8] Благута Р.І., Сибірна Р.І., Бараняк В.М. та ін. Криміналістика: навч. посіб. За ред. Є.В. Пряхіна. Київ: Атіка, 2012. 496 с.

[9] Зуйков Г.Г. Криминалистическое учение о способе совершения преступления: дис. … доктора юрид. наук. Москва, 1970. 395 с.

[10] Белкин Р.С. Курс криминалистики: учеб. пособие. Москва: Юнити-Дана, 2001. 837 с.

[11] Біленчук П.Д., Лисиченко В.К., Клименко Н.І. та ін. Криміналістика: підручник. За ред. П.Д. Біленчука. Київ: Атіка, 2001. 544 с.

[12] Уткин М.С. Особенности расследования и предупреждения хищений в потребительской кооперации. Свердловск: Изд-во Свердл. юрид. ин-та, 1975. 57 с.

[13] Розслідування окремих видів злочинів: навчальний посібник. За ред. М.А. Погорецького, Д.Б. Сергєєвої. Київ: Алерта, 2015. 536 с.

[14] Computer. URL: www.oxfordlearnersdictionaries.com/definition/english/computer (дата звернення: 13.03.2020).

[15] Батурин Ю.М., Жодзишский А.М. Компьютерная преступность и компьютерная безопасность. Москва: Юридическая литература, 1991. 157 с.

[16] Криминалистика: учебник. Под. ред. А.В. Волынского. Москва: Закон и право; Юнити-Дана, 1999. 615 с.

[17] Паламарчук Л.П. Криміналістичне забезпечення розслідування незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: дис. … канд. юрид. наук. Київ, 2004. 214 с.

[18] Вехов В.Б. Компьютерные преступления: способы совершения, методика расследования. Москва, 1996. 182 с. URL: https://lawbook.online/kriminalisticheskaya-metodika-uchebnik/sposobyi-sovershheniya-kompyuternyih-30023.html (дата звернення: 13.03.2020).

[19] Конвенція про кіберзлочинність: міжнародний документ від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 13.03.2020).

[20] Кримінальний кодекс України: Закон України від 05.04.2001. URL: https://zakon.rada.gov.ua/laws/show/2341-14 (дата звернення: 13.03.2020).

[21] Федоров В.В. Компьютерные преступления: выявление, расследование и профілактика. *Законность.* 1994. № 6. С. 45–46.

[22] Шкідливі програми: поняття, ознаки, класифікація. URL: http://elartu.tntu.edu.ua/bitstream/lib/27244/2/IMST_2018_Sinkovskyi_D-Shkidlyvi_prohramy_poniattia_55.pdf (дата звернення: 13.03.2020).

[23] WannaCry. URL: https://uk.wikipedia.org/wiki/WannaCry (дата звернення: 13.03.2020).

[24] Вехов В.Б., Голубев В.А. Расследование компьютерных преступлений в странах СНГ: монография. Волгоград: ВА МВД России, 2004. 304 с.

[25] Про захист суспільної моралі: Закон України від 20.11.2003. URL: https://zakon.rada.gov.ua/laws/show/1296-15 (дата звернення: 13.03.2020).

References:

[1] Busel, V.T. (Eds.). (2001). *Velykyi tlumachnyi slovnyk suchasnoi ukrainskoi movy [Big explanatory dictionary of the modern Ukrainian language]*. Kiev, Irpen: Perun [in Ukrainian].

[2] Kornoukhov, V.E. (Eds.). (2000). *Kurs kriminalistiki. Obshhaia chast [The course of criminology. General part]*. Moscow: Yurist [in Russian].

[3] Konovalova, V.O. (2001). *Vbyvstvo: mystetstvo rozsliduvannia: monohrafiia [Murder: the art of investigation: monograph]*. Kharkiv: Fact. [in Ukrainian].

[4] Shaver, B.M., & Vinberg, A.I. (1950). *Kriminalistika [Criminalistics]*. Moscow: Jurizdat [in Russian].

[5] Shaver, B.M. (1952). *Kriminalistika [Criminalistics]*. Moscow: Jurizdat [in Russian].

[6] Kuranova, E.D. (1962). Ob osnovnykh polozheniiakh metodiki rassledovaniia otdelnykh vidov prestuplenii [On the main provisions of the methodology of investigation of certain types of crimes]. *Voprosy kriminalistiki, # 6-7,* 152-167 [in Russian].

[7] Kolesnichenko, A.N. (1965). *Obshhiie polozheniia metodiki rassledovaniia otdelnykh vidov prestuplenii [General provisions of methods of investigation of certain types of crimes]*. Kharkov [in Russian].

[8] Blahota, R.I., Sibirny, R.I. & Baranak, V.M. (2012). *Kryminalistyka: navch. posib. [Criminalistics: teach. manual]*. Ye.V. Priakhina (Ed.). Kyiv: Atika [in Ukrainian].

[9] Zujkov, G.G. (1970). Kriminalisticheskoie ucheniie o sposobe sovershheniia prestupleniia [Criminalistic science about the method of committing a crime]. *Doctor's thesis.* [in Russian].

[10] Belkin, R.S. (2001). *Kurs kriminalistiki: ucheb. posobiie dlia vuzov [Course of criminalistics: teach. manual for high schools]*. 3rd ed., add. Moscow: Unity-Dana [in Russian].

[11] Bilenchuk, P.D., Lisichenko, V.K., & Klimenko, N.I. et al. (2001). *Kryminalistyka: pidruchnyk [Criminalistics: textbook]*. P.D. Bilenchuk (Ed.). Kyiv: Atika [in Ukrainian].

[12] Utkin, M.S. (1975). *Osobennosti rassledovaniia i preduprezhdeniia khishchenii v potrebitelskoi kooperatcii [Features of investigation and prevention of theft in consumer cooperation]*. Sverdlovsk: Izd-vo Sverdl. yurid. in-ta [in Russian].

[13] *Rozsliduvannia okremykh vydiv zlochyniv: navchalnyi posibnyk [Investigation of certain types of crimes: teach. manual]*. (2015). Edited by Pogoretsky, M.A., & Sergeeva, D.B. Kyiv: Alerta [in Ukrainian].

[14] Computer. *www.oxfordlearnersdictionaries.com*. Retrieved from www.oxfordlearnersdictionaries.com/definition/english/computer [in English].

[15] Baturin, Ju.M., & Zhodzishskij, A.M. (1991). *Kompiuternaia prestupnost i kompiuternaia bezopasnost [Computer crime and computer security]*. Moscow: Yuridicheskaia literatura [in Russian].

[16] *Kriminalistika: uchebnik [Criminalistics: textbook]*. (1999). A.V. Volynskij (Ed.). Moscow: Zakon i pravo, Unity-Dana [in Russian].

[17] Palamarchuk, L.P. (2004). Kryminalistychne zabezpechennia rozsliduvannia nezakonnoho vtruchannia v robotu elektronno-obchysliuvalnykh mashyn (kompiuteriv), system ta kompiuternykh merezh [Criminalistic support of investigation of illegal interference in the work of electronic computers (computers), systems and computer networks]. *Candidate's thesis* [in Ukrainian].

[18] Vehov, V.B. (1996). *Kompiuternyie prestupleniia: sposoby sovershenіia, metodika rassledovaniia [Computer crimes: methods of commission, methods of investigation]*. Moscow. Retrieved from https://lawbook.online/kriminalisticheskaya-metodika-uchebnik/sposobyi-soversheniya-kompyuternyih-30023.html [in Russian].

[19] Konventsiia pro kiberzlochynnist: mizhnarodnyi dokument [Convention on cybercrime: international document]. (2001). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575 [in Ukrainian].

[20] Kryminalnyi kodeks Ukrainy vid 05.04.2001 [Criminal code of Ukraine of 05.04.2001]. Retrieved from https://zakon.rada.gov.ua/laws/show/2341-14 [in Ukrainian].

[21] Fedorov, V.V. (1994). *Kompiuternyie prestupleniia: vyiavleniie, rassledovaniie i profilaktika* [Computer crimes: detection, investigation and prevention]. *Zakonnost, 6,* p. 45-46 [in Russian].

[22] Shkidlyvi prohramy: poniattia, oznaky, klasyfikatsiia [Malware: concept, features, classification]. *elartu.tntu.edu.ua*. Retrieved from http://elartu.tntu.edu.ua/bitstream/lib/27244/2/IMST_2018_Sinkovskyi_D-Shkidlyvi_prohramy_poniattia_55.pdf [in Ukrainian].

[23] WannaCry. *uk.wikipedia.org*. Retrieved from https://uk.wikipedia.org/wiki/WannaCry [in Ukrainian].

[24] Vekhov, V.B., & Golubev, V.A. (2004). *Rassledovaniie kompiuternykh prestuplenii v stranah SNH: monografiia [Investigation of computer crimes in the CIS countries: monograph]*. Volgograd: VA Ministry of internal Affairs of Russia [in Russian].

[25] Pro zakhyst suspilnoi morali: Zakon Ukrainy vid 20.11.2003 [On the protection of public morals: Law of Ukraine of 20.11.2003]. *zakon.rada.gov.ua.* Retrieved from https://zakon.rada.gov.ua/laws/show/1296-15 [in Ukrainian].

Biography of the author:

Name: Nedilko Yaroslav.
Academic titles: PhD student.
Organization: Taras Shevchenko National University of Kyiv.
Personal e-mail: nedilkoyaroslav@gmail.com.