Латиш Катерина Володимирівна,
кандидатка юридичних наук,
асистентка кафедри криміналістики,
Національний юридичний університет
імені Ярослава Мудрого, Україна, м. Харків
e-mail: latysh78@gmail.com
ORCID 0000-0002-9110-116X

doi: 10.21564/2414–990X.153.230429
УДК 343.34

КРИМІНАЛІСТИЧНИЙ АНАЛІЗ КІБЕРІНСТРУМЕНТІВ ВЧИНЕННЯ ЗЛОЧИНІВ

Досліджується використання інформаційно-комунікаційних технологій, що використовуються як кіберінструменти для вчинення злочинів. Аналізується емпірична база кіберзлочинів з урахуванням останніх тенденцій, зумовлених пандемією, що триває.

Ключові слова: кіберзлочини; інформаційно-комунікаційні технології; криміналістичний аналіз; «ботоферми»; кіберінструменти.

Латыш К. В., кандидат юридических наук, ассистент кафедры криминалистики, Национальный юридический университет имени Ярослава Мудрого, Украина, г. Харьков.
e-mail: latysh78@gmail.com ; ORCID 0000-0002-9110-116X

Криминалистический анализ киберинструментов совершения преступлений

Статья посвящена исследованию использования информационно-коммуникационных технологий, которые используются в качестве киберинструментов для совершения преступлений. Анализируется эмпирическая база киберпреступлений с учетом последних тенденций, обусловленных длящейся пандемией.

Ключевые слова: киберпреступления; информационно-коммуникационные технологии; криминалистический анализ; «ботофермы»; киберинструменты.

Постановка проблеми. Пандемія коронавірусу триває вже більше року і змусила майже всі сфери життя перейти в онлайн та використовувати дистанційні інструменти комунікації. Так само і злочинці все частіше почали використовувати інформаційно-телекомунікаційні мережі та кіберінструменти для вчинення протиправних діянь, що дозволяє їм краще маскуватися. Так, зокрема відеоплатформа Zoom також стала майданчиком для викрадення персональних даних користувачів.

Аналіз останніх досліджень і публікацій. Різні аспекти кіберзлочинів розглядали у своїх працях, зокрема, такі науковці, як Г. К. Авдєєва (G. K. Avdieieva),

Ю. А. Бельський (Yu. A. Belskyi), С. А. Буяджи (S. A. Buiadzhy), І. І. Васильковський (I. I. Vasylkovskyi), Б. М. Головкін (B. M. Holovkin), В. А. Журавель (V. A. Zhuravel), О. О. Золотар (O. O. Zolotar), Н. В. Карчевський (N. V. Karchevskyi), Ю. І. Когут (Yu. I. Kohut), М. О. Кравцова (M. O. Kravtsova), Л. В. Лефтеров (L.V. Lefterov), Ю. М. Піцик (Yu. M. Pitsyk), С. М. Правдюк (S. M. Pravdiuk), Д. О. Ричка (D. O. Rychka), Л. Є. Стрельцов (L. E. Streltcov), Є. С. Шевченко (Ie.S. Shevchenko), В. Ю. Шепітько (V.Yu. Shepitko), М. Ю. Яцишин (M.Y.Yatsyshyn) та ін. Однак наукових досліджень щодо криміналістичного аспекту використовуваних кіберзнарядь для вчинення злочинів майже немає. З огляду на це ***мета статті*** полягає у криміналістичному дослідженні кіберінструментів, які використовують злочинці для вчинення злочинів.

Виклад основного матеріалу. Як відомо, кіберзлочинність визнана однією з глобальних проблем у контексті міжнародної безпеки. Рівень латентності цих злочинів сягає 90–95%, а статистичні дані не відбивають повною мірою ситуацію з кіберзлочинністю в Україні [1, с. 335].

Мережа Інтернет являє собою просторову структуру, яка включає ієрархію різних учасників: установ реєстрації доменних імен і безлічі посередників, розподілених асиметричним способом (операторів системи і інших). Усі вони забезпечують кінцевим користувачам можливість доступу до мережевих протоколів і вебсерверів (Zagaris, 1993). Віртуальний простір став самостійним місцем існування людського інтелекту і, як будь-яка об'єктивна реальність, породив безліч проблем, у тому числі і правових [2, с. 203].

Для боротьби з організованою злочинністю успішно використовується метод «Big Data», а для протидії кіберзлочинам добре зарекомендувала себе технологія «Block Chain». В умовах активної цифрової трансформації економіки і суспільства з'являються все нові і нові форми об'єктивно небезпечної поведінки, насамперед у кіберпросторі, а також пов'язаних із глобалізацією економіки та відносин між людьми [3, с. 173].

З огляду на низький рівень розкриття кіберзлочинів вбачається необхідність комплексного розроблення нових засобів та прийомів, що враховують сучасні досягнення криміналістики і суміжних наук. Безперечно, це також вимагає відповідного високого професійного рівня знань слідчих у галузі комп'ютерних технологій та постійної їх актуалізації. Але, на жаль, чимало слідчих не володіють належними навиками інтернет-користувача, і тим паче спеціальною освітою у сфері інформаційних технологій. Тому надзвичайно важливою є взаємодія з іншими фахівцями у цій галузі.

Ще однією проблемою під час розслідування кіберзлочинів є несвоєчасне виявлення таких злочинів, тобто з моменту вчинення злочину проходить значний проміжок часу, що значно ускладнює пошук та фіксацію залишених електронних слідів.

Відсутність напрацьованої слідчої та судової практики з цієї категорії злочинів також становить проблему.

Для вчинення кіберзлочинів використовують заражені мобільні пристрої, унікальне шкідливе програмне забезпечення, здійснюють несанкціоновані цільові атаки на певні об'єкти з проникненням у внутрішні мережі з метою отримання доступу до конфіденційної інформації, уведення в комп'ютерну програму команд, що дають змогу здійснювати незапланові функції («троянський кінь»); модифікація комп'ютерної програми («містифікація»); доступ до баз даних і файлів шляхом знаходження слабких місць у системах захисту («маскарад»); використання помилок і недоліків у комп'ютерній програмі [4, с. 941–944].

Як демонструє слідча практика, частіше з заявами про кіберзлочини звертаються саме юридичні особи приватного та публічного права, ніж громадяни. Це зумовлено зокрема тим, що приватні особи побоюються розголошення конфіденційної інформації широкому загалу у зв'язку з кібератакою.

Класифікація кіберзлочинів, викладена у Конвенції Ради Європи про кіберзлочинність, передбачає чотири компоненти. Так, до першої групи належать протиправні дії, які посягають на цілісність, конфіденційність та доступність комп'ютерних даних і систем (несанкціонований доступ і втручання у бази даних, систему): незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), вплив на комп'ютерні дані (ст. 4) або на системи (ст. 5), протизаконне використання спеціальних технічних пристроїв (ст. 6). Злочини другої групи пов'язані з використанням комп'ютера як засобу маніпуляції з інформацією (наприклад, інтернет-шахрайство та комп'ютерна підробка (ст. 7–8)). Третя група пов'язана зі змістом контенту, який розміщується в інтернет-просторі (наприклад, розміщення дитячої порнографії). Четверта група включає у себе злочини, пов'язані з порушенням авторського права та суміжного права [5].

Складна епідеміологічна ситуація у світі стимулювала злочинців так само змінити «поле діяльності» з офлайн у онлайн. Так, у зв'язку з переходом усіх сфер життя у онлайн простір як засіб комунікації активно використовується відеоплатформа Zoom, що стала об'єктом нападу кіберзлочинців. Версія даного програмного забезпечення для Windows має вразливість у чаті, в якому учасники зустрічей можуть спілкуватися між собою, надсилаючи текстові повідомлення. Натискання на посилання із UNC, що вказує розташування файлу в файловій системі, може дозволити зловмисникам красти дані облікового запису Windows. Наприклад, звичайна URL-адреса, але із UNC (\\ evil.server. com \ images \ cat.jpg) перетворюється у гіперпосилання, на яке можна натиснути аби відкрити вебсторінку у своєму браузері, але в такому разі Windows спробує під'єднатися до віддаленого сайту за допомогою протоколу обміну файлами SMB, щоб відкрити віддалений файл cat.jpg. Здійснюючи це, Windows за замовчуванням надсилає ім'я користувача та хеш пароль NTLM, який можна відновити за допомогою безкоштовних інструментів, таких як Hashcat [6].

Кіберзлочинці умисно одночасно створюють більше тисячі різних IP-адрес задля унеможливлення ідентифікації свого місцезнаходження та використовуваних знарядь.

Новелою є створення та застосування так званих «ботоферм» для вчинення різних видів злочинів: не лише корисливих, але й тих, що посягають на територіальну цілісність та недоторканність України. Співробітники Служби безпеки України встановили, що «ботоферма» створювала і управляла обліковими записами в соціальних мережах, які нібито належали громадянам України, хоча насправді використовували несправжні персональні дані. Потужність «ботоферми» складала понад 5000 спамерських пошукових роботів. Відповідне телекомунікаційне обладнання та спеціалізоване програмне забезпечення організатори придбали через заборонені в Україні російські небанківські платіжні системи. Вони використовували також SIM-карти українських операторів зв'язку і proxy-сервери вітчизняного сегмента Інтернет. Аналіз контенту, який поширювала «ботоферма», виявив публічні заклики до насильницької зміни конституційного ладу і захоплення державної влади. Крім того, боти поширювали неправдиву інформацію про ситуацію в Україні, що виникла через пандемію COVID-19 [7, с. 26].

Криптовалюта використовується для анонімізіції усіх розрахунків за вчинення протиправних дій.

Як кіберінструменти пошуку інформації можуть також використовувати різноманітні сервіси, зокрема, такі, як «Whois», за допомогою якого можна встановити адресу та назву провайдера, а з використанням сайту www.ripe.net або утиліти nslookup (з англійської «name server lookup») отримати IP-адресу. Час роботи користувача в мережі можна встановити за спеціальним log-файлом (журналом). Додаткові відомості про вид, порядок і час підключень користувача до мережі Інтернет і збіг цих даних із log-файлом провайдера може слугувати вагомим доказом несанкціонованого доступу в певну комп'ютерну систему [8, с. 58]. Саме використовуючи такі сервіси, зловмисники ідентифікують та організовують кібератаки на електронні ресурси органів державної влади з метою подальшого їхнього використання у протиправних цілях. Особливо поширеними такі випадки стали після того, як були оприлюднені бази даних з доменними іменами та реальними IP-адресами цих органів, доступ до яких здійснювався через DNS-запити.

Доволі поширеними є випадки, коли від імені псевдодержавних установ надсилаються повідомлення зі шкідливим програмним забезпеченням. Але якщо раніше відмінною особливістю було те, що такі листи надсилалися з традиційних поштових сервісів, які у вільному доступі, то тепер використовуються й псевдоурядові «@gov.ua». У цих повідомленнях містяться файли у звичних форматах з розширенням «.pdf», «.docx», але із вбудованим шкідливим «OLE» об'єктом. Після відкриття документа користувачем запускається шкідливе програмне забезпечення (далі – ШПЗ). Автоматично відбувається додавання запису в реєстр операційної системи для його автозавантаження. Кожен раз ШПЗ запускалось із теки системного диска за посиланням - :\ ProgramData\Microtik\winserv.exe. Виявлене шкідливе програмне забезпечення переходило у прихований режим очікування з'єднання та повною мірою

надавало доступ до ресурсів комп'ютера жертви. Згідно з результатами аналізу вказане ШПЗ є модифікованою версією легального програмного забезпечення «RMS TektonIT» [9].

RAR-архів постійно використовується кіберзлочинцями для вчинення протиправних дій. Так, на початку 2021 р., начебто від імені Адміністрації Держспецзв'язку України, з поштової скриньки zapros@dsszzi.gov.ua надсилався запаролений архів «Електронний запит.rar», який був трояном для віддаленого доступу (RAT) з IP-адреси 212.44.151.60, яка належить до пулу адрес провайдера «Vimpelcom» Російської Федерації [10]. До посадових осіб приватного сектору економіки також надсилалися листи з вкладення з розширенням .lzh (архів), який містив в собі два файли, один з яких був підробленим або раніше викраденим документом формату .xlsx (для прикриття), а інший – JS-скрипт, який при активації завантажує шкідливе програмне забезпечення #Smokeloader в директорію %Temp%, яке використовується для завантаження інших шкідливих програмних забезпечень [11].

У 2019 р. кіберзлочинці як знаряддя знову ж таки використовували традиційну програму WinRAR exploit (#CVE-2018-20250). Так, здійснювалася розсилка архіву zakon.rar в якому містився PDF документ із законом про державне партнерство, після його розпакування вірус завантажував powershell скрипти з їх подальшим виконанням. Таким чином файл розпаковувався з архіву в потрібну зловмиснику папку, а не призначену користувачем. Тобто розміщувався шкідливий код у папку автозавантаження Windows, який автоматично виконувався при кожному завантаженні системи [12].

У 2020 р. найбільш поширеним ШПЗ став Agent Tesla, який виконує функції кейлогера (keylogger), викрадача інформації (stealer) та є вдосконаленим трояном віддаленого доступу (RAT), що написане мовами, які використовуються в Microsoft.Net (C #, Visual Basic .NET, C++/CLI, тощо). Наразі ШПЗ здатне відслідковувати та збирати дані вводу з клавіатури, робити скріншоти та отримувати облікові дані, що використовуються в різних програмах системи (наприклад, Google Chrome, Mozilla Firefox, Microsoft Outlook, IceDragon, FILEZILLA тощо). З'явився Agent Tesla в 2014 р. і виконував функції кейлогера та викрадача паролів. Дане ШПЗ є комерційним, ліцензію на його використання можна придбати на сайті розробників, однак Agent Tesla має використовуватись лише у межах, визначених законом [13].

Зустрічаються випадки, коли як знаряддя злочину використовують звичайні роутери з під'єднаною антеною, яку розміщують на горищі, внаслідок чого радіоелектронний засіб виводиться на рівень з широкосмуговим доступом, для якого необхідно отримати дозвіл. Далі здійснюється блокування сигналу (інформації) з антени РЕЗ ПАТ «Укртелеком», який надходить споживачам телекомунікаційних послуг, незаконно діючою радіоелектронною базовою станцією, розташованою на даху за допомогою радіоелектронного засобу з широкосмуговим радіодоступом, ідентифікованого під назвою D-Link, що частково блокувала сигнал (інформації) [14].

Розкриття кіберзлочинів залишається доволі складним завданням для більшості співробітників органів досудового розслідування, що обумовлено специфікою цього виду злочину. Наявні складнощі з узагальненням матеріалів слідчої та судової практики щодо кіберзлочинів, бракує методичних рекомендацій як з організації розслідування кіберзлочинів, так і з тактики проведення слідчих (розшукових) дій; недостатньою є кваліфікація слідчих для роботи зі специфічними джерелами доказової інформації, оцифрованої у вигляді електронних повідомлень, сторінок, сайтів.

Висновки. Невпинний розвиток інформаційних технологій призвів не лише до позитивних змін у суспільстві, але й появи нових форм злочинності. Така ситуація зумовлена диджиталізацією усіх сфер життя, високою технічною оснащеністю злочинців та застарілістю методів роботи слідства. Типові сліди кіберзлочинів мають електронно-цифрове відображення та складаються з певних змістовно наповнених інформаційних блоків.

Список літератури

1. Кримінологія: Загальна та Особлива частини : підручник / В. В. Голіна, Б. М. Головкін, М. Ю. Валуйська, О. В. Лисодєд та ін. ; за ред. В. В. Голіни і Б. М. Головкіна. Харків : Право, 2014. 440 с.

2. Таволжанський О. В. Сучасні реалії кіберпростору України. *Забезпечення правопорядку в умовах коронакризи* : матеріали панельної дискусії IV Харків. міжнар. юрид. форуму, м. Харків, 23–24 верес. 2020 р. Харків, 2020. С. 203–208.

3. Головкін Б. М. Теперішнє і майбутнє кримінології. *Проблеми законності*. 2020. Вип. 149. С. 168–184. doi: https://doi.org/10.21564/2414-990x.149.200724.

4. Черніков Б. Ю. Кримінологічна характеристика кіберзлочинності. *Молодий вчений*. 2018. № 11 (63). С. 941–944.

5. Конвенції Ради Європи про кіберзлочинність. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text (дата звернення: 30.04.2021).

6. Вразливість в Zoom для Windows. URL: https://cert.gov.ua/article/27 (дата звернення: 30.04.2021).

7. Кібербезпека в інформаційному суспільстві : Інформаційно-аналітичний дайджест / відп. ред. О. Довгань; упоряд. О. Довгань, Л. Литвинова, С. Дорогих; Науково- дослідний інститут інформатики і права НАПрН України; Національна бібліотека України ім. В. І. Вернадського. № 4 (квітень). Київ, 2020. 113 с.

8. Інноваційні засади техніко-криміналістичного забезпечення діяльності органів кримінальної юстиції : монографія / кол. авт. В. Ю. Шепітько, В. А. Журавель, Г. К. Авдєєва та ін. ; за ред. В. Ю. Шепітька, В. А. Журавля. Харків : Вид. агенція «Апостіль», 2017. 260 с.

9. Кіберполіція фіксує випадки розповсюдження вірусу замаскованого під повідомлення від держустанов. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-fiksuje-vipadki-rozpovsyudzhennya-virusu-zamaskovanogo-pid-povidomlennya-vid-derzhustanov/ (дата звернення: 30.04.2021).

10. Масштабна фішингова атака на державні установи України 19.01.2021. URL: https://cert.gov.ua/article/10011 (дата звернення: 30.04.2021).

11. Нові хвилі масових розсилок листів з #Smokeloader. URL: https://cert.gov.ua/article/2707 (дата звернення: 30.04.2021).

12. Зараз в Україні активно розповсюджується шкідливе програмне забезпечення, яке використовує WinRAR exploit (#CVE-2018-20250). URL: https://cert.gov.ua/article/2695 (дата звернення: 30.04.2021).

13. Agent Tesla (шкідливе програмне забезпечення). URL: https://cert.gov.ua/article/3028 (дата звернення: 30.04.2021).

14. Вирок Іванівського районного суду Херсонської області від 7 жовтня 2020 р. по справі №659/829/15-к. URL: https://reyestr.court.gov.ua/Review/92093560 (дата звернення: 30.04.2021).

References

1. Holina, V.V., Holovkin, B.M., Valuiska, M.Yu., Lysodied, O.V. et al. (2014). Kryminolohiia: Zahalna ta Osoblyva chastyny. V. V. Holina, B. M. Holovkin (Eds.). Kharkiv: Pravo [in Ukrainian].

2. Tavolzhanskyi, O.V. (2020). Suchasni realii kiberprostoru Ukrainy. Zabezpechennia pravoporiadku v umovakh koronakryzy: materialy panelnoi dyskusii IV Kharkiv. mizhnar. yuryd. forumu, m. Kharkiv, 23–24 veres. 2020 r. Kharkiv, *203–208* [in Ukrainian].

3. Holovkin, B.M. (2020). Teperishnie i maibutnie kryminolohii [Current and future criminology]. *Problemy zakonnosti – Problems of Legality, issue 149, 168–184.* doi: https://doi.org/10.21564/2414-990x.149.200724 [in Ukrainian].

4. Chernikov, B.Iu. (2018). Kryminolohichna kharakterystyka kiberzlochynnosti. *Molodyi vchenyi, 11 (63), 941–944* [in Ukrainian].

5. Konventsii Rady Yevropy pro kiberzlochynnist. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian].

6. Vrazlyvist v Zoom dlia Windows. URL: https://cert.gov.ua/article/27 [in Ukrainian].

7. Kiberbezpeka v informatsiinomu suspilstvi: Informatsiino-analitychnyi daidzhest (2020). O. Dovhan, L. Lytvynova, S. Dorohykh (Eds.). Naukovo-doslidnyi instytut informatyky i prava NAPrN Ukrainy; Natsionalna biblioteka Ukrainy im. V.I.Vernadskoho. № 4 (kviten). Kyiv [in Ukrainian].

8. Shepitko, V.Yu., Zhuravel, V.A., Avdieieva, H.K. et al. (2017). Innovatsiini zasady tekhniko-kryminalistychnoho zabezpechennia diialnosti orhaniv kryminalnoi yustytsii. V. Yu. Shepitko, V. A. Zhuravel (Eds.). Kharkiv: Vyd. ahentsiia «Apostil» [in Ukrainian].

9. Kiberpolitsiia fiksuie vypadky rozpovsiudzhennia virusu zamaskovanoho pid povidomlennia vid derzhustanov. URL: https://www.npu.gov.ua/news/kiberzlochini/kiberpolicziya-fiksuje-vipadki-rozpovsyudzhennya-virusu-zamaskovanogo-pid-povidomlennya-vid-derzhustanov/ [in Ukrainian].

10. Masshtabna fishynhova ataka na derzhavni ustanovy Ukrainy 19.01.2021. URL: https://cert.gov.ua/article/10011 [in Ukrainian].

11. Novi khvyli masovykh rozsylok lystiv z #Smokeloader. URL: https://cert.gov.ua/article/2707 [in Ukrainian].

12. Zaraz v Ukraini aktyvno rozpovsiudzhuietsia shkidlyve prohramne zabezpechennia, yake vykorystovuie WinRAR exploit (#CVE-2018-20250). URL: https://cert.gov.ua/article/2695 [in Ukrainian].

13. Agent Tesla (shkidlyve prohramne zabezpechennia). URL: https://cert.gov.ua/article/3028 [in Ukrainian].

14. Vyrok Ivanivskoho raionnoho sudu Khersonskoi oblasti vid 7 zhovtnia 2020 r. po spravi № 659/829/15-k. URL: https://reyestr.court.gov.ua/Review/92093560 [in Ukrainian].

Latysh K. V., PhD in Law, Assistant of Criminalistics Department, Yaroslav Mudryi National Law University, Ukraine, Kharkiv.

e-mail: latysh78@gmail.com ; ORCID 0000-0002-9110-116X

Criminalistics analysis of cyber tools for committing crimes

The article is devoted to the problems of the information and communication technologies which are used as cyber tools for committing crimes. Due to the coronavirus and the widespread lockdown, crimes have also moved to online space. The empirical base of cybercrime is analyzed taking into consideration the latest trends caused by the ongoing pandemic. Mostly this category of crimes is latent and quite difficult to investigate. Especially due to the lack of knowledge in the field of informatics, which is constantly being transformed (changed), by investigators and other participants of the pre-trial investigation. Modern

scientific and technical tools are needed to detect, collect and fixed electronic traces of cybercrimes. It should be enhance the technical capabilities of forensic laboratories that specialize in the investigation of cybercrimes related to the use of information technology. But there is a problem because of lack of financial support and needness quite expensive equipment for conducting new computer expertise. This requires significant additional funding, which is not fully provided to the police station by the government. Cybercrime is a transnational crime that has no borders. Criminals from different countries can unite and detect such complicity in a timely manner is quite difficult. So it is necessary international cooperation with FBI, Interpol and other organizations, law-enforcement bodies. During the investigation it should be reconstruct the stages of the hacker's growth and return to his the very beginning, when he was not a such professional, but only gaining experience. The complication of identifying criminals is also that they use traditional tools such as Wi-Fi routers and non-traditional ones such as "boto-farms" which are used as cybertools for committing the crime.

Keywords: cybercrime; information and communication technologies; forensic analysis; «bot-farms»; cybertools.

Рекомендоване цитування: Латиш К. В. Криміналістичний аналіз кіберінструментів вчинення злочинів. *Проблеми законності*. 2021. Вип. 153. С. 165–172. doi: https://doi.org/10.21564/2414-990X.153.230429.

Suggested Citation: Latysh, K.V. (2021). Kryminalistychnyi analiz kiberinstrumentiv vchynennia zlochyniv [Criminalistics analysis of cyber tools for committing crimes]. *Problemy zakonnosti – Problems of Legality, issue 153, 165–172*. doi: https://doi.org/10.21564/2414-990X.153.230429 [in Ukrainian].

Надійшла до редколегії 01.05.2021 р.