DOI: https://doi.org/10.32839/2304-5809/2020-5-81-45
УДК 343.3/.7

Долженко Л.Ю.
Харківський науково-дослідний експертно-криміналістичний центр
Міністерства внутрішніх справ України

КІБЕРЗЛОЧИННІСТЬ: КРИМІНАЛІСТИЧНА ХАРАКТЕРИСТИКА ТА ОСОБЛИВОСТІ РОЗСЛІДУВАННЯ

Анотація. У сучасному світі, з розвитком мережі Інтернет, з'явився новий вид злочинності – кіберзлочинність. Чим більше стає користувачів мережі Інтернет, тим більше шахраїв, які стають більш досвідченими і вигадують нові види шахрайства. Кіберзлочинність становить реальну небезпеку для суспільства і держави, вона здатна спричинити незворотні наслідки. На жаль, багато людей стають жертвами кіберзлочинців. Насамперед це пов'язано з тим, що мало хто приділяє увагу правилам, яких слід дотримуватись, щоб не стати жертвою. Люди мало обізнані з цією тематикою, і саме це є дуже привабливим для злочинців. У статті наведено поняття кіберзлочинності та специфіку вказаного виду злочину; розглянуто об'єктивні та суб'єктивні ознаки для правильної кваліфікації; наведено приклади кіберзлочинів в Україні за останній час та наслідки, які вони завдали; досліджено особливості розслідування кіберзлочинів; запропоновано поради, як не стати жертвою шахраїв та вберегти себе від кіберзлочинності.

Ключові слова: кіберзлочинність, кваліфікація, наслідки, розслідування, шахрайство, вірус Petya, Департамент кіберполіції, короновірус.

Dolzhenko Liubov
Kharkiv Scientific Research Forensic Center of
Ministry of Internal Affairs of Ukraine

CYBER CRIME: CRIMINAL CHARACTERISTICS AND FEATURES OF THE INVESTIGATION

Summary. In today's world, with the development of the Internet, a new type of crime has emerged – cybercrime. The more Internet users, the more fraudsters who become more experienced and invent new types of fraud. Cybercrime – is a real danger to society and the state, it can cause irreversible consequences. The Ukrainian legislator pays great attention to this problem. For the first time, a separate section on cybercrime was enshrined in the Criminal Code of Ukraine. There are also a number of regulations governing the fight against cybercrime. The main ones are the following: Law of Ukraine "On National Police", Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", Law of Ukraine "On Protection of Information in Automated Systems", Convention on Cybercrime, Order of the Ministry of Internal Affairs special police "and a number of others. As practice shows – cybercrime has a latent nature, which complicates the investigation of this type of crime. An important condition for the fight against cybercrime is the training of properly qualified specialists. In Ukraine, there is a Cyberpolice Department of the National Police of Ukraine, whose task is to ensure the country's cybersecurity and prevent cybercrime, but still there is no single base of concepts and terms, not developed forensic techniques and tactics. Unfortunately, many people fall victim to cybercriminals. First of all, this is due to the fact that few people pay attention to the rules that must be followed in order not to become a victim. It is also influenced by the fact that people are little aware of this topic, which is very attractive to criminals. Although many scientists have studied this issue, as practice shows, it is still relevant today. Therefore, the article will present the concept of cybercrime and the specifics of this type of crime; the objective and subjective signs for the correct qualification are considered; examples of cybercrime in Ukraine in recent times and the consequences they have caused are given; features of investigation of cybercrimes are investigated; offers tips on how not to fall victim to scams and protect yourself from cybercrime.

Keywords: cybercrime, qualification, consequences, investigation, fraud, Petya virus, Department of Cyber Police, coronovirus.

Постановка проблеми. Розвиток всесвітньої мережі Інтернет спричинив новий вид злочинності – кіберзлочинність, який з кожним роком набирає свої оберти і несе за собою серйозні, а часом, незворотні наслідки.

Особлива увага приділяється кіберзлочинності, тому що величезний технічний потенціал і безмежні можливості, які має мережа Інтернет, все частіше в сучасному світі можуть бути використані зі злочинною метою.

Дії кіберзлочинців стають більш досконалими, що становить реальну загрозу для суспільства та держави в цілому. Це загострює необхідність боротьби зі злочинами такого роду, створення комп'ютерних систем і технологій з підвищеним рівнем безпеки в мережі Інтернет, а також законодавчої бази, що дозволить притягнути злочинців до відповідальності.

Аналіз останніх досліджень і публікацій. Кіберзлочинці створюють нові методи та способи скоєння злочинів та знаходять помилки в системах безпеки швидше, ніж ті, хто їм протидіє.

Кіберзлочинність – це явище міжнародного значення, рівень якого прямо залежить від рівня розвитку та впровадження сучасних комп'ютерних технологій, мереж їх загального користування та доступу до них.

Основою даної статті стали праці таких українських науковців, як: Р.С. Бєлкіна, В.М. Бутузова, Т.В. Варфаломеєвої, В.Т. Гавловського, В.Д. Маляренка, М.М. Михеєнка, І.Л. Петрухіна, О.Р. Ратінова, В.М. Тертишника, Л.Д. Удало-

вої, В.Ю. Шепітька, а також інших науковців, які зробили вагомий внесок у дослідження проблематики розслідування кіберзлочинів, проведенні досудового розслідування з метою притягнення винних осіб до кримінальної відповідальності за вказаний вид злочинів.

Виділення невирішених раніше частин загальної проблеми. На даний час існує дуже велика кількість видів кіберзлочинів. З кожним днем шахраї вигадують все нові види заробітку для себе і, на жаль, людина не може встигнути захистити себе і проаналізувати ситуацію, в якій опинилась. Питання залишається актуальним та необхідним для дослідження і сьогодні. Саме тому окремі аспекти потребують більш детального вивчення. Наприклад: які найпопулярніші види шахрайства існують сьогодні та як повинна поводити себе людина, щоб захистити себе, а якщо вона вже стала жертвою, то які потрібно вчинити дії, щоб понести мінімальні втрати?

Мета статті. Виявити специфічні ознаки кіберзлочинності, проаналізувати її основні види та методи розслідування, а також запропонувати поради, як вберегти себе від кіберзлочинів та не стати жертвою шахраїв.

Виклад основного матеріалу дослідження. Термін «кіберзлочин» утворений сполученням двох слів: кіберпростір і злочин. Термін «кіберпростір» позначає інтерактивний інформаційний простір, що моделюється за допомогою комп'ютера. Використання цього терміна поширене у світовій науковій літературі.

В українському законодавстві кіберзлочин розуміється як суспільно небезпечне винне діяння у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [5].

Специфіка даного виду злочинності полягає у:

– комфортності вчинення злочинів, тобто їх підготовка та скоєння здійснюється, практично, не відходячи від «робочого місця»;

– доступності – тому що існує тенденція постійного зниження цін на комп'ютерну техніку. Майже у кожної людини є комп'ютер або мобільний телефон з підключенням до мережі Інтернет;

– широкій географії скоєння злочинів, але враховуючи те, що основна кількість комп'ютерів розташована у великих населених пунктах, то саме на них і припадає більша частина злочинності;

– віддаленості об'єкту злочинних посягань – він може знаходитись за тисячі кілометрів від місця скоєння злочину;

– складності виявлення, фіксації та вилучення криміналістично-значущої інформації при здійсненні оперативно-розшукових та слідчих дій для використання її в якості речового доказу.

Слід зауважити, що український законодавець приділяє велику увагу цій проблемі: вперше новий Кримінальний кодекс України передбачив самостійний розділ про ці злочини, а саме розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», що свідчить про актуальність цієї проблеми в суспільстві, зокрема статті 361, 361^1, 361^2,362, 363, 363^1 Кримінального кодексу України [1].

Також діяльність кіберзлочинців кваліфікується за ст. 200 КК України «Незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення» та ч. 3 ст. 190 КК України «Шахрайство з використанням електронно-обчислювальної техніки», ст. 231 КК України «Незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю».

Також у Конвенції про кіберзлочинність, що набрала чинності 01.07.2006 року, представлена класифікація кіберзлочинів. Усі вони характеризуються наявністю наміру як елемента суб'єктивної сторони. Всього чотири категорії кіберзлочинів:

1. Злочини проти конфіденційності, цілісності та допустимості комп'ютерних даних і систем – незаконний доступ, незаконне перехоплення, втручання у дані, систему, зловживання пристроями.

2. Комп'ютерні злочини – фальсифікація і підробка, що здійснюються з використанням комп'ютерної техніки.

3. Злочини, пов'язані зі змістом – виробленя з метою розповсюдження, пропонування або надання доступу, розповсюдження або передача, здобуття для себе чи іншої особи, володіння дитячою порнографією за допомогою комп'ютерних систем.

4. Злочини, пов'язані з порушенням авторських та суміжних прав.

Перш за все, для того щоб кваліфікувати діяння як злочин, потрібно визначити його об'єктивні та суб'єктивні ознаки.

Об'єкт злочину – сукупність діянь, що заподіюють шкоду нормальній роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж і мереж електрозв'язку [6].

Родовим об'єктом цієї категорії злочинів є встановлений порядок використання автоматизованих електронно-обчислювальних машин (комп'ютерів), їх систем та комп'ютерних мереж і мереж електрозв'язку.

Безпосереднім об'єктом є право власності на інформацію, для якої її власником встановлюється обмежений (особливий) режим доступу або такий доступ забороняється взагалі з метою недопустимості її доступності з різних причин.

Згідно з Законом України від 5 липня 1994 року «Про захист інформації в автоматизованих системах» предметом злочину можуть бути: автоматизовані системи, носії інформації, інформація, що циркулює в автоматизованих системах.

Суб'єкт злочину загальний, тобто суб'єктом є фізична осудна особа, яка вчинила злочин у віці, з якого відповідно до цього Кримінального кодексу України може наставати кримінальна відповідальність, тобто особа, якій до вчинення злочину виповнилося шістнадцять років [1].

Об'єктивна сторона злочину проявляється у формі несанкціонованого втручання у роботу електронно-обчислювальних машин (комп'ютерів), їх систем, комп'ютерних мереж чи мереж електрозв'язку, наслідком якого є: витік,

втрата, підробка, блокування інформації, спотворення процесу обробки інформації або порушення встановленого порядку її маршрутизації [6].

Суб'єктивна сторона злочину характеризується умисною виною. Злочинні дії можуть бути вчинені лише з прямим умислом, тоді як психічне ставлення винного до наслідків може характеризуватись як умисною (прямим чи непрямим умислом), так і необережною формою вини (злочинною самовпевненістю чи злочинною недбалістю) [6].

Практично кожен чув про кіберзлочинність і, можливо, навіть зіткнувся з нею особисто. Кіберзлочинність включає в себе різні види злочинів, що здійснюються за допомогою комп'ютера або мобільного телефону, а також в мережі Інтернет.

Можна навести декілька прикладів кіберзлочинів, які вважаються найрозповсюдженими на даний час.

Одним з масштабніших злочинів, який заподіяв багато негативних наслідків є «вірус Petya». Це була масштабна хакерська атака. Хакерські атаки в Україні – це цілеспрямовані масштабні хакерські напади на мережі українських державних підприємств, установ, банків, медіа тощо, які відбулись 27 червня 2017 року. У результаті цих атак була заблокована діяльність наступних підприємств: аеропорт «Бориспіль», ЧАЕС, Укртелеком, Укрпошта, Ощадбанк, Укрзалізниця та ряд великих комерційних підприємств. Шахраї вимагали внести визначену грошову суму на їх рахунки для відновлення і подальшої роботи сайтів.

Ще одним прикладом кіберзлочину може бути шахрайство, у якому шахраї в повідомленнях присилають прохання зателефонувати на певний номер, а при розмові запитують конфіденційні дані власника картки. Частіше за все приходить СМС-повідомлення з таким текстом: «Ваша картка заблокована. Баланс 0 грн. Зателефонуйте за певним номером» і вказано мобільний номер. Коли особа телефонує на вказаний номер, шахраї дізнаються реквізити банківської картки особи та під різними приводами схиляють до розголошення даних картки, за допомогою яких можливо здійснювати інтернет-платежі (зокрема, cvv-коду). Потім зловмисники використовують платіжні системи для виведення коштів з картки потерпілого. На жаль, люди не можуть одразу зорієнтуватися та зателефонувати на гарячу лінію банку, яким користуються.

На жаль, Україна зіштовхнулась ще з однією проблемою, такою як COVID-19 (короновірус). Після виявлення цього захворювання, держава повинна була ввести карантинні заходи. Для багатьох людей це велика трагедія, а для шахраїв ще один різновид заробітку. З початку карантину шахраї розсилають СМС-повідомлення або телефонують та повідомляють інформацію про державні компенсації для громадян, такі як: виплата коштів на лікування, придбання тестів для визначення короновірусу, компенсація за втрату місця роботи тощо; розповсюджують фейки з метою поширення паніки та дестабілізації ситуації в країні в умовах карантину; вчиняють певні шахрайські дії з метою заволодіння грошима чи особистими даними під приводом продажу захасних масок, антисептиків, медичного обладнання тощо.

Нещодавно, 14 травня 2020 року було опубліковано відео, на якому кілька молодих людей ламають термінал для поповнення електронних проїзних. На ролику видно двох хлопців, один з яких активно громить термінал. Спочатку б'є по апарату ногами, потім кастетом – в результаті розбиває пластикову вставку. Його напарник проявляє меншу активність і великої шкоди апарату не завдає. Ще одна людина знімає те, що відбувається на відео.

Співробітникам Департаменту кіберполіції вдалося встановити правопорушників – одним із причетних до псування міського майна виявився студент Харківського національного університету міського господарства імені О.М. Бекетова.

За інформацією соцмереж, вандали розгромили термінал в ніч з 13 на 14 травня транслюючи, що відбувається в Instagram.

Для того щоб захистити себе потрібно:

– в жодному разі не повідомляти особисту інформацію;

– не розкривати реквізити банківських карток;

– звертати увагу на рядок адреси сайту. Зрозуміло, що справжні продавці вже зайняли адреси з назвою власного бренду, тому шахраї додають туди ще якесь слово. Наприклад, замість brand.com пишуть brand.hit.com або brand.best.com. Шахраї купляють рекламу на свій сайт і тому у пошуку вони з'являються на першому рядку;

– пошукати відгуки про компанію в соцмережах, але це теж є дуже оманливим, оскільки зараз купити відгуки і накрутити лайки не складає великих складнощів. На мою думку, потрібно писати тим, хто залишає коментарі, і запитувати за ту марку, яка вас цікавить;

– отримувати інформацію лише з перевірених джерел: офіційний сайт Кабінету Міністрів України, Міністерства охорони здоров'я, Міністерства внутрішніх справ;

– купувати товари тільки за допомогою накладеного платежу.

Розслідування таких злочинів ускладняється їх підвищеною латентністю. У злочинців є можливість змінити, приховати комп'ютерні дані, що можуть бути доказами у досудовому розслідуванні. Існує проблема огляду комп'ютерних систем, технічних пристроїв, на яких міститься інформація. Також ускладненою є процедура вилучення, дослідження та фіксації слідів вчинення кіберзлочинів. Цьому сприяє недостатнє технічне забезпечення органів досудового розслідування, оперативних підрозділів. Для розкриття подібних правопорушень обов'язковим є залучення спеціалістів та експертів, що мають спеціальні знання у комп'ютерно-технічній сфері [9].

Першочерговим завданням слідчого на початковому етапі розслідування кіберзлочинів є аналіз інформаційного середовища вчинення злочину:

– визначення типу електронно-обчислювальної машини (носія), де зберігалася або оброблялася комп'ютерна інформація, до якої здійснено неправомірний доступ (Web-сервер, персональний комп'ютер, мобільний телефон, електронна кредитна карта), що визначить напрямок всього подальшого розслідування;

– встановлення типу операційної системи комп'ютера (сервера), до якого здійснено непра-

вомірний доступ (Unix, Linux, Windows тощо), а також використаного для вчинення злочину програмного забезпечення, що значною мірою допоможе звузити коло можливих підозрюваних;

– визначення апаратного та програмного забезпечення, яке піддалося впливу в ході неправомірного доступу, а також інформації про засоби і знаряддя вчинення такого доступу, що дозволить скласти об'єктивну картину слідів злочину [8].

Важливою умовою боротьби з кіберзлочинністю є підготовка фахівців належної кваліфікації для збільшення ефективності розслідування та розкриття злочинів даної специфіки.

В Україні існує Департамент кіберполіції Національної поліції України, завданням якого є забезпечити кібербезпеку країни і запобігти кіберзлочинності. Але немає єдиної бази ключових термінів і понять, не розроблені криміналістичні техніка та тактика, використовуючи які співробітники кіберполіції змогли б ефективніше проводити розслідування кіберзлочинів.

У 2018 році увагу працівників Департаменту кіберполіції було зосереджено на розслідуванні злочинів, вчинених у сфері високих інформаційних технологій. Так, протягом року працівники Департаменту кіберполіції були залучені до розслідування понад 11 тисяч кримінальних проваджень. Найбільша кількість злочинів була скоєна у місті Києві, а також на території Одеської, Миколаївської та Львівської областей.

Згідно зі статистикою, переважна більшість підозрюваних – чоловіки у віці від 25 до 40 років. Найбільше виявлено користувачів шкідливого програмного забезпечення, які вчиняли злочини, використовуючи придбані віруси у DarkNet [10].

За результатами міжнародної співпраці служби безпеки кількох країн знешкодили міжнародну групу кіберзлочинців під назвою Avalanche. В операції з ліквідації злочинної мережі брали участь співробітники правоохоронних органів Болгарії, Німеччини, Грузії, Молдови, США та України.

Крім того, зараз підписано договори про взаємодію у сфері боротьби з кіберзлочинністю з організаціями як державного, так і приватного секторів. Серед них – представники міжнародних кампаній у сфері інформаційної безпеки та IT-компанії, а також поліцією Австралії, Сінгапуру, Катару та ще ряду країн [10].

Висновки та пропозиції. Якщо звернути увагу на вищевикладене, то можна дійти висновку, що кіберзлочинність становить велику небезпеку для усіх сфер життя людини, а також держави в цілому. Для того щоб хоч якось захистити себе і не стати жертвою кіберзлочинів, потрібно дотримуватись наступних порад:

– створювати надійні паролі, які захищають інформацію та періодично їх змінювати;

– бути обізнаним про розповсюджені прийоми, які використовують злочинці для того, щоб розпізнавати їх. І, на мій погляд, це основне. Оскільки, чим більше людина буде знати про види кіберзлочинів, які існують, тим надійніше вона зможе захистити свої дані;

– захищати пристрої, встановлювати ліцензійні антивірусні програми. Тому що не ліцензійні антивіруси, які можна завантажити в мережі Інтернет, можуть приховують у собі вірус;

– використовувати захищені мережі;

– перевіряти свої облікові записи;

– не розголошувати конфіденційну інформацію незнайомцям;

– не натискати на підозрілі вкладення чи посилання від неперевірених контактів;

– не користуватись незахищеним Wi-Fi з'єднанням без нагальної потреби.

Таким чином, сучасний рівень інформатизації суспільства вимагає від України забезпечити належний та ефективний механізм боротьби із кіберзлочинами як однієї із серйозних загроз національній безпеці держави.

Можемо зазначити, що кіберзлочини носять латентний характер, а тому їх виявлення та розслідування становить цілу програму поетапно здійснених заходів, передбачених кримінально-процесуальним законодавством. З однієї сторони є особа, яка володіє знаннями та навичками у сфері IT-технологій, а з іншої – уповноважена службова особа (слідчий, прокурор), які можуть і не знати тонкощі розслідування таких злочинів. Важливим є залучення експертів та спеціалістів на стадії досудового розслідування з метою отримання консультацій, а в подальшому проведення експертиз та складання висновків.

Список літератури:

1. Кримінальний кодекс України : Закон України від 05 квітня 2001 р. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/print (дата звернення: 30.04.2020).
2. Про захист інформації в автоматизованих системах : Закон України від 31 травня 2005 р. № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/2594-15 (дата звернення: 27.04.2020).
3. Про кіберзлочинність : Конвенція від 01 липня 2006 р. URL: https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення: 02.05.2020).
4. Про національну поліцію : Закон України від 02 липня 2015 р. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19 (дата звернення: 30.04.2020).
5. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 р. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/card/2163-19 (дата звернення: 06.05.2020).
6. Науково-практичний коментар до Кримінального кодексу України / відп. ред. С.С. Яценко. 4-те вид., перероб. та доп. Київ : А.С.К., 2005. 848 с. URL: http://ir.nusta.edu.ua/jspui/handle/doc/819 (дата звернення: 06.05.2020).
7. Кіберзлочинність у всіх її проявах: види, наслідки та способи боротьби: веб-сайт. URL: https://www.gurt.org.ua/articles/34602/ (дата звернення: 30.04.2020).
8. Бурбело Б.А. Актуальні питання розслідування кіберзлочинів : матеріали Міжнар. наук.-практ. конф. Харків: 10 груд. 2013 р. МВС України, Харк. нац. ун-т внутр. справ. Харків : ХНУВС, 2013. 272 с. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/553/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf?sequence=1&isAllowed=y (дата звернення: 04.05.2020).
9. Бутузов В.М., Гавловський В.Д., Скалозуб Л.П. та ін. Організаційно-правові та тактичні основи протидії злочинності у сфері високих інформаційних технологій : навчальний посібник. Київ : Нац. акад. СБУ України, 2011. 404 с.

10. Офіційний сайт Департаменту кіберполіції Національної поліції України. URL: https://cyberpolice.gov.ua/results/2018/ (дата звернення: 03.05.2020).

References:

1. Kryminal′nyy kodeks Ukrayiny: Zakon Ukrayiny vid 05 kvitnya 2001 r. № 2341-III. URL: https://zakon.rada.gov.ua/laws/show/2341-14/print (accessed 30.04.2020).
2. Pro zakhyst informatsiyi v avtomatyzovanykh systemakh: Zakon Ukrayiny vid 31 travnya 2005 r. № 2594-IV. URL: https://zakon.rada.gov.ua/laws/show/2594-15 (accessed 27.04.2020).
3. Pro kiberzlochynnist′: Konventsiya vid 01 lypnya 2006 r. URL: https://zakon.rada.gov.ua/laws/show/994_575 (accessed 02.05.2020).
4. Pro natsional′nu politsiyu: Zakon Ukrayiny vid 02 lypnya 2015 r. № 580-VIII. URL: https://zakon.rada.gov.ua/laws/show/580-19 (accessed 30.04.2020).
5. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny: Zakon Ukrayiny vid 05.10.2017 r. № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/card/2163-19 (accessed 06.05.2020).
6. Naukovo-praktychnyy komentar do Kryminal′noho kodeksu Ukrayiny / vidp. red. S.S. Yatsenko. 4-te vyd., pererob. ta dop. Kyiv: A.S.K., 2005. 848 s. URL: http://ir.nusta.edu.ua/jspui/handle/doc/819 (accessed 06.05.2020).
7. Kiberzlochynnist′ u vsikh yiyi proyavakh: vydy, naslidky ta sposoby borot′by: veb-sayt. URL: https://www.gurt.org.ua/articles/34602/ (accessed 30.04.2020).
8. Burbelo, B.A. Aktual′ni pytannya rozsliduvannya kiberzlochyniv: materialy Mizhnar. nauk.-prakt. konf. Kharkiv: 10 hrud. 2013 r. MVS Ukrayiny, Khark. nats. un-t vnutr. sprav. Kharkiv: KHNUVS, 2013. 272 s. URL: http://dspace.univd.edu.ua/xmlui/bitstream/handle/123456789/553/Aktualni%20pytannia%20rozsliduvannia%20kiberzlochyniv_Materialy%20konferentsii_2013.pdf?sequence=1&isAllowed=y (accessed 04.05.2020).
9. Butuzov V.M., Havlovs′kyy V.D., Skalozub L.P. ta in. Orhanizatsiyno-pravovi ta taktychni osnovy protydiyi zlochynnosti u sferi vysokykh informatsiynykh tekhnolohiy: navchal′nyy posibnyk. Kyiv: Nats. akad. SBU Ukrayiny, 2011. 404 s.
10. Ofitsiynyy sayt Departamentu kiberpolitsiyi Natsional′noyi politsiyi Ukrayiny. URL: https://cyberpolice.gov.ua/results/2018/ (accessed 03.05.2020).