formation and use” with the word “fund”, and thus formulate this budget norm in the following wording: “...1) budget – fund of financial resources for providing tasks and functions, carried out respectively by public authorities, authorities of the Autonomous Republic of Crimea, bodies of local self-government during the budget period...”.

The legislator has fixed inflated indicators of large and especially large sizes, in the presence of which the actions qualify under Article 210 of the Criminal Code of Ukraine, which practically makes it impossible to apply this rule, which necessitates a reduction of the lower level of these sizes to 500 and 1000 times, respectively, exceeding the tax-free minimum income of citizens.

Keywords: *crime article, budget funds, financial resources fund, extrabudgetary funds, state extrabudgetary funds, local extrabudgetary funds, misuse.*

УДК 343.98

DOI: 10.31733/2078-3566-2020-2-134-141

Василь СТРАТОНОВ[©]

доктор юридичних наук, професор,

Заслужений юрист України

(Херсонський державний університет)

«КОМП'ЮТЕРНІ ЗЛОЧИНИ»: ОКРЕМІ ОСОБЛИВОСТІ ТА ХАРАКТЕРИСТИКИ

На превеликий жаль, поряд із позитивними здобутками інформатизація, як і будь-яке соціальне явище, має й негативні прояви, а саме можливість використання комп'ютерів та їх систем для вчинення правопорушень, зокрема злочинів.

Оскільки «комп'ютерні злочини» мають транснаціональний характер, ми повинні об'єднати зусилля для боротьби з цим видом правопорушень. У розвинутих країнах цей вид злочинності завдає величезних збитків, змушує витратити значні кошти на розробку та впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її перекручення чи знищення. Зважаючи на це принципово важливим є вивчення способів учинення злочинів у сфері використання комп'ютерів, комп'ютерних систем і мереж та мереж електронного зв'язку. Ці злочини характеризуються такими особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказування в суді, високим збитком навіть від одиного злочину. Тому на основі аналізу як теоретичних напрацювань, так і результатів практики ми перш за все акцентуємо увагу на окремих способах учинення «комп'ютерних злочинів», розкриваємо їх зміст, форми та способи вчинення в реаліях сьогодення.

Ми характеризуємо найбільш розповсюджені способи та прийоми несанкціонованого отримання інформації як із самого комп'ютера, так і з інформаційних мереж. Знання способів учинення злочинів дозволить надалі ефективніше попереджувати вчинення таких правопорушень, уживати превентивних заходів.

Ключові слова: *способи вчинення, комп'ютерні злочини, автоматизовані системи, технічний захист, криміналістика.*

Постановка проблеми. Аналізуючи ситуацію, яка склалася в період боротьби з COVID-19, зазначимо, що суспільство оцінило можливості дистанційного спілкування та на практиці апробувало сучасні інформаційні технології. Під час карантину світовий інформаційний простір буквально «розривало» від наповнення інформацією. Тож виникає потреба з'ясування й усвідомлення всіх позитивних та негативних явищ інформаційної цивілізації, розуміння наслідків впровадження інформаційних технологій на основі комп'ютерної техніки у всі сфери суспільного життя. Так, як показала практика, ми були недостатньо підготовлені до дистанційної роботи з використанням сучасних можливостей інформаційних технологій, особливо в освітньому процесі, правоохоронній та судовій системах. Але досить швидко всі зрозуміли: порятунок потопаючих – справа рук самих потопаючих, тож кожен, хто був налаштований оптимістично, почав підвищувати рівень своїх

© Стратонов В.М., 2020

ORCID iD : <https://orcid.org/0000-0002-7548-0630>

stratonov@ksu.ks.ua

знань, навчатися, адаптуватися до умов. Свідченням цього є пошук в різних родах курсів із підвищення комп'ютерних знань, отримання сертифікатів і повідомлення про це у фейсбуці. Почали використовувати різних родів «площадки» для виконання тих чи інших функцій, наприклад, читання лекцій для студентів тощо. Не залишилися осторонь і антисуспільні елементи: значно почастишали спроби вчинення шахрайських дій із використанням різноманітних форм спілкування з потенційними «жертвами», що завершувалося застосуванням нових форм зняття коштів із карткових рахунків тощо. Не завжди керівники держустанов спрямовували роботу своїх кадрів на апробовані електронні площадки, наприклад, Zoom. Наслідки швидко проявились, але лише через місяць роботи почали аналізувати проблеми та надавати методичні рекомендації щодо уникнення «вторгнення зі сторони» хакерів та інших осіб [1]. Тож постає необхідність актуалізувати питання щодо способів учинення злочинів в інформаційній та телекомунікаційній сфері (комп'ютерних системах і мережах та мережах електрозв'язку).

Аналіз публікацій, у яких започатковано розв'язання цієї проблеми. Звичайно, проблеми злочинів у комп'ютерній системі не нові. Про це свідчить кримінальне законодавство України. Так, ще в 1999 році в законі була лише одна норма, яка передбачала кримінальну відповідальність за вторгнення в систему електронних обчислювальних машин. Сьогодні це цілий XVI розділ.

Учені працюють над цією проблематикою вже понад двадцять років, але коли одні проблеми було вирішено, виникали інші. Якщо взяти лише останні десять років, то тільки на монографічному рівні підготували та надрукували роботи такі вчені, як В. М. Бутузов [2], М. В. Карчевський [3, 4], М. В. Плугатир [5], Н. А. Савінова [6]. Значний внесок зробили Д. С. Азаров [7], В. О. Голубєв, В. Д. Гавловський, В. С. Цимбалюк [8], В. М. Стратонов [9], а також багато інших авторів збагатили власними доробками напрацювання в боротьбі з кримінальними правопорушеннями проти порядку використання комп'ютерів, комп'ютерних систем і мереж та мереж електрозв'язку.

Метою статті є вивчення способів учинення злочинів у сфері інформаційних технологій.

Виклад основного матеріалу. На превеликий жаль, поряд із позитивними здобутками інформатизація, як і будь-яке соціальне явище, має й негативні прояви: можливість використання комп'ютерних технологій для вчинення правопорушень, зокрема злочинів. Зважаючи на це принципово важливим є вивчення способів учинення правопорушень, які посягають на інформаційні відносини.

Під способом скоєння злочину в криміналістичному змісті звичайно розуміють об'єктивно й суб'єктивно обумовлену систему поведінки суб'єкта до, у момент і після вчинення злочину, що залишає різних родів характерні сліди, які дозволяють за допомогою криміналістичних прийомів і засобів одержати уявлення про суть події, яка відбулася, своєрідності злочинного поведінки правопорушника, його окремих особистісних даних і, власне, визначити найбільш оптимальні методи вирішення завдань розкриття злочину [10, с. 109]. Іншими словами, спосіб скоєння злочину складається з комплексу специфічних дій правопорушника з підготовки, учинення й маскування злочину, що представляють в інформаційному плані своєрідну модель злочину. Спосіб скоєння злочину завжди є результатом сукупної дії значного числа факторів. І чим більше будуть вони виявлятися в діях, тим більше слідів буде залишати злочинець, тим більшою інформацією буде володіти слідчий для висунування слідчих і пошукових версій [8, с. 198-201].

З урахуванням розглянутих проблем найбільшу цінність будуть представляти сліди, які вказують на те, яким чином злочинець здійснив такі дії: потрапив на місце злочину, покинув його, переборював різних родів перешкоди, використовував своє службове становище, виконав намічену злочинну мету, які навички, знання, фізичні зусилля застосував, намагався (чи не намагався) сховати сліди вчиненого діяння. Не менш істотними є сліди, які свідчать про характер зв'язку злочинця з предметом злочинного посягання тощо.

У наш час у вітчизняній і закордонній криміналістичній науці не існує чітко визначених понять у питаннях характеристики способів здійснення комп'ютерних злочинів, їх конкретних назв і класифікації.

Ця проблема настільки нова для науки, що перебуває поки що в стадії осмислення й теоретичних розробок. Особливо це стосується вітчизняної криміналістичної науки, що всерйоз стала займатися цими питаннями лише з початку 90-х років, тоді як закордонні дослідники – із кінця 70-х років [11, 12]. У наших закордонних колег у цьому плані вже існує ряд розробок, які необхідно використовувати під час вивчення й вирішення

аналогічних питань у вітчизняній криміналістичній науці з урахуванням визначених об'єктивних і суб'єктивних виправлень і наближень, що продиктовані реальністю функціонування й розвитку нашого суспільства, його політичними, правовими, соціальними й економічними складовими.

Сьогодні в юридичній літературі існують різні точки зору на питання виділення, класифікації й назви способів учинення комп'ютерних злочинів. Наприклад, Американський національний інститут комп'ютерної безпеки та ФБР провели опитування про найбільш розповсюджені комп'ютерні злочини [13, 14].

Основними способами несанкціонованого одержання інформації, сформульованими за даними закордонних видань, є: застосування пристроїв для підслуховування (закладок); дистанційне фотографування; перехоплення електронних випромінювань; містифікація (маскування під запити системи); перехоплення акустичних випромінювань і відновлення тексту принтера; розкрадання носіїв інформації та виробничих відходів («збір сміття»); зчитування даних із масивів інших користувачів; копіювання носіїв інформації з подоланням засобів захисту; маскування під зареєстрованого користувача; використання програмних пасток; незаконне підключення до апаратури й ліній зв'язку; виведення з ладу механізмів захисту тощо [14, с. 12-13].

У зв'язку з відсутністю аналогічних вітчизняних статистичних даних із розглянутого кола питань можна з визначеним ступенем умовності оперувати даними закордонних досліджень щодо вітчизняної практики. Тим паче, що матеріали конкретних кримінальних проваджень підтверджують правоту закордонних дослідників.

На основі аналізу конкретних проваджень щодо злочинних дій, учинених із використанням засобів комп'ютерної техніки, а також вивчення спеціальної літератури можна виділити понад 20 основних способів учинення комп'ютерних злочинів і близько 40 їх різновидів, число яких постійно збільшується через використання злочинцями різних їхніх комбінацій і логічної модифікації алгоритмів.

Усі способи вчинення комп'ютерних злочинів об'єднують у 5 основних груп. При цьому за основну класифікаційну ознаку виступає метод використання злочинцем тих чи інших дій, спрямованих на одержання доступу до засобів комп'ютерної техніки з різними намірами. Керуючись цією ознакою, Ю. М. Батурін пропонує підхід, відповідно до якого виділяє такі загальні групи: 1) вилучення засобів комп'ютерної техніки (ЗКТ); 2) перехоплення інформації; 3) несанкціонований доступ до ЗКТ; 4) маніпуляція даними й керуючими командами; 5) комплексні методи [15, с. 68].

Розглянемо їх більш докладно. До першої групи належать традиційні способи вчинення звичайних видів («не комп'ютерних») злочинів, у яких дії злочинця спрямовані на вилучення чужого майна. Під чужим майном у цьому випадку розуміють засоби комп'ютерної техніки. Із кримінально-правової точки зору подібні злочини будуть кваліфікуватися відповідними статтями кримінального законодавства, наприклад, шпигунство, розкрадання, розбій, вимагання тощо.

До другої групи належать способи вчинення комп'ютерних злочинів, засновані на діях злочинця, спрямованих на одержання даних і машинної інформації за допомогою використання методів аудіовізуального й електромагнітного перехоплення, які широко практикують в оперативно-розшуковій діяльності правоохоронних органів. Відразу необхідно відзначити, що в цій і наступній групах засоби комп'ютерної техніки будуть виступати і як предмет, і як знаряддя вчинення злочинного діяння. Такими способами є:

1. Безпосереднє (активне) перехоплення. Здійснюється за допомогою безпосереднього підключення до телекомунікаційного устаткування комп'ютера, комп'ютерної системи чи мережі, наприклад, лінії принтера чи по телефонному проводу каналу зв'язку, використовуюваного для передачі даних і керуючих сигналів комп'ютерної техніки, або безпосередньо через відповідний порт персонального комп'ютера. У зв'язку з цим розрізняють: *форсоване перехоплення* — являє собою перехоплення повідомлень, які направляють робочі станції, що мають неполадки в устаткуванні чи каналах зв'язку; *перехоплення символів* — виділення з тексту, який набирає користувач на клавіатурі терміналу, знаків, не передбачених його стандартним кодом; *перехоплення повідомлень* — несанкціоноване підключення спеціального терміналу до лінії зв'язку, прийом і використання повідомлень, які циркулюють між абонентськими пунктами й ЕОМ. Підключення здійснюється за допомогою використання побутових засобів та устаткування: телефона, відрізка проводу, що складає телефонний кабель, комп'ютерного напівпровідного шлейфу, затискачів типу «крокодил», спеціальних шупів-головок від контрольно-

вимірювальної апаратури, набору радіомонтажних інструментів, касетного портативного магнітофона, принтера тощо. Після підключення до каналу зв'язку вся інформація записується на фізичний носій чи переводиться в форму за допомогою побутової чи спеціальної електронної апаратури.

Як спеціальну апаратуру злочинці можуть використовувати: а) комп'ютеризовані аналізатори провідних ліній зв'язку типу РК-1155, що дозволяють водночас прослуховувати до 256 ліній зв'язку; б) багатофункціональний цифровий реєстратор сигналів типу MSR (Multi Signal Registrator) – звичайний персональний комп'ютер, реалізований на базі платформи Intel із використанням плати обробки сигналів на основі процесора ADSP з 16-канальним автоматичним цифровим перетворювачем; він забезпечує тривале безупинне перехоплення мовної, факсимільної та цифрової інформації з 4-8-16-32 каналів провідного й радіозв'язку (на вибір) із подальшою її автоматичною фільтрацією (видаленням шумів тощо), розпізнаванням (ідентифікацією голосу), обробкою й архівуванням.

2. Електромагнітне (пасивне) перехоплення. Не завжди перехоплювальні пристрої вимагають безпосереднього підключення до системи. Дані й інформація можуть бути перехоплені не тільки в каналі зв'язку, але й у приміщеннях, у яких знаходяться засоби комунікації, а також на значному віддаленні від них. Так, без прямого контакту можна зафіксувати й закріпити на фізичний носій електромагнітне випромінювання, яке виникає під час функціонування багатьох засобів комп'ютерної техніки, включаючи й засоби комунікації. Адже робота всіх без винятку електронних пристроїв супроводжується електромагнітним випромінюванням, у результаті чого в різних електронних приймальних пристроях виникають небажані перешкоди. Електронно-променева трубка випромінює в навколишній простір електромагнітні хвилі, які несуть певну інформацію, дані («електронний смог»). Хвилі, випромінювані цим приладом, приблизно так само, як і в разі телевізійного мовлення, проникають крізь різні фізичні перешкоди з деяким коефіцієнтом ослаблення, наприклад, через скло віконних прорізів і стіни будівель, а приймати їх можна, як показують дані численних експериментів, на відстані до 1 000 м. Як тільки ці сигнали прийняті відповідною апаратурою й передані на інший комп'ютер (злочинця), можна одержати зображення, ідентичне зображенню, що виникає на моніторі «передавального» комп'ютера, для чого досить налаштуватися на його індивідуальну частоту. Кожен комп'ютер можна ідентифікувати за конкретними параметрами: робочою частотою, інтенсивністю електромагнітного випромінювання тощо. Наприклад, для здійснення злочинних цілей іноді досить змонтувати приймальну антену за типом хвильового каналу, що має більш гостру, несиметричну діаграму спрямованості. Після чого розробити (чи використовувати готову) програму розшифрування «знятих» даних. Під час учинення комп'ютерного злочину зазначеним способом злочинці використовують прийоми й методи оперативно-розшукової діяльності, а також спеціальну техніку, наприклад, сканувальні пристрої.

3. Аудіоперехоплення чи зняття інформації з віброакустичного каналу. Цей спосіб є найбільш небезпечним і досить розповсюдженим. Захист від витоку по цьому каналу дуже складний. Такий спосіб знімання інформації має два різновиди: заходовий (заносний) і беззаходовий. Перший полягає в установленні інфінітивного телефону (підслуховувального пристрою – «таблетки», «клопа», «жучка» тощо) до апаратури засобів обробки інформації, у різні технічні пристрої, на провідні комунікаційні лінії (радіо, телефон, телевізійний кабель, охоронно-пожежну сигналізацію, електромережу тощо), а також у різні конструкції інженерно-технічних споруд і побутових предметів, які знаходяться на об'єкті, з метою перехоплення розмов працюючого персоналу та звукових сигналів технічних пристроїв (визначення номера викликуваного абонента АТС тощо). Установка «клопа» чи іншої розвідувальної апаратури на об'єкт можлива трьома способами. У першому необхідне таємне чи відкрите проникнення в приміщення; у другому випадку радіопередавальну й звукозаписну апаратуру встановлюють під час будівлі чи ремонту приміщення; у третьому апаратуру здобуває чи заносить сама потерпіла сторона (монтується в предмети, які здобувають). Як приклади спеціальної техніки можна навести: спеціальні мікрофони з можливим дистанційним управлінням; диктофони з тривалим записом; цифрові адаптивні фільтри типу АФ-512, DAC-256 і DAC-1024, що дозволяють проводити обробку «засмічених» мовних сигналів. Знайти апаратуру знімання інформації вкрай важко, тому що її зазвичай дуже добре маскує злочинець (під мікросхему, запальничку тощо) [16, с. 287-288].

Другий (беззаходовий) різновид – найбільш небезпечний. Полягає він у такому.

Акустичні й вібраційні датчики знімання інформації встановлюють на інженерно-технічні конструкції, які знаходяться за межами охоронюваного приміщення, з якого необхідно приймати мовні сигнали. Виділяють такі типові конструкції інженерно-технічних споруд: несучі стіни будинків, перегородки, перекриття, вікна, віконні рами, двері та дверні коробки, вентиляційні повітроводи, трубопроводи. При цьому обов'язково проникати в приміщення – досить наблизитися до нього зовні. Датчик встановлюють або безпосередньо, або дистанційно. В останньому використовують різні пристрої, які вистрілюють, призначені для дистанційного зняття мовної інформації через відчинені вікна, двері тощо.

4. Відеоперехоплення. Цей спосіб учинення злочину полягає в діях злочинця, спрямованих на одержання інформації шляхом використання різної відеооптичної техніки. Він має 2 різновиди: *фізичний* та *електронний*. У першому випадку перехоплення інформації здійснюється за допомогою застосування злочинцем різної побутової відеооптичної апаратури, наприклад, підзорної труби, бінокля, мисливського приладу нічного бачення, оптичного прицілу тощо. Злочинець проводить спостереження за об'єктом (жертвою) з деякої відстані з метою одержання необхідної інформації, яка в окремих випадках фіксується на фізичний носій. За таких умов знаряддя злочину знаходиться безпосередньо в руках злочинця. У другому випадку процес одержання інформації злочинцем здійснюється з використанням спеціальної техніки: передавальний пристрій знаходиться безпосередньо на об'єкті спостереження, а приймальний – у руках злочинця. Може використовуватися така спецтехніка: спеціальні відеомагнітофони з тривалим записом, устаткування для прихованої відеозйомки тощо.

5. «Збирання сміття». Цей спосіб учинення злочину полягає в неправомірному використанні злочинцем технічних відходів інформаційного процесу, залишених користувачем після роботи з комп'ютерною технікою. Він здійснюється у двох формах: *фізичний* та *електронний*. У першому випадку пошук відходів зводиться до уважного огляду вмісту смітневих кошиків, баків для технологічних відходів і збору залишених чи викинутих фізичних носіїв інформації. Електронний варіант вимагає перегляду, а іноді й подальшого дослідження даних, які знаходяться в пам'яті комп'ютера.

У деяких випадках злочинець може здійснюватися дії, спрямовані на відновлення й подальший аналіз даних, які містяться в стертих файлах. Досягнення цих цілей припускає обов'язкове використання як знаряддя злочину різних програмних засобів спеціального призначення, що є інструментальними програмними засобами. Один із них – програмний комплекс PC Tools Deluxe, який містить універсальну програму pcr.exe, що дозволяє відновлювати раніше стерті програми та файли.

До третьої групи способів учинення комп'ютерних злочинів належать дії злочинця, спрямовані на одержання несанкціонованого доступу до засобів комп'ютерної техніки [10, с. 135-156]. Це такі способи:

а) «за дурнем» – типовий прийом фізичного проникнення, добре відомий спеціалістам, які займаються питаннями вдосконалення оперативної-розшукової діяльності. Він полягає в такому: тримаючи в руках предмети, пов'язані з роботою на комп'ютерній техніці (елементи маскування), потрібно очікувати будь-кого, хто має санкціонований доступ, біля замкнених дверей, за якими знаходиться предмет посягання. Коли з'являється законний користувач, залишається лише ввійти всередину разом із ним чи попросити його допомогти донести нібито необхідні для роботи на комп'ютері предмети. Цей спосіб розрахований на низьку пильність співробітників організації й осіб, які її охороняють. При цьому злочинець може використати прийом проникнення з «легендою»;

б) «за хвіст» – це спосіб знімання інформації, що полягає в такому: злочинець підключається до лінії зв'язку законного користувача (з використанням засобів комп'ютерного зв'язку) й терпляче чекає сигналу, який позначає кінець роботи, переходяє його «на себе», а потім, коли законний користувач закінчує активний режим, здійснює доступ до системи;

в) «комп'ютерний аборт» – це спосіб учинення комп'ютерного злочину шляхом випадкового підбору (чи заздалегідь добутого) абонентного номера комп'ютерної системи потерпілої сторони з використанням, наприклад, звичайного телефонного апарата. Іноді для цих цілей злочинець використовує спеціально створену саморобну або заводську (в основному закордонного виробництва) програму автоматичного пошуку пароля. Алгоритм її роботи полягає в тому, щоб, використовуючи швидкодію сучасних комп'ютерних пристроїв, перебирати всі можливі варіанти комбінацій букв, цифр і спе-

ціальних символів, наявних на стандартній клавіатурі персонального комп'ютера, і у випадку збігу комбінації символів з оригіналом робити автоматичне з'єднання зазначених абонентів. Варто звернути увагу, що існує безліч програм-«зламувачів», які називають професійною мовою HACK TOOLS (інструмент зламу). Але ці програми стають малоефективними в комп'ютерних системах, які володіють програмою-«сторожем» комп'ютерних портів. Тому останнім часом злочинці стали активно використовувати метод «інтелектуального перебирання», заснований на підборі передбачуваного пароля, виходячи із заздалегідь визначених тематичних груп його належності. Тому і в роботі із Zoom рекомендують встановлювати кодові слова (паролі), поновлювати версії телефонного або комп'ютерного додатка тощо.

Висновки. «Комп'ютерна злочинність», особливо її транснаціональна складова, стала однією з міжнародних проблем, що зумовлено широким упровадженням глобальних інформаційних мереж, насамперед мережі Internet, яка вже поєднує більшість країн земної кулі і використання якої поширюється далі. У розвинутих країнах цей вид злочинності завдає величезних збитків, змушує витратити значні кошти на розробку та впровадження програмних, технічних та інших засобів захисту від несанкціонованого доступу до інформації, її перекручення чи знищення. Ці злочини характеризуються такими особливостями: високою латентністю, складністю їх виявлення та розслідування, складністю доказування в суді, високим збитком навіть від одиначного злочину.

Висока латентність таких злочинів пояснюється насамперед тим, що державні й комерційні структури, які зазнали нападу, особливо в банківській діяльності, не дуже довіряють можливості розкриття цих злочинів правоохоронними органами. На наш погляд, однією з основних причин високої латентності та низького рівня розкриття злочинів у сфері комп'ютерної інформації є проблеми, які виникають перед правоохоронними органами на стадії досудового провадження внаслідок складності кваліфікації злочинних діянь та особливостей проведення окремих слідчих дій. Тому на основі аналізу як теоретичних напрацювань, так і практики ми перш за все акцентуємо увагу на окремих способах учинення «комп'ютерних злочинів», розкриваємо зміст, форми та способи їх учинення в реаліях сьогодення.

Розглядаючи проблеми, які виникають у процесі розслідування цих злочинів, необхідно мати на увазі, що існує багато особливостей, які потрібно враховувати під час проведення таких дій, як огляд місця події, обшук та вилучення речових доказів, допит потерпілих і свідків, призначення експертизи. Для того щоб фактичні дані були визнані доказами, вони повинні бути отримані з джерел із дотриманням правил, які встановлені кримінальним процесуальним кодексом.

Ще однією проблемою є відсутність спеціалістів-практиків у галузі попередження й боротьби з такими видами злочинів. Як уже було зазначено, суб'єктами злочинів виступають спеціалісти дуже високого рівня, злочинці-інтелектуали. Правоохоронні органи, на жаль, ще не можуть ефективно їм протидіяти. Тому розслідування «комп'ютерних злочинів» необхідно в обов'язковому порядку проводити із залученням спеціаліста в галузі інформаційних технологій. Необхідність цього підтверджується й досвідом роботи правоохоронних органів інших країн.

Список використаних джерел

1. Как безопасно пользоваться Zoom, что бы избежать попадания в ловушку. URL: <https://ukrnews.com/news/699115-kak-pravilno-polzovatsya-prilozheniem-zoom-eksperty>.
2. Бутузов В. М. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз): монографія. Київ: КНТ, 2010. 408 с.
3. Карчевський М. В. Злочини у сфері використання комп'ютерної техніки: навч. посіб. Київ: Атіка, 2010. 168 с.
4. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України: монографія. Луганськ: РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. 528 с.
5. Плугатир М. В. Імплементація Україною міжнародно-правових зобов'язань щодо відповідальності за злочини у сфері комп'ютерної інформації: автореф. дис. ... канд. юрид. наук. Київ, 2010. 18 с.
6. Савінова Н. А. Кримінально-правове забезпечення розвитку інформаційного суспільства в Україні: теоретичні та практичні аспекти: монографія. Київ: ДКС, 2012. 342 с.
7. Азаров Д. С. Злочини у сфері комп'ютерної інформації (кримінально-правове дослідження). Київ: Атіка, 2007. 304 с.
8. Голубев В. О., Гавловський В. Д., Цимбалюк В. С. Проблеми боротьби зі злочинами у сфері використання комп'ютерних технологій: навч. посіб. / за заг. ред. Р. А. Каложного. Запоріжжя: ЗІДМУ, 2002. 292 с.
9. Стратонов В. М. Криміналістична теорія пізнавальної діяльності: монографія. Херсон:

Вид-во Херсон. держ. ун-ту, 2009. 440 с.

10. Голубев В. О., Юрченко О. М. Злочини в сфері комп'ютерної інформації: способи скоєння та засоби здійснення / під. ред. О. П. Снігер'єва. Запоріжжя, 1998. 157 с.

11. Компьютерные преступления и методы борьбы с ними. *Проблемы преступности в капиталистических странах*. Москва: ВИНТИ, 1985. № 1. С. 3-7.

12. Компьютерные преступления и обеспечение безопасности ЭВМ. *Проблемы преступности в капиталистических странах*. Москва: ВИНТИ, 1983. № 6. С. 3-6.

13. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Cybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, D.C., 28 March 2000.

14. Computer Crime: A Crime fighter's Handbook. D. Icove, K. Seger, W. Von Sorsh. O'Reilly & Associates, Inc., 1995. 437 p.

15. Батурин Ю. М. Проблемы компьютерного права. Москва: Юрид. лит., 1991. 57 с.

16. Лучин И. Н., Желдаков А. А., Кузнецов Н. А. Взламывание парольной защиты методом интеллектуального перебора. *Информатизация правоохранительных систем*. Москва: Академия МВД России, 1996. С. 287-288.

Надійшла до редакції 30.04.2020

References

1. Kak bezopasno pol'zovat'sya prilozheniyem Zoom, chtoby izbezhat' popadaniya v lovushku [How to safely use the Zoom application to avoid falling into the trap]. URL: <https://ukrnews.com/news/699115-kak-pravilno-polzovatsya-prilozheniem-zoom-eksperty>. [in Russ.]

2. Butuzov, V. M. (2010) Protydiya komp'yuterniy zlochynnosti v Ukrayini (systemno-strukturnyy analiz) [Counteraction to computer crime in Ukraine (system-structural analysis)]: monohrafiya. Kyiv: KNT, 408 s. [in Ukr.]

3. Karches'kyi, M. V. (2010) Zlochyny u sferi vykorystannya komp'yuternoyi tekhniki [Crimes in the field of computer technology]: navch. posib. Kyiv: Atika, 168 s. [in Ukr.]

4. Karches'kyi, M. V. (2012) Kryminal'no-pravova okhrona informatsiynoi bezpeky Ukrainy [Criminal and legal protection of information security of Ukraine]: monohrafiya. Luhansk: RVV LDUVS im. E. O. Didorenka, 528 s. [in Ukr.]

5. Pluhaty, M. V. (2010) Implementatsiya Ukrainoyu mizhnarodno-pravovykh zobov'yazan' shchodo vid-povidal'nosti za zlochyny u sferi komp'yuternoyi informatsiyi [Implementation by Ukraine of international legal obligations regarding responsibility for crimes in the field of computer information]: avtoref. dys. ... kand. yuryd. nauk. Kyiv, 18 s. [in Ukr.]

6. Savinova, N. A. (2012) Kryminal'no-pravove zabezpechennya rozvytku informatsiynoho suspil'stva v Ukrayini: teoretychni ta praktychni aspekty [Criminal-legal support of information society development in Ukraine: theoretical and practical aspects]: monohrafiya. Kyiv: DKS, 342 s. [in Ukr.]

7. Azarov, D. S. (2007) Zlochyny u sferi komp'yuternoyi informatsiyi (kryminal'no-pravove dosli-dzhennya) [Crimes in the field of computer information (criminal legal research)]. Kyiv: Atika, 304 s. [in Ukr.]

8. Holubyev, V. O., Havlovs'kyi, V. D., Tsymbalyuk, V. S. (2002) Problemy borot'by zi zlochynamy u sferi vykorystannya komp'yuternykh tekhnolohiy [Problems of combating crime in the use of computer technology]: navch. posib. / za zah. red. R. A. Kalyuzhnoho. Zaporizhzhya: ZIDMU, 292 s. [in Ukr.]

9. Stratonov, V. M. (2009) Kryminalistychna teoriya piznaval'noyi diyal'nosti [Forensic theory of cognitive activity]: monohrafiya. Kherson: Vyd-vo Kherson. derzh. un-tu, 440 s. [in Ukr.]

10. Holubyev, V. O., Yurchenko, O. M. (1998) Zlochyny v sferi komp'yuternoyi informatsiyi: sposoby skoyennya ta zasoby zdiysnennya [Crimes in the field of computer information: methods of commission and means of implementation] / pid. red. O. P. Sniher'ova. Zaporizhzhya, 157 s. [in Ukr.]

11. Komp'yuternyye prestupleniya i metody bor'bi s nimi [Computer crimes and methods of combating them]. *Problemy prestupnosti v kapitalisticheskikh stranakh*. Moskva: VINITI, 1985. № 1. С. 3-7. [in Russ.]

12. Komp'yuternyye prestupleniya i obespecheniye bezopasnosti ÉVM [Computer crimes and computer security]. *Problemy prestupnosti v kapitalisticheskikh stranakh*. Moskva: VINITI, 1983. № 6. С. 3-6. [in Russ.]

13. Statement for the Record of Louis J. Freeh, Director Federal Bureau of Investigation on Sybercrime Before the Senate Committee on Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, D.C., 28 March 2000.

14. Computer Crime: A Crime fighter's Handbook. D. Icove, K. Seger, W. Von Sorsh. O'Reilly & Associates, Inc., 1995. 437 p.

15. Baturin, Yu. M. (1991) Problemy komp'yuternogo prava [Problems of computer law]. Moskva: Yurid. lit., 57 s. [in Russ.]

16. Luchin, I. N., Zheldakov, A. A., Kuznetsov, N. A. (1996) Vzlamyvaniye parol'noy zashchity metodom intellektual'nogo perebora [Hacking password protection by the method of intellectual search]. *Informatzatsiya pravookhranytel'nykh sistem*. Moskva: Akademiya MVD Rossii, S. 287-288. [in Russ.]

SUMMARY

Vasyl M. Stratonov. "Computer crimes": some features and characteristics. Unfortunately, along with positive achievements, informatization also has negative manifestations, namely, the possibility of using computer technology to commit crimes. The world has long been talking about "cybercrime" about "computer crime," and chapter 16 of the Criminal Code of Ukraine deals with crimes in the use of comput-

ers, computer systems and networks, as well as telecommunications. Therefore, we can state that a unified approach to the definition of a concept does not exist. However, the introduction of certain norms into the law does not solve the problems. Problems arise with the direct implementation of these standards in everyday life. Since "computer crimes" are transnational in nature, we must join forces to combat such crimes. In developed countries, this type of crime leads to huge losses, significant funds that are spent on the development and implementation of software, technical and other means of protection against unauthorized access to information, its distortion or destruction. With this in mind, it is fundamentally important to study methods of committing crimes using computers, computer systems and telecommunication networks. Therefore, we characterize some of the most common ways of committing computer crimes.

Such crimes are characterized by the following features: the complexity of their detection and investigation, the difficulty of proving in court, the high damage even from one crime. Therefore, based on the analysis of both theory and the results of practice, we primarily focus on individual methods of committing "computer crimes". We reveal in the article the content, forms and methods of committing computer crimes in the realities of today.

We focus on the main methods of unauthorized receipt of information, namely: the use of a device that listens (bookmarks); deleted photo; interception of electronic radiation; hoax (disguise for system requests); interception of acoustic radiation and restoration of printer text; theft of media and industrial waste (garbage collection); reading data from arrays of other users; copying storage media with overcoming protection measures; masking a registered user; use of software traps; illegal connection to equipment and communication lines; failure of defense mechanisms.

We characterize the most common both methods and methods of unauthorized receipt of information from computer and information networks. Knowing the ways of committing crimes will help to further prevent the commission of crimes, take preventive measures.

Keywords: *commission methods, computer crimes, automated systems, technical protection, forensics.*

УДК 343.35

DOI: 10.31733/2078-3566-2020-2-141-146

Володимир ШАБЛИСТИЙ[®]
доктор юридичних наук, доцент
(Дніпропетровський державний
університет внутрішніх справ)

ПРО ВИКРИВАЧІВ КОРУПЦІЇ ТА КРИМІНАЛЬНЕ ПРАВО

Розглянуто зміни та доповнення до Кримінального кодексу України та інших законів щодо викривачів корупції, особливо їх права на винагороду за повідомлення про корупційний злочин. Визначено проблему існування інших порушень Закону України «Про запобігання корупції», за які не встановлено кримінальної, адміністративної, дисциплінарної та/або цивільно-правової відповідальності та про які може повідомляти викривач.

Стверджується, що за повідомлення про декларування недостовірної інформації викривач на винагороду може не розраховувати у будь-якому разі. Незаконне збагачення не може бути і ніколи не буде корупційним злочином, воно є наслідком вчинення справді корупційних злочинів, а тому викривач на винагороду знову може не розраховувати.

Для усунення вказаних протиріч запропоновано у примітці 2 до ст. 45 КК України визначити перелік злочинів, пов'язаних із корупцією, а особу викривача зробити відповідальною хоча б у частині вибачення за оприлюднення інформації, що судом не підтверджена. Для реалізації таких пропозицій до дискусії варто запросити не тільки вчених-криміналістів, а й фахівців у галузі адміністративної відповідальності, трудового та цивільного права і процесу.

Ключові слова: *корупція, корупційне правопорушення, правопорушення пов'язане із корупцією, корупційний злочин, викривач, юридичне невігластво.*

Постановка проблеми. 17 жовтня 2019 року Верховна Рада України прийняла Закон України «Про внесення змін до Закону України «Про запобігання корупції» щодо викривачів корупції» [1], який набув чинності 01 січня 2020 року. Зважаючи на великий