УДК 343.98

ХАРАКТЕРИСТИКА ТЕХНОЛОГІЙ ВЧИНЕННЯ ЗЛОЧИНІВ У КІБЕРПРОСТОРІ

Самойленко О.А., к. ю. н.,
доцент кафедри криміналістики
Національний університет «Одеська юридична академія»

Стаття присвячена характеристиці технологій вчинення злочинів у кіберпросторі. Виділено сім груп таких технологій. У розгляді кожної технології автором робиться акцент на закономірностях її застосування. Наводяться показові приклади технологій із матеріалів судово-слідчої практики.

Ключові слова: *алгоритм, злочинна діяльність, злочин, кіберпростір, несанкціоноване втручання, персональні дані, технологія.*

Статья посвящена характеристике технологий совершения преступлений в киберпространстве. Выделены семь групп таких технологий. При рассмотрении каждой технологии автором делается акцент на закономерностях ее применения. Приводятся показательные примеры технологий из материалов судебно-следственной практики.

Ключевые слова: *алгоритм, преступная деятельность, преступление, киберпространство, несанкционированное вмешательство, персональные данные, технология.*

Samoilenko O.A. CHARACTERISTICS OF TECHNOLOGIES OF PERFECTION OF CRIMES IN CYBER SPACE

The article is devoted to the characterization of technologies of committing crimes in cyberspace. Seven groups of such technologies are identified, in particular:

1) technology of illegal enrichment, based on the previous acquisition of personal data / commercial secret of an individual / legal entity by unauthorized interference with the operation of computer equipment;

2) the technology of taking non-cash funds through the use of electronic payment systems based on the previous unauthorized interference with the operation of computer equipment;

3) "espionage" technologies based on previous access to state / commercial secrets by unauthorized interference with the operation of computer equipment;

4) technology of official theft through the use of electronic payment systems, based on unauthorized actions with information, perpetrated by a person who has the right of access to it;

5) technology to conceal the illicit origin of non-cash funds, based on the previous unauthorized interference with the operation of computer equipment;

6) technology of illegal enrichment, based on the previous unauthorized interference with the operation of a computer, computer system, network in order to neutralize intellectual protection means;

7) technology of illegal enrichment by illegal actions with payment cards. When considering each technology, the author focuses on the patterns of its application.

Illustrative examples of technology based on forensic practice are given.

Key words: *algorithm, criminal activity, crime, cyberspace, unauthorized interference, personal data, technology.*

Технології вчинення злочинів у кіберпросторі є малодослідженими в криміналістичній науці. Водночас необхідно визнати, що більшість криміналістів здійснювали дослідження технологій через способи вчинення суто комп'ютерних злочинів шляхом їх різноманітних класифікацій, як-от: за видом комп'ютерного злочину (В.В. Крилов, О.П. Снегірьов, В.О. Голубєв) [1–3], типом комп'ютерного захисту (Д. Айков, К. Сейгер, У. Фонсторх) [4], методом виконання злочинцем

тих чи інших дій, спрямованих на отримання доступу до засобів комп'ютерної техніки (П.Д. Біленчук, М.А. Зубань) [5–7]. Адже поєднання таких способів здійснюється в процесі реалізації злочинцем або їх групою певної технології вчинення злочинів із використанням обстановки кіберпростору.

Як свідчить судово-слідча практика, технологія дійсно передбачає наявність відповідного алгоритму дій. Алгоритм традиційно становить певну послідовність дій, виконання яких дає можливість досягти запланованого (бажаного суб'єктом) результату. Тому пізнання сутності технології вчинення злочинів у кіберпросторі має відбуватися на системному рівні, з позицій процесу досягнення злочинного результату. Метою цієї статті є характеристика технологій вчинення злочинів у кіберпросторі.

Терміном «технологія» позначають типову, алгоритмічну систему методів і прийомів, що забезпечує вирішення однотипних завдань із метою підвищення ефективності відповідних процесів і рентабельності кінцевої продукції [8, с. 24]. Така «однотипність завдань» під час учинення в обстановці кіберпростору злочинів різної кримінально-правової класифікації набуває форм додаткового й основного мотивів аналізованої злочинної діяльності. Оскільки саме мотив покладається в основу криміналістичної класифікації злочинів досліджуваної категорії, про характерні технології вчинення злочинів у кіберпросторі можна висновувати у разі вчинення сукупності злочинів у межах однієї або декількох класифікаційних підгруп злочинів. Як свідчить аналіз матеріалів слідчо-судової практики, типовість технологій учинення злочинів із використанням обстановки кіберпростору найяскравіше виявляється стосовно злочинів, учинених у кіберпросторі з корисливих і соціально-економічних мотивів.

На підставі аналізу матеріалів слідчо-судової практики можна визначити типові для України технології вчинення злочинів у кіберпросторі, розподіливши їх за такими групами:

1. Технології незаконного збагачення, засновані на попередньому заволодінні персональними даними / комерційною таємницею фізичної / юридичної особи шляхом несанкціонованого втручання в роботу комп'ютерної техніки. Такі технології найчастіше застосовують злочинець – досвідчений користувач та / або злочинець – користувач-професіонал. Останній часто діє в складі організованої групи з розподілом ролей, де є організатором. Така злочинна діяльність утворюється сукупністю способів вчинення злочинів із двох умовних груп: 1) злочини, передбачені ст. 189 (вимагання) та / або ст. 190 (шахрайство); 2) злочини, передбачені окремими статтями розділу XVI КК України, зокрема ст. 361 (несанкціоноване втручання в роботу ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку) та / або ст. 361-1 (створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут). Можна визначити загальні закономірності застосування цієї технології: 1) початкові дії злочинця, спрямовані на отримання доступу до комп'ютера жертви шляхом здійснення незаконного впливу на засоби комп'ютерної техніки та інформацію; 2) залежно від змісту отриманих персональних даних жертви злочинець може корегувати свої подальші дії з незаконного збагачення, вчиняючи вимагання або шахрайство; 3) в основу функціонування технологій покладено застосування сукупності кібертехнологій, часто технологій функціонування соціально орієнтованих мереж, технологій електронної комерції, сервісів електронної дошки оголошень, шкідливого програмного забезпечення.

Розглянемо показовий приклад учинення вимагання [9]. Мешканець Львівської області, маючи необхідні навички у сфері програмування, створив Інтернет-сайт «xakercki-poslygu[.]hol.es», на якому пропонував свої послуги щодо зламу облікових записів, електронних скриньок. Листування між ним і клієнтами відбувалося за допомогою закритої спільноти, яку він адміністрував у соціальній мережі. Під час спілкування з клієнтами він також надавав їм посилан-

ня на нібито форму зворотного зв'язку, звертаючись до якої, користувачі потрапляли на фішинговий сайт (фіктивний, спеціально створений злочинцем з метою отримання від жертви інформації, зокрема логінів і паролів). Отримавши таким чином доступ до облікових записів жертв, злочинець блокував доступ законних користувачів до акаунтів шляхом змінення паролю. За повернення доступу він висував вимоги майнового характеру. Суми, які він вимагав, коливалися залежно від платоспроможності жертви. Також слідством було встановлено, що під виглядом додатку для злому соціальних мереж зловмисник розмістив для вільного завантаження шкідливе програмне забезпечення, призначене для несанкціонованого втручання в роботу мобільних телефонів з операційною системою «Android», внаслідок чого хакер мав змогу переглядати телефонну книжку, фотографії та записи вхідних і вихідних викликів жертви. Цю інформацію надалі могло бути використано для вчинення вимагання або шахрайства.

2. Технології заволодіння безготівковими коштами шляхом застосування електронних платіжних систем, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки. Застосовують такі технології зазвичай злочинець – досвідчений користувач та / або злочинець – користувач-професіонал. Така злочинна діяльність утворюється сукупністю способів вчинення злочинів, передбачених ст. 185 (крадіжка) або ст. 190 (шахрайство) та статей розділу XVI КК України, залежно від суті дії для отримання доступу до інформації (ст. 361 (несанкціоноване втручання) та ст. 361-1 (дії щодо шкідливих програмних чи технічних засобів) або ст. 363-1 (шкідливий спам)). Характерною особливістю цієї групи технологій є їх застосування організованою злочинною групою.

Кожен учасник злочинної діяльності за відсутності транснаціонального компонента в такій групі виконує покладену на нього функцію, зокрема зі: 1) створення фіктивного підприємства для маскування злочинної діяльності; 2) здійснення несанкціонованого втручання в роботу комп'ютерної техніки та дій, спрямованих на забезпечення незаконної трансакції; 3) реалізації механізмів легалізації отриманих безготівкових коштів і переведення їх у готівкову форму. Показовою є діяльність групи осіб у м. Луцьку [10]. Так, 29 листопада 2012 р. група осіб, серед яких – не встановлені слідством особи, діючи за попередньою змовою з метою заволодіння чужим майном, маючи спеціальні знання, вміючи користуватися спеціалізованим програмним забезпеченням, призначеним для проникнення в комп'ютер через Інтернет, проникли до системи електронних платежів «Приват24», сформували електронне платіжне доручення від 29 листопада 2012 р. за № 1047, у якому зазначили, що Луцьке підприємство електротранспорту здійснює електронний платіж безготівкових коштів у сумі 138 440 грн на рахунок ТОВ «Спектрум Україна». Засвідчивши платіжне доручення електронним підписом для проведення платежу, зловмисники передали його через систему електронних платежів «Приват24» до ВГРУ ПАТ КБ «Приват Банк», яке здійснило перерахування безготівкових коштів у сумі 138 440 грн із рахунку Луцького підприємства електротранспорту на рахунок заздалегідь створеного фіктивного ТОВ «Спектрум Україна». Ці гроші під виглядом законного переказу було переведено на картковий рахунок ТОВ «Спектрум Україна» в ПАТ «Укрсиббанк». З використанням корпоративної картки безготівкові кошти через банкомати було конвертовано в готівку й розділено між співучасниками. Дії організатора цієї злочинної схеми було кваліфіковано за ч. 1 ст. 205; ч. 2 ст. 361; ч. 3 ст. 190; ч. 2 ст. 200; ч. 2 ст. 209. У перебігу досудового слідства також було встановлено вчинення цією особою іншого злочину з використанням обстановки кіберпростору, зокрема передбаченого ч. 2 і 3 ст. 301 КК України.

Коли йдеться про діяльність транснаціональної мережевої злочинної групи, організатор злочину та сума загального збитку найчастіше залишаються невстановленими. Тому за матеріалами слідчо-судової практики такі злочини кваліфікують лише за сукупністю стат-

тей розділу XVI КК України. Наприклад, у травні 2016 р. група осіб вступила у злочинну змову з метою проведення несанкціонованих платіжних операцій із рахунків українських і зарубіжних користувачів через систему миттєвих Інтернет-розрахунків «WebMoney Transfer» [11]. Гр. А., маючи спеціальні технічні знання у сфері програмування, в Херсонській області за допомогою невстановленого комп'ютера створив з метою використання та розповсюдження програмне забезпечення за назвою «grafon.apk» і файл «restricted» для мобільних комп'ютерів на базі операційної системи «Android», після чого передав логін і пароль доступу до панелі управління бот-мережею «SexDrugWokrug.apk» зазначеного програмного забезпечення гр. Б. У травні 2016 р. за декількома електронними адресами, де знаходилися панелі управління зазначеної бот-мережі, гр. Б. використав і розповсюдив у мережі Інтернет через низку власних сайтів вищезгаданий програмний засіб. Останній, за висновками комп'ютерно-технічної експертизи, є шкідливим програмним забезпеченням («троян»), що встановлюється як звичайна програма та надалі отримує права суперкористувача, працює таємно у фоновому режимі, перехоплює платіжні операції, а також збирає особисті дані користувача. Управління ним здійснюється з віддалених Інтернет-серверів, а саме розміщується на веб-сайтах вільного доступу. Останні мають ідентичний зміст про нібито додаток до АС «Android» за назвою «SexDrugWokrug.apk», який за описом призначений для пошуку друзів і спілкування, але насправді є шкідливим програмним засобом. Після завантаження на мобільний термінал потерпілого шкідливого програмного засобу «SexDrugWokrug.apk» цю програму встановлюють під виглядом системного процесу як SystemUpdate, а після першого запуску вона вимагає надання додаткових повноважень для доступу до системи. Отримавши повноваження, програма видаляє свою «іконку-ярлик» і переходить у фоновий режим, намагаючись з'єднатися з сервером та передати інформацію з електронного приладу жертви. Отримавши дані, програма перевіряє наявність встановленого мобільного банкінгу на телефоні жертви, надсилаючи смс-запити на запрограмовані спеціальні номери, та в разі позитивного результату намагається заволодіти грошовими коштами потерпілого шляхом здійснення несанкціонованих платежів через систему миттєвих Інтернет-розрахунків «WebMoney Transfer».

3. Технології «шпигунства», засновані на попередньому отриманні доступу до державної / комерційної таємниці шляхом несанкціонованого втручання в роботу комп'ютерної техніки. В Україні такі технології типово застосовують злочинець – упевнений користувач і злочинець – досвідчений користувач, які діють одноосібно з власних мотивів або на замовлення. Діяльність злочинця кваліфікується за сукупністю статей, що передбачають відповідальність за вчинення злочинів із двох умовних груп:

1) злочини, пов'язані зі збиранням або передаванням відповідного виду інформації з обмеженим доступом (ст. 231 (незаконне збирання з метою використання відомостей, що становлять комерційну чи банківську таємницю) та / або ст. 232 (розголошення комерційної або банківської таємниці); ст. 111 (державна зрада) та / або ст. 114 (шпигунство));

2) злочини у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку, про які йдеться в розділі XVI КК України (ст. 361 (несанкціоноване втручання особи, що не має права доступу до інформації) та / або ст. 362 (несанкціоновані дії з інформацією особи, що має право доступу). Технології зберігання й обробки інформації, шкідливого програмного забезпечення, електронної розсилки та вікі(viki)-технології є найчастіше використовуваними злочинцем.

Видається доречним такий приклад [12]. 12 червня 2013 р. о 01 год 34 хв гр. М., діючи умисно, віддалено з метою незаконного втручання в роботу комп'ютера шляхом подолання системного захисту, встановленого на сервері ТОВ «Укрнет2», видаючи себе за користувача системи, без згоди останнього

змінив пароль доступу до електронної поштової скриньки та, в такий незаконний спосіб створивши умови для вчинення подальших протиправних дій, отримав можливість змінювати на свою користь режим роботи поштового сервера, ознайомлюватися з відомостями, що становлять комерційну таємницю фізичної особи-підприємця О. Після цього з метою комерційного шпигунства шахрай змінив режим роботи вузлового комп'ютера ТОВ «Укрнет». Для цього в обліковому записі без дозволу О. активував додаткову функцію «Пересилання» та в налаштуваннях зазначив параметри, за яких усі вхідні листи, отримані на електронну адресу О., автоматично пересилалися до спеціально створеної ним поштової скриньки. Як результат, зловмисник отримав можливість ознайомлюватися з листуванням потерпілого. Таким шляхом М. скопіював клієнтську базу О., яку використовував у своїй комерційній діяльності, та отримав можливість повністю видаляти проекти робіт і замовлення, адресовані потерпілому. У цивільному позові матеріальну шкоду, завдану О., було оцінено в розмірі 200 000 грн. Гр. М. було притягнуто до кримінальної відповідальності за вчинення сукупності злочинів, передбачених ст. 231 та ч. 2 ст. 361 КК України.

Варто додати, що в разі вчинення такої злочинної діяльності «на замовлення» замовник часто залишається невстановленим, через що в суді вину підтверджують лише за статтями розділу XVI КК України. Показовою в цьому сенсі є діяльність старшого оперуповноваженого з особливо важливих справ інформаційно-моніторингового відділу Головного управління внутрішньої безпеки Міністерства доходів і зборів України А., який неодноразово здійснював несанкціонований збут інформації з обмеженим доступом іншій особі за щомісячну грошову винагороду. Його діяльність було кваліфіковано за ст. 361-2, 362 КК України [13].

4. Технології службових розкрадань шляхом застосування електронних платіжних систем, засновані на несанкціонованих діях з інформацією, учинені особою, котра має право доступу до неї. В Україні такі технології типово застосовує злочинець – упевнений користувач, що діє одноосібно з власних мотивів або в групі осіб із чітким розподілом ролей. Діяльність злочинця кваліфікується за сукупністю ст. 191 КК України зі статтями розділу XVI КК України (найчастіше ст. 361-2, 362, 363; іноді ст. 361, 361-1, 363-1 стосовно дій, що характеризують способи приховування злочину). Злочинні технології базуються на використанні банківських технологій, електронної комерції, електронних платіжних систем. Особливо складним для слідчого є встановлення корисливої мети діяльності злочинця. Так, мешканка м. Києва, перебуваючи на посаді адміністратора торговельного залу супермаркету «Варус», мала право доступу та безпосередній доступ до електронної програми касових операцій «Утиліта» зазначеного супермаркету. Маючи умисел щодо внесення неправдивих відомостей до розділу названої програми, а саме змінення суми фактичного залишку грошових коштів, зловмисниця неодноразово вносила зміни до розділу фактичного залишку грошових коштів, зменшуючи суму. Попри наявність фактичного матеріального збитку, спричиненого такими діями, розслідуванням не було доведено корисливу мету злочинця [14]. Учиняючи такі злочини, шахраї зазвичай посилаються на помилкові дії або намагання приховати нестачу, яка фактично існувала до моменту їх злочинної дії.

5. Технології приховування незаконного походження безготівкових коштів, засновані на попередньому несанкціонованому втручанні в роботу комп'ютерної техніки. Такі технології вдало застосовує група осіб, що дозволяє організатору злочинної схеми уникати кримінальної відповідальності, причому поза увагою слідчого залишається багато обставин учинення злочину. Через це злочинна діяльність часто кваліфікується за ст. 361 та ст. 361-2 КК України або за ст. 205, 209 КК України. Така ситуація не дає можливості чітко впорядкувати сукупність злочинів, поєднаних цією технологією у єдиний ланцюг поведінки.

Розглянемо приклад. Невстановлені особи, перебуваючи у невстановлено-

му місці, на початку листопада 2014 р., діючи умисно, з корисливих мотивів прийняли рішення зареєструвати в системі розрахунків «WebMoney Transfer» облікові записи на анкетні дані сторонніх осіб з метою їх подальшого незаконного використання для проведення незаконних трансакцій із титульними одиницями обліку майнових прав, також вони розробили відповідний план і розподілили між собою злочинні ролі [15]. На початку листопада 2014 р. на сайті WebMoney невстановлені особи запропонували гр. К. створити декілька акаунтів за винагороду, на що той погодився. Користуючись довірою до себе з боку працівників Дружківського МВ ГУМВС України в Донецькій області, К. незаконно отримав доступ до персональних даних фізичних осіб і паспортів осіб, які проходили як свідки, потерпілі, підозрювані за кримінальними провадженнями. Ці дані зловмисник використав для створення акаунтів (облікових записів окремих осіб у системі WebMoney Transfer). Пізніше невстановлені особи, незаконно використовуючи реквізити доступу до записів у системі, шляхом здійснення електронних трансакцій перевели з платіжної системи Epayments грошові кошти в сумі 20 265 та 9 000 дол. США, легальне походження яких документально не підтверджено. З метою подальшої конвертації коштів у безготівкові кошти в банківській системі України особи здійснили трансакції з переведення титульних одиниць обліку майнових прав на облікові записи інших користувачів системи.

6. Технології незаконного збагачення, засновані на попередньому несанкціонованому втручанні в роботу комп'ютера, комп'ютерної системи, мережі з метою нейтралізації засобів інтелектуального захисту. Нині цю технологію не застосовує лише злочинець – користувач низького рівня. Кваліфікується така діяльність за сукупністю ст. 176 (порушення авторського та суміжних прав) та ст. 361 КК України. Так, у 2017 р. мешканець м. Львова з корисливих мотивів з метою отримання прибутку, не маючи відповідного дозволу від правовласника програмного продукту «1С» – ДП «Єврософтпром», маючи дистрибутив програмного продукту «1С:Підприємство 8 (8.3.6.236)», єдиної автоматизованої системи, до складу якої віднесено безпосередньо програмне забезпечення та систему захисту від несанкціонованого використання із застосуванням апаратних ключів HASP, шляхом використання програмних засобів (патчів) для змінення функціональності програмних продуктів «1С» втрутився в роботу автоматизованої системи, що призвело до незаконного запуску та використання програмного продукту на платформі «1С:Підприємство 8 (8.3.6.236)». Зазначені дії ОСОБА_1 призвели до порушення встановленого порядку маршрутизації інформації, внаслідок чого програмний продукт «1С:Підприємство 8 (8.3.6.236)» став спроможним завантажуватися та працювати без електронного (апаратного) ключа захисту [16].

7. Технології незаконного збагачення шляхом незаконних дій із платіжними картками. Така злочинна діяльність в Україні найчастіше кваліфікується за сукупністю ст. 200, 190 КК України. Можна навести такі сучасні закономірності названої злочинної діяльності: 1) складність технологій і тип злочинця нерозривно пов'язані; чим вищий професійний рівень зловмисника, тим складнішою є технологія; 2) початкові дії традиційного злочинця не спрямовані на незаконний вплив на засоби комп'ютерної техніки та інформацію; 3) така злочинна діяльність пов'язана із застосування комплексу спеціальних комп'ютерних технологій, що дозволяють виготовити дублікат справжньої банківської картки.

Найбільшого поширення сьогодні набула технологія з визначеними етапами злочинної діяльності: 1) через електронні дошки оголошень або соціальні спільноти злочинець замовляє й отримує пристрій, що має функції зчитування, стирання, запису інформації на магнітній смузі пластикової платіжної карти; 2) використовуючи ті самі ресурси, злочинець підшукує персональні банківські відомості – т. зв. «дампи» про чужі банківські карти, їх власників / утримувачів і за допомогою криптовалюти «btc» (біткоін) через власний особистий рахунок набуває

собі «дампи», емітовані іноземними банками, інформацію яких зберіг на власній Інтернет-сторінці; 3) підбір платіжних карт у вигляді емітованих в установленому законодавством порядку пластикових карток, що використовуються для переказу грошей з рахунку платника або відповідного рахунку банку, оплати товарів і послуг через банківські термінали; 4) за допомогою придбаного раніше обладнання здійснюється запис інформації на магнітні смуги підібраних для цього платіжних карток і їх використання.

Так, гр. К., реалізовуючи свій злочинний намір з використанням Інтернет-ресурсу «Google Disk», отримував від невстановленої особи на свій обліковий запис «Google» електронні файли, що містили інформацію про дані магнітних смуг платіжних карток клієнтів АТ «Ощадбанк» (що дають можливість ідентифікувати платіжну систему й емітента), які були необхідні для незаконного виготовлення «дублікатів» платіжних банківських пластикових карток і їх ПІН-кодів [17]. Для підробки платіжних карт К. за погодженням із невстановленою особою використовував спеціальні платіжні засоби у вигляді емітованих в установленому законодавством порядку пластикових карток (банківські платіжні картки, зокрема строк дії яких завершився, картки надання дисконтних знижок у різноманітних закладах харчування, АЗС тощо з наявною відповідною магнітною смугою), а також білі пластикові картки з магнітними смугами. З квітня 2016 р., діючи за попередньою змовою з невстановленою особою, шахрай з'єднував зазначене обладнання в єдиний програмно-технічний комплекс, під'єднував до мережі Інтернет та за допомогою пристроїв «MSR606» (с/н 20130821 та с/н 20132176) записував на магнітні смуги підшуканих платіжних карток реквізити (отримані від не встановлених розслідуванням осіб текстові та цифрові дані) банківських карт клієнтів АТ «Ощадбанк», отримуючи таким чином їх копії. Частина з них була не персоніфікованою, але функціональною за призначенням. Після виготовлення таких копій банківських карток клієнтів АТ «Ощадбанк» зловмисник провів низку несанкціонованих трансакцій через банкомати.

Наприкінці вважаємо за необхідне відзначити, що знання типових технологій учинення злочинів у кіберпросторі дозволить слідчому в перебігу розслідування конкретного кримінального правопорушення якісно та методично обґрунтовано поставитися до висування версій, планування й організації досудового слідства.

ЛІТЕРАТУРА:

1. Крылов В.В. Расследование преступлений в сфере информации. М., 1998. 264 с.

2. Снігерьов О.П., Голубєв В.О. Проблеми класифікації злочинів у сфері комп'ютерної інформації. Вісник Університету внутрішніх справ МВС України. 1999. № 5. С. 25–28.

3. Настільна книга слідчого / ред. кол. В.Я. Тацій, М.Г. Панов, В.Ю. Шепітько. К., 2003. 716 с.

4. Айков Д. Сейгер К., Фонсторх У. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями / пер. с англ. М., 1999. 351 с.

5. Батурин Ю.М. Проблемы компьютерного права. М., 1991. 72 с.

6. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти: навч. посіб. К., 1994. 72 с.

7. Вехов В.Б. Компьютерные преступления: Способы совершения и раскрытия / под ред. Б.П. Смагоринского. М., 1996. 182 с.

8. Цехан Д.М. Використання високих інформаційних технологій в оперативно-розшуковій діяльності органів внутрішніх справ: монографія / за ред. О.О. Подобного. Одесса, 2011. 216 с.

9. Викрито хакера, який зламав облікові записи користувачів соціальних мереж / Департамент кіберполіції. URL: https://cyberpolice.gov.ua/news/kiberpolicziya-vykryla-xakera-u-zlami-oblikovyx-zapysiv-korystuvachiv-soczialnyx-merezh-6339/.

10. Вирок у справі № 161/10410/13-к від 21 жовтня 2013 р. Луцького міськрайонного суду Волинської області. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/34405754.

11. Вирок у справі № 161/1345/18 від 21 березня 2018 р. Луцького міськрайонного суду Волинської області. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/72886703.

12. Вирок у справі № 161/20739/13-к від 12 травня 2014 р. Луцький міськрайонний суд Волинської області. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/38642120.

13. Вирок у справі № 761/10994/14-к від 23 квітня 2014 р. Шевченківський районний суд м. Києва. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/38502750.

14. Вирок у справі № 753/15944/16-к від 25 жовтня 2016 р. Дарницького районного суду м. Києва. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/62224792.

15. Вирок ЄУН 229/2951/16-к від 11 жовтня 2016 р. Дружківський міський суд Донецької області. Єдиний державний реєстр судових рішень. URL: http://reyestr.court.gov.ua/Review/62206468.

16. Вирок у справі № 465/2887/17 від 23 червня 2017 р. Франківський районний суд м. Львова. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/67455018.

17. Вирок у справі № 761/39282/16-к від 30 листопада 2016 р. Шевченківського районного суду м. Києва. Єдиний державний реєстр судових рішень. URL: http://www.reyestr.court.gov.ua/Review/63392350.