such organization and methods of work became ineffective very quickly. The scope of activities was expanded and working methods changed with the further development and improvement of organizational and legal forms of the activities of Kharkiv militia. Decisions on releasing militia from extrinsic functions were repeatedly made during this period; nevertheless, it was overloaded with them. According to various estimates, up to 80 % of performed work was not within the direct scope of protecting public order, which certainly had a negative effect on the state of public safety.

Keywords: workers and peasants' militia, Kharkiv region, agencies of keeping public order, militia districts of the city, district superintendent, sanitary and administrative department, public safety.

УДК 343.1:65.012.8

О. В. Манжай,
кандидат юридичних наук, доцент,
доцент кафедри захисту інформації факультету № 4 (кібербезпеки)
Харківського національного університету внутрішніх справ;
ORCID: http://orcid.org/0000-0001-5435-5921

ОСОБЛИВОСТІ ОГЛЯДУ ЗАСОБІВ КОМП'ЮТЕРНОЇ ТЕХНІКИ

Проаналізовано особливості огляду засобів комп'ютерної техніки та сформульовано загальний порядок його проведення. Охарактеризовано основні види такого огляду, засоби комп'ютерної техніки, з якими доводиться стикатися правоохоронним органам. Проаналізовано головні проблемні моменти, які існують у досліджуваній сфері. Розкрито особливості роботи правоохоронних органів на підготовчих етапах, а також безпосередньо під час огляду. Акцентовано увагу на важливості збирання та документування волатильних даних, наведено два основні способи їх збирання. Окреслено особливості огляду мобільних засобів комп'ютерної техніки, наведено приклади.

Ключові слова: комп'ютер, огляд, алгоритм, правоохоронні органи, протидія злочинності, засоби комп'ютерної техніки.

Постановка проблеми. Засвоєння практично всіма прошарками суспільства комп'ютерних технологій (за даними Міжнародного союзу електрозв'язку, в 2015 р. у світі частка окремих осіб-користувачів Інтернету становила 43,4 % [1, с. 1, 3]) сприяє невпинному зростанню випадків їх використання із протиправною метою. Так, лише за статистичними даними за окремою категорією зареєстрованих кіберзлочинів можна простежити експоненційне зростання принаймні виявлених правопорушень (рис. 1).

Зважаючи на викладене, правоохоронні органи все частіше стикаються з необхідністю огляду засобів комп'ютерної техніки (далі – ЗКТ) як під час здійснення оперативно-розшукових заходів, так і в рамках провадження слідчих і негласних слідчих (розшукових) дій.

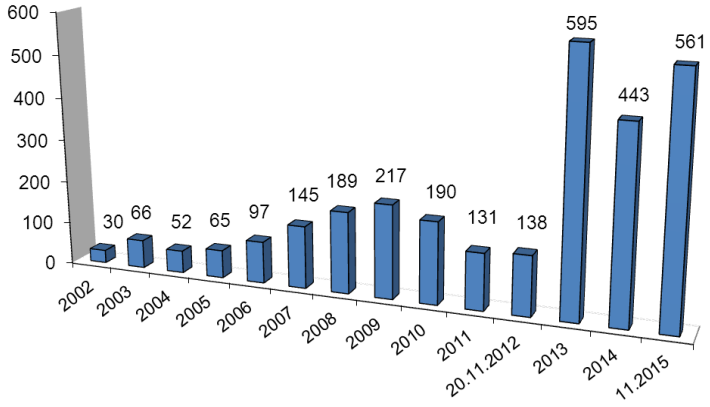

Рис. 1. Зареєстровані злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку за 2002–2015 рр.

Стан дослідження. Вивченням процедури огляду ЗКТ у різні часи займалися Г. К. Авдєєва, В. В. Бірюков, А. Ф. Волобуєв, Еоган Кейсі, Рональд Ван Дер Кніф, Роб Лі, М. Ю. Літвінов, Л. П. Паламарчук, Д. В. Пашнєв, Даріо Форте, В. Ю. Шепітько, М. Г. Щербаковський та ін. Проте велика кількість напрацювань у сфері техніки огляду ЗКТ на пострадянському просторі видаються вкрай поверховими та такими, що не відповідають сучасним умовам технологічного розвитку.

Метою цієї статті є проаналізувати особливості техніки огляду ЗКТ на сучасному етапі та сформулювати загальний порядок такого огляду.

Виклад основного матеріалу. Основними ЗКТ, з якими доводиться мати справу працівникам правоохоронних органів, на сьогодні є:

– стаціонарні персональні комп'ютери (робочі станції або сервери);
– ноутбуки та нетбуки;
– планшети;
– бортові комп'ютери автомобілів;
– телевізори з функцією SMART;
– GPS-навігатори;
– носії цифрової інформації (диски, флеш-носії тощо);
– периферійне обладнання (принтери, сканери тощо);
– мобільні комп'ютерні пристрої з функцією телефону [2, с. 105].

Враховуючи особливості роботи з наведеними пристроями, а також відповідне апаратне та програмне забезпечення, яке використовується для їх огляду, відповідний процес можна умовно поділити на чотири види:

1) огляд стандартних ЗКТ, носіїв і периферійних пристроїв;
2) огляд мобільних ЗКТ:

– з функцією телефона;
– автомобільних пристроїв;
3) огляд побутових ЗКТ («розумних речей»);
4) огляд інших ЗКТ.

Аналіз наукової, методичної, навчальної літератури та нормативних джерел дозволив виділити низку проблемних моментів, які існують у досліджуваній сфері.

1. На сьогодні не існує єдиної методики здійснення огляду ЗКТ. Наприклад, дискусії викликає питання, чи можна вилучати пристрої у ввімкненому стані, зокрема мобільні пристрої. Якщо вони вилучені таким чином, то як підтримувати їх джерела живлення в зарядженому стані?

2. У країнах пострадянського простору, а також у вітчизняній науковій та експертній сферах переважно спостерігається тяжіння до адаптації старих методик у нових умовах розвитку техніки. Причому увага чомусь концентрується не на порядку вилучення інформації (навіть у загальному вигляді), а на процедурі опису відповідних пристроїв у протоколі та їх опечатуванні. Так, наприклад, у російському підручнику з криміналістики 2007 року [3, с. 382] пропонується під час огляду місця події, де наявні ЗКТ, шукати коаксіальні кабелі, стримери, дискети тощо. Навіть у 2007 році, не говорячи про сучасну правоохоронну практику, такі ситуації були радше випадковістю, ніж звичайною практикою. Аналогічний підхід можна побачити в дисертації І. Є. Мазурова [4, с. 86–91], де навіть згадуються перфокарти.

3. Мовний бар'єр призводить до того, що найкращі методики здійснення огляду ЗКТ лишаються незатребуваними в Україні або впроваджуються із суттєвим запізненням, в окремих випадках як переклад відповідних методик однієї з країн колишнього СРСР, які імплементували ці методики із західної правоохоронної практики.

4. Розвиток технологій відбувається надто випереджаючими темпами порівняно із впровадженням відповідної нормативної та методичної бази, а також порівняно з процесом підвищення кваліфікації працівниками правоохоронних органів. У результаті знання та навички працівників правоохоронних органів є недостатніми для здійснення якісного та всеосяжного огляду ЗКТ.

5. Висока вартість техніки, потрібної для здійснення огляду ЗКТ, призводить до того, що на місцях її не вистачає, а низька оплата праці правоохоронців, задіяних у досліджуваній сфері, призводить до високої плинності кадрів у відповідних підрозділах.

6. Оскільки правоохоронним органам часто доводиться мати справу з великим обсягом даних, що підлягають огляду, то відповідно це призводить до суттєвих витрат часових, матеріальних і людських ресурсів (наприклад, час копіювання даних із жорсткого диска Seagate ST3320310CS 320 GB на Seagate ST3320613AS 320 GB за допомогою пристрою EPOS DiskMaster Portable складає 1 годину 26 хвилин. Аналогічна операція зі створення образу диска за допомогою стандартних ЗКТ збільшує цей час приблизно в 1,5 рази).

7. Нестача експертів, які мають право проводити комп'ютерно-технічну експертизу, утворює черги, які можуть тривати більше року, що є неприйнятним для забезпечення розумних строків кримінального провадження.

8. Особливості зберігання цифрових даних роблять їх легко втрачуваними та змінюваними.

9. Застарілі навчально-методична та матеріальна бази призводять до неактуальності знань, які набувають майбутні правоохоронці у вишах.

10. Використання клієнт-серверних технологій та термінального доступу, розподілений характер збереження даних можуть викликати труднощі юрисдикційного характеру (див. [5, с. 217–218]), а також неможливість відкладеного дослідження відповідних даних.

Перед проведенням відповідного огляду важливо правильно підібрати інструментарій оглядача. При цьому слід пам'ятати, що швидкий розвиток технологій, а також велика кількість умов, які виникають під час огляду ЗКТ, з чисто практичної точки зору унеможливлюють так звану сертифікацію відповідних апаратних та/або програмних засобів. Це підтверджується і правозастосовною практикою провідних західних країн [6, с. 26]. В Україні така сертифікація також не проводиться, зважаючи на її недоречність. Так само у процесі огляду потрібно намагатись уникати використання програм, наявних у системі, що підлягає огляду, адже потім буде складно підтвердити правильність їх роботи.

Тому, враховуючи українське законодавство, вважаємо за доцільне акцентувати увагу на двох важливих аспектах. По-перше, засоби, що використовуються, мають бути з відповідною відкритою ліцензією або такими, що перебувають на балансі правоохоронного органу, щоб можна було в будь-який час перевірити коректність їх роботи. По-друге, якщо використовується відкрите програмне забезпечення, наприклад, Live-CD під керуванням Linux, то відповідну копію з гешсумою диска потрібно долучити як додаток до протоколу огляду.

Основними інструментами, які можуть знадобитися працівникові правоохоронних органів для огляду ЗКТ, є: портативний комп'ютер з автономним джерелом живлення; привод CD-ROM (DVD-ROM); викрутки та інший інструмент; комплекти запасних батарей; диски з операційними системами та іншими програмними засобами, накопичувачі інформації, серед яких обов'язково має бути носій, ємністю більшою від ємності накопичувача, який підлягає огляду, блокувач жорсткого диска та/або набір дублікаторів, польовий комплект експерта-криміналіста тощо [2, p. 106–107]. Перелік інструментарію залежить від конкретної ситуації. У цьому сенсі у процесі його підбору вельми корисними стають регулярно оновлювані каталоги криміналістичних програмних та апаратно-програмних засобів. Наприклад, перелік криміналістичного програмного забезпечення, протестованого Американським інститутом стандартизації (NIST), можна зайти за інтернет-адресою http://www.cftt.nist.gov.

Після підготовки відповідного інструментарію, який можна вважати підготовчим етапом огляду, проведення інших підготовчих

заходів працівники правоохоронного органу переходять безпосередньо до збирання даних на місці події. З урахуванням вивчення сучасної зарубіжної та вітчизняної практики [7; 8; 9, p. 135–145], а також критичного осмислення цього матеріалу сам алгоритм огляду ЗКТ у загальному вигляді можна представити так:

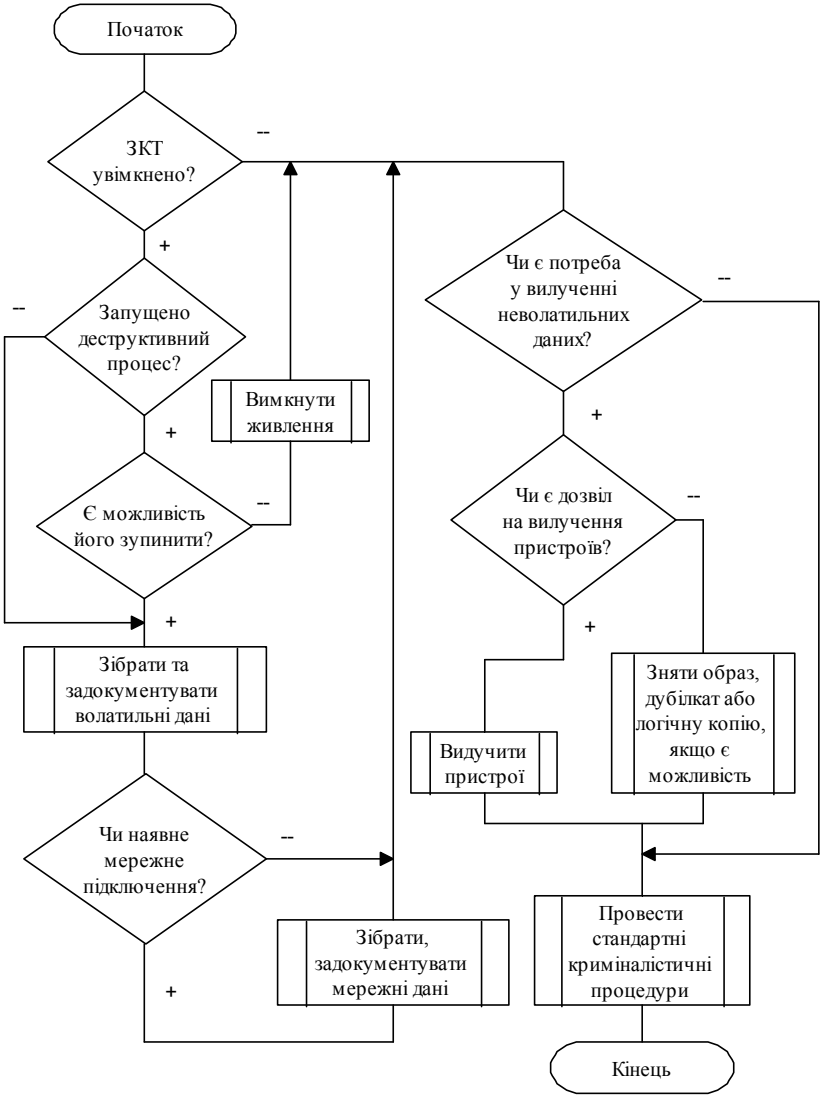

Рис. 2. Загальний алгоритм техніки огляду ЗКТ

Коментуючи окремі елементи цього алгоритму, потрібно зауважити, що на сьогодні в Україні практично не відбувається збирання та документування нестійких волатильних даних (зберігаються в енергозалежних запам'ятовувальних пристроях: оперативній пам'яті, кеші, регістрах), хоча саме вони часто містять ключі до різних криптоконтейнерів, останні повідомлення в мережі та відкриті документи тощо. Також само потрібно звернути увагу на мережні технології віддаленого зберігання даних (хмари, термінали тощо).

Щодо копіювання неволатильних даних, то на сьогодні у світі застосовується 3 головні способи одержання копій цифрових носіїв, що містять слідову інформацію:

1) створення образу відповідного носія;

2) створення дубліката носія;

3) логічне копіювання окремих даних.

Перший спосіб є більш повільним, однак з його допомогою працівник правоохоронних органів одразу одержує готовий для дослідження програмними засобами матеріал, який можна достатньо легко тиражувати для здійснення розподіленого дослідження декількома фахівцями одночасно.

У будь-якому випадку для убезпечення цифрових доказів рекомендується робити дві копії цифрового носія, одна з яких є контрольною (еталонною) та зберігається на випадок втрати або пошкодження іншої, робочої копії цифрового носія. Вилучені пристрої та носії потрібно належним чином зберігати та досліджувати. Наприклад, для дослідження мобільних пристроїв потрібно використовувати клітку Фарадея.

Перед зняттям копії більшості цифрових носіїв потрібно одержати геш-значення для вихідного носія інформації (джерела) за алгоритмом SHA-1 або SHA-2. Підрахунок гешу за допомогою алгоритму MD5 проводити не рекомендується, враховуючи можливості знаходження колізій із прийнятною обчислювальною складністю [10], що неодноразово демонструвалися дослідниками для цього алгоритму.

Слід пам'ятати, що особливості зберігання даних на окремих носіях (флеш-карти, SSD-вінчестери), а також вирівнювання ступеня їх зношеності [11] призводять до того, що посекторне геш-значення такого носія може не збігатися під час наступного підрахунку. У цьому випадку можна говорити лише про можливість підтвердження геш-значеннями так званих логічних структур даних, наприклад, окремих файлів.

Перед одержанням дубліката цифрового носія інформації (джерела) потрібно простерилізувати носій, на який будуть копіюватися відповідні дані (приймач). Цей носій, по-перше, має бути за ємністю більшим від джерела, по-друге, перед створенням дубліката його потрібно заздалегідь стерилізувати, тобто заповнити всі сектори нулями. Деякі дослідники пропонують лише частково стерилізувати

носій уже після копіювання даних у частині, що не зайнята скопійованими даними. Під час огляду стандартних ЗКТ провести процес стерилізації в операційній системі Windows можна, наприклад, за допомогою X-ways Forensics (Winhex). У Linux аналогічна процедура може бути виконанна командами:

```
fdisk -l
# перегляд інформації про носії;
dd if=/dev/zero of=/dev/sd[a-z] bs 2048
# заповнення нулями відповідного носія;
killall -USR1 dd
# перевірка стану роботи процесу dd (вводиться в іншому терміналі).
```

Підтвердити перед понятими, що диск є дійсно стерилізованим, можна:

1) в операційній системі Windows за допомогою підрахунку контрольної суми (Cheksum – логічна сума за допомогою операції «або») в програмі X-ways Forensics (Winhex);

2) у Linux з використанням команди пошуку ненульових значень:

```
grep -a -v '0' /dev/sd[a-z]
# у квадратних дужках вказано обрання відповідної літери для диска приймача.
```

У подальшому скопійовані дані найчастіше передаються для дослідження експерту, проте слідчий має право самостійно оглянути їх у рамках процедури огляду речей, результати чого зафіксувати у відповідному протоколі.

Якщо слідчий має необхідну кваліфікацію або залучив спеціаліста, то за допомогою відповідних засобів він може, наприклад, дослідити робочу копію образу.

У загальному вигляді такий огляд з урахуванням певних міркувань [12] можна представити так:

1. Аналіз даних, одержаних з оперативних запам'ятовуючих областей, у тому числі з буфера обміну

2. Аналіз залишкових слідів в елементах ОС, які вказують на дані, що оброблялися системою:

2.1. дослідження програмного забезпечення, яке використовується;

2.2. дослідження елементів системних файлів;

2.3. дослідження та перевірка назв і реквізитів ярликів;

2.4. дослідження файлів історій відповідних програмних засобів;

2.5. дослідження налаштувань інтернет-браузерів;

2.6. дослідження атрибутів і метаданих файлів, що викликали інтерес під час перевірки.

3. Аналіз безпосередньо файлів із даними шляхом контекстного пошуку за ключовими фразами:

3.1. дослідження файлів, які зберігаються на цифрових носіях, *зокрема:*

3.1.1. пошук прихованих і зашифрованих даних;

3.1.2. пошук і перевірка тимчасових файлів;

3.1.3. аналіз специфічних даних, передбачених структурою файлової системи, наприклад, альтернативних потоків даних;

3.1.4. аналіз файлів, що пов'язані з мережною активністю;

3.2. відновлення з наступним аналізом видалених файлів, *у тому числі:*

3.2.1. дослідження залишків файлів у кластерах;

3.2.2. перевірка вільного простору носіїв інформації;

3.2.3. перевірка файлів підкачки, якщо вони мають місце.

Огляд мобільних ЗКТ має свої особливості. Найбільш складним елементом у цьому процесі є зняття дампа даних мобільного пристрою, оскільки для цього потрібно мати спеціальні права доступу до нього. Дамп, як правило, знімається програмним шляхом, проте окремі апаратно-програмні комплекси дозволяють проводити зняття фізичного дампу пристроїв безпосередньо з відповідних чіпів (наприклад, UFED, XRY).

Висновки. У липні 2016 року в Харківському національному університеті внутрішніх справ завершується навчання першого потоку слухачів, які будуть працювати в кіберполіції. Досліджувана у статті тема була лише однією з багатьох, які засвоїли майбутні кіберполіцейські. Проте цілком очевидно, що саме правильно проведений з технічної та юридичної точок зору огляд ЗКТ є базою для успішного виявлення, припинення та розслідування кіберзлочинів.

Список бібліографічних посилань: **1.** Измерение информационного общества. Отчет 2015 год. Резюме/Международный союз электросвязи, Бюро развития электросвязи. Женева, 2015. [VII, 42] с. URL: https://www.itu.int/en/ITU-D/Statistics/Documents/publications/misr2015/MISR2015-ES-R.pdf. **2.** Виявлення, попередження та розслідування злочинів торгівлі людьми, вчинених із застосуванням інформаційних технологій (проект): навч. курс/В. Гузій, Д. Девіс, В. Дубина, М. Каліжевський, О. Манжай, В. Марков. Київ: Координатор проектів ОБСЄ в Україні, 2015. 158 с. **3.** Криминалистика: информационные технологии доказывания: учеб. для вузов/под ред. В. Я. Колдина. М.: Зерцало-М, 2007. 752 с. **4.** Мазуров И. Е. Методика расследования хищений, совершенных с использованием Интернет-технологий: дис. … канд. юрид. наук: 12.00.12. Казань, 2015. 197 с. **5.** Манжай О. В. Використання кіберпростору в оперативно-розшуковій діяльності. *Право і Безпека.* 2009. № 4 (31). С. 215–219. **6.** Handbook of Digital Forensics and Investigation/edited by Eoghan Casey. Elsevier Academic Press, 2010. 567 p. **7.** Петрович Л, В'ятов Н. Пошук та вилучення доказів: тренінг для тренерів з викладання тематики розслідування кіберзлочинів для представників навчальних закладів МВС України. Київ: Проект ОБСЄ «Посилення кримінального переслідування торгівлі людьми з використанням інформаційних технологій в Україні», 2014. 60 с. **8.** Літвінов М. Ю. Проблемні питання фіксації комп'ютерних слідів під

час здійснення огляду // Протидія кіберзлочинності в фінансово-банківській сфері: матеріали Всеукр. наук.-практ. конф. (Харків, 23 квіт. 2013 р.)/МВС України, Харків. нац. ун-т внутр. справ; Незалеж. асоц. банків України, Харків. банк. союз. регіон. представник НАБУ. Харків: Харків. нац. ун-т внутр. справ, 2013. С. 20–23. **9.** Mccoy M., Elliott R. Collection and Preservation of Digital Evidence // The Detective's Handbook/edited by John A. Eterno, Cliff Roberson. London; New-York: CRC Press, 2015. 358 с. **10.** MD5 // Википедия: свобод. энцикл. URL: https://ru.wikipedia.org/wiki/MD5. **11.** TRIM // Википедия: свобод. энцикл. URL: https://ru.wikipedia.org/wiki/TRIM. **12.** Манжай О. В., Бучак Т. А. Методика контекстного пошуку документів, які оброблялися в інформаційно-телекомунікаційній системі, в рамках проведення контрольних заходів по перевірці стану інформаційної безпеки організації // Інформатизація вищих навчальних закладів МВС України: матеріали наук.-практ. конф. (Харків, 27 квіт. 2007 р.)/МВС України, Харків. нац. ун-т внутр. справ. Харків, 2008. С. 151–153.

Надійшла до редколегії 01.07.2016

Манжай А. В. Особенности осмотра средств компьютерной техники

Проанализированы особенности осмотра средств компьютерной техники и сформулирован общий порядок его проведения. Охарактеризованы основные виды такого осмотра, средства компьютерной техники, с которыми приходится сталкиваться правоохранительным органам. Проанализированы основные проблемные моменты, которые существуют в исследуемой сфере. Раскрыты особенности работы правоохранительных органов на подготовительных этапах, а также непосредственно во время осмотра. Акцентировано внимание на важности сбора и документирования волатильных данных, приведены два основных способа их сбора. Очерчены особенности осмотра мобильных средств компьютерной техники, приведены примеры.

Ключевые слова: компьютер, осмотр, алгоритм, правоохранительные органы, противодействие преступности, средства компьютерной техники.

Manzhai O. V. Features of computer technique facilities examination

The features of examination of computer technique facilities have been analyzed; and the general procedure of its holding has been formulated. Special attention has been paid to the relevance of the studied issue, relevant statistics on Internet users and some types of committed cybercrimes have been provided. The author has determined the main means of computer facilities, which law enforcement agencies face. The main types of examination of computer technique facilities based on the type of studied means (standard, mobile, consumer, etc.) have been provided. On the basis of the analysis of scientific, methodical, educational literature and regulatory sources the author has highlighted a number of problematic issues that exist in the studied area. The author has revealed the features of law enforcement agencies' activities at the preparatory stages (tools formation, work with catalogs of forensic software, hardware means, and directly during the examination (general algorithm for data

collection, methods of securing collected data, peculiarities of working with flash drives, methods of sterilization of carriers in operating systems Linux and Windows, the procedure of examination of the collected data, etc.).

The attention has been paid on the importance of collecting and documenting volatile data (RAM, network processes, terminal clients' work). Two main ways of collecting non-volatile data (creating an image of corresponding carrier and its duplicate) have been revealed; their advantages and disadvantages have been analyzed. The peculiarities of examining mobile computer facilities, software and physical way of removing the backup of mobile devices have been outlined; some examples have been provided.

It has been concluded that properly conducted examination of computer technique facilities from technical and legal points of view is the basis for the successful detection, suppression and investigation of cybercrimes.

Keywords: computer, examination, algorithm, law enforcement authorities, crime combating, computer technique facilities.

УДК 343.31

Я. О. Морозова,
кандидат юридичних наук, докторант
Харківського національного університету внутрішніх справ

СУЧАСНИЙ СТАН ПРАВОВОГО РЕГУЛЮВАННЯ ПРОТИДІЇ ПІДРОЗДІЛАМИ КРИМІНАЛЬНОЇ ПОЛІЦІЇ ОРГАНІЗОВАНІЙ ЗЛОЧИННОСТІ ЗАГАЛЬНОКРИМІНАЛЬНОЇ СПРЯМОВАНОСТІ

Визначено правовідносини, що притаманні процесу протидії підрозділами кримінальної поліції організованій злочинності загальнокримінальної спрямованості, та, враховуючи їх правову природу, виокремлено нормативно-правові акти, що є правовим підґрунтям їх існування. В результаті проведеного дослідження констатовано, що сучасний стан правового регулювання оперативно-розшукової протидії підрозділами кримінальної поліції характеризується наявністю як двосторонніх, так і багатосторонніх та різнопланових за своєю юридичною природою правовідносин, які регулюються великою кількістю нормативно-правових актів.

Ключові слова: підрозділи кримінальної поліції, правове регулювання, організована злочинність, загальнокримінальна спрямованість.

Постановка проблеми. Аналіз статистичних даних правоохоронних органів України свідчить про щорічне зростання кількості вчинення злочинів, у тому числі загальнокримінальної спрямованості*. Водночас вбачається позитивна до зросту тенденція вчинення

* Див., наприклад, статистичні дані Генеральної прокуратури України (http://www.gp.gov.ua/ua/stat.html).