УДК 343.98

Я.Ю. Коліса, *експерт Науково-дослідного експертно-криміналістичного центру при УМВС України в Полтавській області*

ВЗАЄМОДІЯ СЛУЖБ У БОРОТЬБІ З КІБЕРЗЛОЧИННІСТЮ

Досліджено термін «кіберзлочинність». Визначено основні завдання комп'ютерно-технічної експертизи. Сформульовано основні проблеми, які виникають під час упакування комп'ютерної техніки у кримінальних справах. Запропоновано шляхи підвищення ефективності боротьби з кіберзлочинністю.

Ключові слова: кіберзлочинність, комп'ютерно-технічна експертиза, комп'ютер, віртуальний простір.

Исследовано понятие «киберпреступность». Определены основные задачи компьютерно-технической экспертизы. Сформулированы основные проблемы, возникающие при упаковке компьютерной техники по уголовным делам. Предложены пути повышения эффективности борьбы с киберпреступностью.

Explore the concept of cybercrime. Formulated basic problems in the packaging of computers equipment in criminal cases. Identified basic tasks of technical computer expertise. Suggested ways to improve the effectiveness in counteraction cybercrime.

Комп'ютеризація та інформатизація майже всіх сфер соціальної діяльності людини разом з безліччю переваг має й певні негативні наслідки. Йдеться насамперед про появу нового виду організованої злочинності — кіберзлочинності — та засоби її здійснення [1]. Цей порівняно новий вид злочинності багато в чому залежить від рівня захищеності комп'ютерних систем. Зрозуміло, що з розвитком комп'ютеризації та інформатизації суспільства еволюціонує і кіберзлочинність.

Слід зазначити, що сьогодні у вітчизняній криміналістиці немає чіткого визначення поняття кіберзлочину. Проте попри різні точки зору об'єктом незаконного посягання є інформація, яка обробляється в комп'ютерній системі, а засобом вчинення злочину — комп'ютер. Саме завдяки цьому засобу вчинення злочину злочинність і називають кіберзлочинністю, або комп'ютерною злочинністю. Пов'язаність цих понять з однаковим суспільно-небезпечним діянням дозволяє вважати їх рівнозначними. Але з огляду на те, що Україна 7 вересня 2005 року ратифікувала Конвенцію про кіберзлочинність, доцільно вживати термін «кіберзлочинність» [2].

Загалом кіберзлочинність — це злочинність у так званому віртуальному просторі — модельованому за допомогою комп'ютера інформаційному просторі, що містить відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому вигляді, які перебувають у процесі руху по локальних і глобальних комп'ютерних мережах, або відомості, які

зберігаються в пам'яті будь-якого фізичного чи віртуального пристрою та іншого носія, спеціально призначеного для їх зберігання, обробки і передачі [3].

Відповідальність за злочини зазначеної категорії передбачена розділом XVI Кримінального кодексу України «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» [4].

Одним із важливих засобів у створенні доказової бази для розкриття кіберзлочинної діяльності є комп'ютерно-технічна експертиза, успішне проведення якої значною мірою залежить від правильності упакування комп'ютерної техніки, яку вилучають. При цьому «правильною» упаковкою вважають заводську картонну коробку або поліетиленовий пакет, призначений для комп'ютерної техніки. При цьому горловини пакетів мають бути зав'язані нитками, на кінцях яких приклеюють аркуші паперу з відповідними написами та печатками органу, який вилучав техніку. У разі застосування заводських картонних коробок аркуші паперу наклеюють на них.

Також як упакування, зокрема для ноутбуку, може слугувати його сумка. Замки «блискавки» на сумці зшивають між собою, і до кінців нитки приклеюють паперову бирку з відповідними написами [5, с. 13].

Застосування зазначених видів упакування забезпечує зберігання об'єкта дослідження та запобігання несанкціонованому доступу до нього, а отже, в такому вигляді органи слідства повинні надсилати об'єкти дослідження на комп'ютерно-технічну експертизу.

Проте на практиці техніку часто упаковують неправильно. У кращому випадку об'єкти надсилають у полімерних пакетах, обклеєних клейкою прозорою стрічкою типу «скотч», під якою знаходиться аркуш паперу. З огляду на те, що прозору стрічку типу «скотч» можна доволі легко від'єднати від поверхні пакета, значних перешкод для несанкціонованого доступу до об'єктів дослідження за таких умов немає.

У такому випадку навіть якщо було прийнято рішення використати прозору стрічку типу «скотч», однаково потрібно дотримувати принципу поєднання пакувальних засобів обв'язування (зокрема, ниток) і аркушів паперу з печатками. І якщо немає можливості зав'язати горловину упакування ниткою, можна застосувати метод обв'язування всього упакування. Клапани коробки при цьому слід оклеїти липкою стрічкою, а саму коробку — перев'язати капроновою ниткою методом «хрест-на-хрест» [5, с. 10].

Водночас, як свідчить досвід експертної практики, непоодинокими є випадки, коли системні блоки персональних комп'ютерів взагалі не упаковують, а лише обклеюють важливі для його роботи гнізда чи кнопки паперовими бирками [5, с. 12]. Трапляються і випадки заклеювання аркушем паперу роз'єму живлення.

Зрозуміло, що неправильне упакування об'єктів дослідження може негативно впливати не лише на проведення комп'ютерно-технічної експертизи, а й на перебіг усього слідства.

Покращенню ситуації та підвищенню якості розслідування комп'ютерних злочинів сприятиме залучення відповідного спеціаліста для участі в огляді місця події. Він допоможе слідчому визначити, які саме об'єкти слід надавати експертові для проведення експертизи [6, с. 136; 7, с. 34].

При цьому слідчий має бути обізнаний з тими завданнями, які вирішує комп'ютерно-технічна експертиза, першим з яких є встановлення технічного стану комп'ютерної техніки (для цього слідство має надати експертові як комп'ютерну техніку, так і технічну документацію до неї). Технічно-справною є комп'ютерна техніка, яка виконує свої функції за призначенням.

Завданням комп'ютерно-технічної експертизи є і виявлення інформації, що міститься на комп'ютерних носіях, і визначення її цільового призначення (для цього експертові надають не лише комп'ютерну техніку, а й комп'ютерний носій інформації). Інколи можна обмежитися наданням лише комп'ютерного носія, попередньо проконсультувавшись з експертом. Для цього слідчий має пояснити експертові, яка саме інформація його цікавить. Такий підхід дозволить скоротити час, потрібний для проведення дослідження. Слід також пам'ятати, що пошук будь-яких файлів бажано здійснювати за 2—3 ключовими словами, а отже, слідчий має дотримувати цієї вимоги, а не писати речення у постанові про призначення експертизи, яку він виносить, як ключові слова. Адже у цьому випадку експерт мусить виокремлювати ключові слова із цих речень і проводити за ними пошук, що не лише ускладнює дослідження, а й суттєво його подовжує.

До завдань комп'ютерно-технічної експертизи належить також пошук і визначення вірусів та наявних програмних продуктів, у тому числі й шкідливих, призначених для несанкціонованого втручання в роботу комп'ютерів і комп'ютерних мереж. Це завдання доволі складне, адже є багато програмних продуктів, про існування яких нічого не відомо, призначення яких доволі складно визначити навіть після виконання їх програмного коду, а надто зі 100-відсотковою впевненістю стверджувати, що їх немає на комп'ютерному носії. Це так би мовити бомби уповільненої дії.

Таким чином, призначення судової комп'ютерно-технічної експертизи потребує максимально конкретного визначення кола питань, які ставлять на її вирішення, та обсягу потрібних для експертного дослідження матеріалів, а отже, попередньої консультації судового експерта [6, с. 136].

Зазначені суб'єктивні недоліки не є катастрофічними і можуть бути усунені або принаймні мінімізовані. Одним із вагомих інструментів для цього є посилення взаємодії з Експертною службою МВС України, зміст якої становить:

– обмін оперативною, статистичною, науково-методичною інформацією;

– проведення узгоджених слідчих дій;

– розробка і впровадження спільних рекомендацій щодо запобігання таким злочинам;

– розробка методики виявлення, вилучення та упакування комп'ютерної техніки;

– розробка методичних рекомендацій (інформаційно-довідкових матеріалів) для судово-слідчих органів з питань призначення комп'ютерно-технічних експертиз.

Потреба у подальшому проведенні наукової роботи з питань боротьби з кіберзлочинністю зумовлена швидкою динамікою технічних характеристик комп'ютерних систем, які не лише відкривають широкі можливості з їх використання, а й сприяють виникненню нових злочинних діянь у сфері інформаційних технологій.

Отже, як свідчить закордонний досвід практики боротьби з такими злочинами, суттєво підвищуються вимоги до рівня професійної підготовки працівників органів внутрішніх справ. Вони повинні мати глибокі юридичні знання, добре орієнтуватися бодай у базових поняттях інших наук (зокрема, математики, фізики, інформатики) та активно застосовувати їх на практиці.

Підбиваючи підсумок, слід наголосити на тому, що саме організація тісної взаємодії і координації зусиль правоохоронних органів, спецслужб, судової системи у боротьбі з кіберзлочинністю та наявність належної матеріально-технічної бази сприятимуть суттєвому підвищенню її ефективності.

Список використаної літератури

1. *Комп'ютерно-технічна* експертиза (загальна частина) : методика / [укл. Ковальов К.М., Корнійко С.М., Княждвірський В.О.]. — К. : ДНДЕКЦ МВС України, 2007. — 24 с.

2. *Конвенція* про кіберзлочинність. Ратифікована із застереженнями і заявами Законом України від 07.09.2005 № 2824-IV // Вісник Верховної Ради. — 2006. — № 5-6. — Ст. 7.

3. *Дзюндзюк В.Б.* Поява і розвиток кіберзлочинності [Електронний ресурс] / В.Б. Дзюндзюк, Б.В. Дзюндзюк // Державне будівництво. — 2013. — № 1. — Режим доступу до журн. : http://www.kbuapa.kharkov.ua/e-book/db/index.html.

4. *Кримінальний* кодекс України : станом на 8 серп. 2013 р. / Верховна Рада України. — Суми : ТОВ «ВВП НОТІС», 2013 — 180 с.

5. *Виявлення*, вилучення та упакування комп'ютерної техніки по кримінальних справах : метод. реком. / [уклад. А.М. Гаркуша]. — К. : ДНДЕКЦ МВС України, 2009. — 36 с.

6. *Сабадаш Р.В.* Судова комп'ютерно-технічна експертиза: правові підстави й особливості призначення / Р.В. Сабадаш // Науковий вісник Чернівецького університету. — 2013. — № 660. — С. 134—138.

7. *Дяченко Н.М.* Особливості проведення огляду місця події при вчиненні комп'ютерних злочинів : навч.-метод. реком. / Дяченко Н.М., Корнійко С.М., Княждвірський В.О. — К. : ДНДЕКЦ МВС України, 2007. — 42 с.