Крім суб'єктивних причин, присутні й об'єктивні труднощі в організації і проведенні медичного огляду затриманих та арештованих на предмет визначення наркотичного сп'яніння. Ні органи внутрішніх справ, ні органи охорони здоров'я на сьогодні не мають сучасних експрес-діагностичними приладів для визначення наявності наркотиків у біологічному середовищі людини. Звідси можна зробити висновок: аналізовані статистичні свідчення не зовсім повно і точно відображають картину стану і динаміки злочинів, скоєних споживачами наркотиків або під впливом наркотиків. Для фахівців наявність зв'язку незаконного обігу наркотиків і зловживання ними зі злочинністю очевидна, і, звичайно, загальна кількість злочинів, скоєних на грунті наркотизації, судячи з оцінок, не дві і не три тисячі, як це відбито в статистичній звітності, а набагато більша – десятки і навіть сотні тисяч. У цілому ж структура злочинів, скоєних споживачами наркотиків, мало чим відрізняється від структури загальнокримінальних злочинів.

Щоб забезпечити себе наркотиками, наркомани повинні мати значні кошти (за цінами «чорного ринку» один грам кокаїну, наприклад, коштував на початку 2000 р. порядку 100–150 доларів США). З огляду на непрацездатність багатьох наркоманів, їх соціальну занедбаність і кримінальне минуле неважко припустити, звідкіля і яким шляхом беруться гроші на придбання наркотиків. Квартирні і кишенькові крадіжки, шахрайство, вимагання, грабіж і розбій, придбання і збут майна, свідомо добутого злочинним шляхом, – ось далеко не повний перелік протиправних діянь, за допомогою яких «заробляються» гроші на покупку наркотиків. Вивчення архівних справ оперативного обліку за забарвленням «наркоманія» показало, що кожен третій розроблюваний був причетний до здійснення корисливого чи корисливо-насильницького злочину, причому деякі з них за 1-2 місяці скоювали серію таких злочинів.

Таким чином, наведені додаткові свідчення дозволяють говорити про те, що кожен третій майновий злочин по лінії УР здійснюється на грунті наркотизації.

**Список літератури:** 1. Клаггес Х. Борьба с преступностью, вызванной применением опиянящих веществ // Kriminalistik. 1990. № 11 (Сборник переводов. № 539). 2. Хартнол Л. *Современная ситуация, связанная с оценкой масштабов распространения наркомании* в европейских странах // Бюллетень по наркотикам. ООН, 1986 (Сборник переводов № 539). 3. Звіт перед українським народом. Десять років на варті правопорядку // Міліція України. 2002. №2.

*Надійшла до редколегії 15.02.02*

*Д.О. Бондаренко*

## КОМП'ЮТЕРНІ ЗЛОЧИНИ І НОВІТНІ ДЕРЖАВНІ СТРУКТУРИ ПО БОРОТЬБІ З НИМИ (НА ПРИКЛАДІ НАЦІОНАЛЬНОГО ПІДРОЗДІЛУ ПО БОРОТЬБІ ЗІ ЗЛОЧИНАМИ В СФЕРІ ВИСОКИХ ТЕХНОЛОПІЙ ВЕЛИКОЇ БРИТАНІЇ)

Інтернет – глобальна комп'ютерна мережа, що охоплює увесь світ. Сьогодні Інтернет має близько 15 мільйонів абонентів у більш ніж 150 країнах світу. Щомісяця розмір мережі збільшується на 7–10%. Інтернет утворює нібито ядро, яке забезпечує зв'язок різних інформаційних мереж, що належать різноманітним установам в усьому світі.

Інтернет, що включає World-Wide-Web, привернув пильну увагу вчених з різних галузей знання (утім, і незнання теж). Серед них гуманітарії – філософи, політики і політологи, теологи, економісти, соціологи, лінгвісти, етнографи, психологи, а також фахівці в галузі технічних наук – електроніки, математики, програмування, зв'язку й ін.

Бурхливий ріст Інтернет разом з істотним набором нових можливостей і послуг приносить і ряд нових проблем, найбільш неприємною з яких є проблема безпеки в цій мережі. Британська влада, піклуючись про національну безпеку в цілому, приділяє величезну увагу й безпеці комп'ютерних технологій. Вивчення й сприйняття досягнень у цій галузі розвинутих країн має збагатити невеликий досвід нашої держави, стати у пригоді як в сфері захисту національних комп'ютерних мереж, так і у вдосконалюванні управління в системі правоохоронних органів.

18 квітня 2001 року у Центральній частині Лондона був створений *Національний підрозділ по боротьбі зі злочинами в сфері високих технологій* (the National High-Tech Crime Unit – NHTCU) – перший у Великій Британії національний правоохоронний орган по боротьбі з кібер-злочинністю. Його засновник – міністр внутрішніх справ Джек Страв (Home Secretary, Jack Straw). *Основна функція цього відділу — боротьба з організованою кібер-злочинністю*, під якою розуміється хакерство, недавно прирівняне британським законодавством до тероризму, і різні фінансові шахрайства з використанням високих технологій.

Звертає на себе увагу скрупульозний підхід до підбору професіоналів на відповідальні посади в даному відділі. Главою відділу був призначений Льон Хінде (Len Hynds) (43 роки), що мав досвід служби в Міській поліції і *спеціалізувався в проведенні операцій, зв'язаних з дослідженням тяжких і організованих злочинів*. До цього він служив у Національному Карному Відділі Англії й Уельсу (the National Crime Squad of England and Wales). Основну задачу при відкритті Національного підрозділу по боротьбі зі злочинами в сфері високих технологій Льон Хінде висловив у своїй програмній промові: «За останні 100 років британська поліція змінилася докорінно. Наш Національний відділ по боротьбі зі злочинами в сфері високих технологій сформований на національній основі. Його діяльність буде *спрямована* на боротьбу з on-line злочинністю. Однак є реальна загроза того, що злочинці будуть намагатися всіляким способами заважати нашій роботі. Для формування підрозділу необхідні час і люди, які здатні працювати сумлінно й володіють професійними навичками щодо розкриття комп'ютерних злочинів. Програма по прийому службовців на роботу вже розроблена» [1].

Розглянемо структуру Національного відділу по боротьбі зі злочинами в сфері високих технологій. Він складається з 4 підрозділів: 1) розшуку (Investigations); 2) інформаційного відділу (Intelligence); 3) допоміжного відділу(Support); 4) відділу судового пошуку злочинців (Forensic Retrieval). У відділі працюють фахівці правоохоронної діяльності, які відібрані з числа працівників: 1) Національного злочинного відділу (the National Crime Squard); 2) Національного карного інформаційного відділу (the National Criminal

Intelligence Service): 3) Митного й Акцизного управління (HM Customs and Excise); 4) поліцейських підрозділів (police forces). Набрано близько 40 фахівців на такі посади: офіцери пошукового відділу (investigative officers); судові експерти (forensic experts); комп'ютерні консультанти (computer consultants). Окрему групу працівників складає Допоміжний персонал (support staff).

*Національний відділ по боротьбі зі злочинами в сфері високих технологій* прямо зв'язаний з Відділами з комп'ютерних злочинів (Computer Crime Units), що працюють при поліцейських дільницях, а так само з підрозділами, що охороняють закон. Тісна взаємодія і співробітництво з *Національним інфраструктурним секретним координаційним центром* (the National Infrastructure Security Coordination Center) дає можливість Національному відділу по боротьбі зі злочинами в сфері високих технологій вчасно розкривати, а так само припиняти тяжкі й організовані злочини, зроблені на національному і міжнародному рівнях. Відповідальна роль в оперативній відсічі «атак» злочинців на комп'ютерні системи належить *Підрозділу Розшуку національного відділу по боротьбі зі злочинами в сфері високих технологій* (Investigations of the NTHCU), який розслідує тяжкі і організовані комп'ютерні злочини. Він працює разом з *Відділом карного розшуку* (the Criminal Investigations). Ступінь втручання в справи Відділу карного розшуку з боку Національного відділу по боротьбі зі злочинами в сфері високих технологій залежить від серйозності «нападу» на комп'ютерні системи, а так само від території, на якій відбулися злочину.

*Інформаційний підрозділ Національного відділу по боротьбі зі злочинами в сфері високих технологій* (the Intelligence section of the NHTCU) тісно взаємодіє з Національним карним дослідницьким відділом (the National Criminal Intelligence Service) для визначення й аналізу загрози, що виходить від злочинних дій. Узагальнення комп'ютерних злочинів, з одного боку, відіграють ключову роль у припиненні і пошуку злочинців, з іншого – дають зведення політикам, уряду й іншим структурам держави про можливі злочини, волаючи їх до пильності і надійної охорони комп'ютерних систем. Задача *Допоміжного відділу Національного відділу по боротьбі зі злочинами в сфері високих технологій* (the Support section of the NHTCU) полягає у пошуку і добору фахівців в галузі комп'ютерних технологій, а так само у взаємодії з колегами за кордоном. *Відділ судового пошуку злочинців Національного відділу по боротьбі зі злочинами в сфері високих технологій* (the Forensic Retrieval Section of the NHTCU) збирає і систематизує дані про злочини, надає їм електронного вигляду.

Злочини в мережі Інтернет, в основному, відбуваються з метою одержання грошей електронним шляхом. Як вважають британські фахівці в галузі комп'ютерних технологій, одним зі способів запобігання таких злочинів є партнерство з закордонними правоохоронними організаціями. А для більш ефективної роботи необхідне співробітництво з органами, взаємодіючими з промисловістю і банківською сферою [2].

Закордонними фахівцями розроблені різні класифікації способів здійснення комп'ютерних злочинів. Нижче приведені назви способів

здійснення подібних злочинів, що відповідають кодифікатору Генерального Секретаріату Інтерполу. У 1991 р. даний кодифікатор був інтегрований в автоматизовану систему пошуку і в даний час доступний більш ніж 100 країнам. Усі коди, що характеризують комп'ютерні злочини, мають ідентифікатор, що починається з літери Q. Для характеристики злочину можуть використовуватися до п'яти кодів, розташованих у порядку убування тяжкості скоєного кібер – злочину: 1) **QA – Несанкціоновані доступ і перехоплення** (**QAH** – комп'ютерний абордаж; **QAI** – перехоплення; **QAT** – крадіжка часу; **QAZ** – інші види несанкціонованого доступу і перехоплення); 2) **QD – Зміни комп'ютерних даних** (**QUL** – логічна бомба; **QDT** – троянський кінь; **QDV** – комп'ютерний вірус; **QDW** – комп'ютерний хробак; **QDZ** – інші види зміни даних); 3) **QF – *Комп'ютерне шахрайство*** (**QFC** – шахрайство з банкоматами; **QFF** – комп'ютерна підробка; **QFG** – шахрайство з ігровими автоматами; **QFM** – маніпуляції з програмами введення-виведення; **QFP** – шахрайства з платіжними засобами; **QFT** – телефонне шахрайство; **QFZ** – інші комп'ютерні шахрайства); 4) **QR – Незаконне копіювання** (**QRG** – комп'ютерні ігри; **QRS** – інше програмне забезпечення; **QRT** – топографія напівпровідникових виробів; **QRZ** – інше незаконне копіювання); 5) **QS – Комп'ютерний саботаж** (**QSH** – з апаратним забезпеченням; **QSS** – із програмним забезпеченням; **QSZ** – інші види саботажу); 6) **QZ – Інші комп'ютерні злочини** (**QZB** – з використанням комп'ютерних дошок оголошень; **QZE** – розкрадання інформації, що складає комерційну таємницю; **QZS** – передача інформації конфіденційного характеру; **QZZ** – інші комп'ютерні злочини).

Комп'ютерні злочини – надзвичайно багатогранні і складні явища. Об'єктами таких злочинних зазіхань можуть бути самі технічні засоби (комп'ютери і периферія) як матеріальні об'єкти або програмне забезпечення і бази даних, для яких технічні засоби є оточенням; комп'ютер може виступати як предмет зазіхання або як інструмент. До основних видів комп'ютерних злочинів можна віднести наступні: несанкціонований доступ до інформації, що зберігається в комп'ютері; введення в програмне забезпечення «логічних бомб», що спрацьовують при виконанні визначених умов і виводять частково чи цілком з ладу комп'ютерну систему; розробка і поширення комп'ютерних вірусів; розкрадання комп'ютерної інформації.

*Національний відділ по боротьбі зі злочинами в сфері високих технологій пропонує такі заходи протидії кібер-злочинам*, як: 1) *технічні* (захист від несанкціонованого доступу до комп'ютерної системи; резервування важливих комп'ютерних систем; уживання конструкційних заходів захисту від розкрадань і диверсій; забезпечення резервним електроживленням; розробка і реалізація спеціальних програмних і апаратних комплексів безпеки й ін.); 2) *організаційні* (охорона комп'ютерних систем; підбор персоналу; виключення випадків ведення особливо важливих робіт тільки однією людиною; наявність плану для відновлення працездатності центра у випадку виходу його з ладу; організація обслуговування обчислювального центра сторонньою організацією або особами, незацікавленими у приховані фактів порушення роботи центру; універсальність засобів захисту від усіх користувачів (включаючи вище

керівництво); покладання відповідальності на осіб, що повинні забезпечити безпеку центра; вибір місця розташування центра і т.п.); 3) *правові* (розробка норм права, що установлюють відповідальність за комп'ютерні злочини; захист авторських прав програмістів; удосконалювання кримінального і цивільного законодавства, а також судочинства; громадський контроль за розроблювачами комп'ютерних систем і т.п.).

Захист інформаційної системи є насущною задачею правоохоронних органів України, яким бажано перейняти досвід організаційно-правового регулювання боротьби з комп'ютерними злочинами, який накопичено у Великій Британії. Утішно, що в Україні вже створений Центр дослідження проблем комп'ютерної злочинності (директор Голубєв В., кандидат юридичних наук). Поки головні зусилля Центра спрямовані на обґрунтування необхідності удосконалювання українського законодавства в цьому напрямку, зокрема Кримінального кодексу, його розділу XVI «Злочини в сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж» [3, с.4; 4, с.5]. Уявляється, що правотворчий (законодавчий) і правозастосувальний (правоохоронний) процеси в Україні, наукові пошуки і практична діяльність у сфері відносин «людина-комп'ютер» повинні удосконалюватися паралельно, розвиватися узгоджено. Крім Центру досліджень проблем комп'ютерної злочинності необхідне створення спеціалізованого Центру на зразок Національного підрозділу по боротьбі зі злочинами в сфері високих технологій Великої Британії (можливо, з відділеннями в АРК і областях), що діяв би цілеспрямовано і злагоджено для своєчасного припинення зловживань комп'ютерними технологіями.

**Список літератури:** 1. http://www.nationalcrimesquad.police.uk. 2. http:// www. nhtcu.org. 3. В. Голубєв. Комп'ютерна злочинність // Юридичний вісник. 2002. 9–15 лютого. 4. В.Голубєв. Комп'ютерна злочинність // Юридичний вісник. 2002. 16–22 лютого.

*Надійшла до редколегії 12.03.02*

*І.І. Шинкаренко*

## ПСИХОЛОГІЧНІ АСПЕКТИ ОТРИМАННЯ ОПЕРАТИВНОЇ ІНФОРМАЦІЇ

Закон України «Про оперативно-розшукову діяльність»(ст.8) визначає, що працівники оперативних підрозділів як суб'єкти ОРД мають право збирати дані, що характеризують діяльність підприємств, установ, організацій, а також спосіб життя окремих осіб, підозрюваних у підготовці або вчиненні злочину, джерело та розмір їх доходів.

Одним з методів, завдяки якому оперативні працівники можуть отримати цю інформацію, є опитування.

Опитування – один з найбільш розповсюджених методів дослідження різних проблем суспільного життя. Його метою є отримання зі слів опитуваних інформації про об'єктивні та суб'єктивні факти, про обставини, які можуть бути важливими чи мати доказове значення під час здійснення оперативно-розшукової діяльності чи проведення розслідування [1, с.60].

В оперативно-розшуковій діяльності опитування – це метод, за допомогою якого оперативні працівники (суб'єкти) отримують інформацію у осіб