УДК 343.919:343.533

Л. В. Борисова

СУБ'ЄКТ (ОСОБА) ТРАНСНАЦІОНАЛЬНОГО КОМП'ЮТЕРНОГО ЗЛОЧИНУ: КРИМІНАЛІСТИЧНІ Й ПСИХОФІЗІОЛОГІЧНІ АСПЕКТИ

Виявлення на місці злочину слідів, які визначають характерний «почерк» злочинця, деякі особливості соціально-психологічних ознак, свідчать про наявність у злочинця спеціальних знань і навичок, а часто фахової освіти, стать, вік, особливості відносин з потерпілими, мотивації та цілі його злочинної поведінки. Мотивація є важливим елементом психології особи взагалі та особи злочинця зокрема. Мотивація злочинної поведінки пов'язана з об'єктивними умовами соціального середовища і на переконання В. Г. Асєєва «пронизує її основні структурні утворення: спрямованість особистості, характер, емоції, здібності, діяльність і психічні процеси» [1, 9]. Найбільше поширення отримало уявлення стосовно мотиву як потреби та розглядається як спонукання людини до діяльності. За визначенням К. Є. Ігошева: «Мотив злочинної поведінки можна визначити як сформоване під впливом соціального середовища і життєвого досвіду особи спонукання, яке є внутрішньою безпосередньою причиною злочинної діяльності та виражає особистісне ставлення до того, на що спрямована злочинна діяльність» [2, 66]. У зв'язку з цим говорять про мотиви, спонукання, імпульси, тенденції та потребу [3, 36]. У певних умовах мотивами визнаються наміри, які «є відносно стійкими утвореннями» й «формуються в стані холодного розуму і розрахунку» [4, 143].

Мотиви вчинення транснаціональних комп'ютерних злочинів різноманітні й частину їх можна віднести до «вічних»: жадоба, цікавість чи помста. Вважаємо, що значне місце в цьому списку мотивів займає ***унікальний за своєю суттю мотив — інтелектуальна боротьба між людиною і комп'ютерною системою.*** За висловом Ю. М. Батуріна, наприклад, основним чинником, який спрощує розслідування, звичайно є обмежене коло здібних вчинити хитріший комп'ютерний злочин, що полегшує «виявлення» злочинця»[1] [5, 41].

Отримання достатньо повних відомостей стосовно особи злочинця може стати для слідства неоцінимою послугою. Комп'ютерним злочинцям даються неоднозначні соціально-психологічні характеристики, які засновані на узагальнених емпіричних даних, оскільки сам предмет розгляду недостатньо вивчений з причин специфічності й складності комп'ютерних злочинів, а також бракує інформації стосовно кожного конкретного злочину. Вітчизняні та зарубіжні дослідження дають змогу визначитися із загальними характерними рисами комп'ютерного злочинця. Згідно з визначенням американського кримінолога, який першим досліджував цю проблему в 1940-х роках, «білокомірцева» злочинність — це злочини, які вчиняються представниками вищих верств суспільства і пов'язані з їхньою професійною діяльністю [6, 45–59]. З часів Е. Сатерленда ця проблема не тільки не втратила своєї актуальності, але стала більш значною[2].

З урахуванням комп'ютеризації різних сфер діяльності, а також аналізу транснаціональних комп'ютерних злочинів і загальних тенденцій розвитку цього виду злочинів «зарубіжні експерти роблять висновок про обумовленість розширення потенціальних можливостей для вчинення злочинів даної категорії» [7, 265–267]. Особливу групу комп'ютерних злочинців становлять хакери. Глобальні оцінки хакерства варіюються у відповідності до екстраполяцій журналу Jane's Intelligence Review, що базуються на оцінках 1990-х років, наведених В. Стерлінгом у його дослідженнях «Падіння хакера: закон і безладдя на електронній границі». Згідно з цими оцінками, загальна кількість хакерів близько 100 тисяч, з яких 10 тисяч є відданими ентузіастами комп'ютерної справи. Група чисельністю 250–1000 чоловік утворює еліту хакерів, які є спеціалістами високого фаху, спроможними здійснити проникнення в корпоративні мережі й зруйнувати корпоративну безпеку [9, 4].

Створюючи типову модель комп'ютерних злочинців, треба намагатися спростити завдання оптимізації діяльності з виявлення кола осіб, підозрюваних у вчиненні аналізованого злочину. Відповідно до результатів досліджень, які проводилися спеціалістами Dafapro Information Services Group, відмічено значне збільшення кількості спроб несанкціонованого доступу до інформації, циркулюючої у комп'ютерній мережі загального використання. Статистика порушень така: близько 3 % — зовнішні порушення, а саме проникнення на територію; 70–75 % — внутрішні порушення, з яких: 10 % — вчинені невдоволеними службовцями — користувачами системи; 10 % — вчинені з корисливих спонукань персоналом системи; 50–55 % — результат несвідомих помилок персоналу та/або користувачів системи як наслідок недбайливості, халатності або некомпетентності [10]. На основі аналізу слідчих матеріалів швейцарської поліції були виявлені такі характерні особливості комп'ютерних злочинців. Переважна частина — чоловіки. Вік 87 % злочинців 20–40 років, 13 % — старші 40 років. Більшість злочинців (77 %) мали середній рівень інтелектуального розвитку, 21 % — вище середнього і тільки 2 % — нижче середнього; 52 % правопорушників мали спеціальну підготовку в галузі автоматизованої обробки інформації. Більшу частину правопорушників (97 %) становили службовці обчислювальних центрів і відповідних установ, у тому числі 30 % злочинців мали безпосереднє відношення до експлуатації комп'ютерних пристроїв. Більшість злочинців здійснювали протиправні дії з метою збагачення. Згідно із слідчими матеріалами за справами стосовно комп'ютерного шпіонажу виявлені такі характерні особливості злочинців: із усіх правопорушників 93 % — чоловіки. Вік 92 % злочинців був від 20 до 40 років, інші старші 40 років, 50 % злочинців закінчили народні школи, 44 % — середні, 6 % — вищі навчальні заклади. У 93 % злочинців був середній рівень інтелектуального розвитку, в інших — вище середнього. Більше 80 % правопорушників мали спеціальну підготовку в галузі автоматизованої обробки інформації. Серед них 48 % виявилися службовцями установ і фірм, в яких були вчинені комп'ютерні злочини. Аналіз слідчих матеріалів швейцарської поліції в справах комп'ютерного саботажу виявив, що вік 25 % злочинців не перевищував 20 років, інші — 20–

40 років. За оцінками експертів, 90 % осіб, які вчинили злочини, мали середній рівень інтелектуального розвитку, інші — вище середнього. Усі злочинці мали спеціальну підготовку і половина злочинців були співробітниками постраждалих установ, організацій та фірм [11, 299].

У професійно-кваліфікаційному плані коло комп'ютерних злочинців надзвичайно широке: до них відносять різноманітні категорії керівників і спеціалістів — комерційні директори, банківські службовці, фінансисти, програмісти, інженери-наладчики і монтажники комп'ютерного устаткування, бухгалтери тощо. Серйозною проблемою для слідчого є суміщення професій при експлуатації обчислювальної техніки (бухгалтер є програмістом і оператором). Як результат взаємні перевірки ускладнюються, ймовірність зловживань зростає, а це ускладнює слідчі дії. Виходячи з цього, в літературі пропонуються різноманітні класифікації подібного кола осіб.

Наприклад, Д. С. Страубом і К. Уідомом виділяються чотири типові групи [12, 431–441] (табл. 1).

Таблиця 1

Мотив	Групи ймовірних злочинців
1 Ігнорування етики	Професійні порушники режимів експлуатації комп'ютера
2 Користь (особиста нажива)	Злочинці в «білих комірцях»
3 Користь (корупція)	Високопоставлені чиновники
4 Інші антисуспільні мотиви	Професійні злочинці, хакери, особи з психічними порушеннями

Опитувані представники служб безпеки організацій вважають, що основна небезпека щодо вчинення комп'ютерного злочину виходить саме від безпосередніх користувачів і ними вчиняється 94 % злочинів, при цьому 70 % — це клієнти — користувачі комп'ютерної системи, 24 % — обслуговуючий персонал [13, 42].

Виходячи з аналізу вітчизняних і зарубіжних літературних джерел, доцільно поділити замахи на внутрішні й зовнішні у відповідності до класифікації категорій доступу до засобів комп'ютерної техніки для користувачів: внутрішні користувачі і зовнішні користувачі, де користувач — фізична особа, яка взаємодіє з комп'ютерною системою. Загрозу можна вважати «внутрішньою» і у випадку, коли працівник фірми або організації передає стороннім особам інформацію, що сприяє несанкціонованому проникненню до локальної комп'ютерної системи.

Отже, групи осіб, які ймовірно можуть бути злочинцями, розподіляються в такий спосіб (табл. 2)[3].

Розглянемо докладніше кожну з категорій користувачів.

Перша група — особи, які спромоглися використати можливості комп'ютерних мереж у своїх злочинних цілях і які не належать ні до числа праців-

Таблиця 2

	Внутрішні	**Зовнішні**
Особи, які не мають трудових відносин з організацією-жертвою	ні	так
Особи, які мають санкціонований доступ до комп'ютерної системи постраждалої організації	так	так
Особи, які знаються на роботі комп'ютерної системи і зуміли використати її у корисливих цілях	так	так
Посадові особи організацій	так	ні
Користувачі комп'ютерних систем, які зловживали своїм становищем	так	ні

ників організації, ні до числа тих, хто займається сервісним обслуговуванням комп'ютерних систем відповідно до договору, укладеному даною організацією.

До другої групи осіб належать працівники організації з санкціонованим доступом до периферійних пристроїв та іншого устаткування, що входить до єдиного контуру локальної комп'ютерної чи телекомунікаційної мережі, а також особи, які не є такими, але мають доступ до комп'ютерних систем по комп'ютерним мережам (особи, які займаються сервісним обслуговуванням обладнання).

Третя група — це особи, які за родом своєї фахової діяльності безпосередньо пов'язані з комп'ютерними системами або відповідають за їхнє нормальне функціонування (технічне обслуговування) як працівники даної організації. В інтелектуальному відношенні вони можуть застосовувати більш складні засоби для вчинення і приховування комп'ютерних злочинів.

До четвертої групи належать працівники всіх рангів, навіть й такі, які недостатньо обізнані в роботі комп'ютерної системи, але сприяють вчиненню комп'ютерного злочину (наприклад, передача сторонній особі кодів доступу до ресурсів комп'ютерної системи).

П'ята група — працівники, які згідно зі своєю посадою мають санкціонований доступ до приміщень з комп'ютерними системами та периферією і виконують на ЕОМ певні дії, що входять до їхніх обов'язків.

Отже, вважаємо, що зловмисник скоріше за все буде діяти в тій сфері фахової діяльності, в якій він найбільше обізнаний. Пропонуємо шукати підозрілих осіб серед тих, хто за родом фахової діяльності спроможний вчинити комп'ютерний злочин тим чи іншим способом.

Сьогодні із упевненістю можна сказати:

– сучасне розширення інформаційного простору створює нові можливості для організованої злочинності, яка рухається у структурному плані до домінування гнучких мереж і, відповідно, стає можливим використання Інтернет не тільки для правопорушень, але й для створення злочинних груп, що може втілитися в перехід існуючих груп хакерів і кракерів, які координують свої опе-

рації, до формування кримінальних організацій, членам яких не має потреби зустрічатися або знаходитися в одній державі, тобто відбувається поєднання організованої злочинної діяльності з суттєвими елементами неорганізованої злочинності — крупні правопорушення, що пов'язані з використанням комп'ютерних технологій чи проти цих технологій, вчиняються правопорушниками-одинаками;

– суб'єктивні дані особи, яка вчиняє злочин у сфері інформаційних технологій, її психічні та психологічні характеристики визначають спосіб кримінального впливу на інформаційні системи, інформацію та програмне забезпечення, як предмет злочинного посягання, в результаті послідовних у просторі та часі дій цієї особи;

– у комп'ютерну злочинність втягнуто широке коло осіб від висококваліфікованих фахівців до дилетантів.

Примітки

1. У Москві в травні 2000 року відбулася зустріч СПРИНГ-2К — другий зліт комп'ютерного андеграунду Росії та деяких інших прикордонних з нею країн. У програмі злъоту було заплановано демонстрацію хакерами і демогрупами, дослідниками «небезпечних комп'ютерних технологій» та звичайними програмістами-професіоналами мистецтва й тасмниць своєї майстерності. На СПРИНГу проводився очний етап Софтулійських ігор, демо-бліцтурнір, змагання по комп'ютерному мережевому злому технічного захисту інформації та злому комп'ютерних програм. Організатори СПРИНГу зробили заявку на демонстрування суспільству, що хакери — це не злочинці, якими їх малює «жовта преса», а розумні та інтелігентні люди і за їхнім переконанням людині із сильними етичними принципами можна довіряти будь-які небезпечні технології. (Див.: htt://sprryg.hackzone.ru; htt://www.hackzone.ru./forum). На нашу думку, це має значення, якими слід вважати хакерів — «поганими чи хорошими», є та грань закону, яка обов'язкова як для реального світу, так і для віртуального: технологічна зацікавленість, любов до програмування — це один бік медалі; інший, сумний, бік — це нехтування законами, правовий нігілізм і, як результат, злом комп'ютерних систем, викрадення грошових коштів, використання інформаційних технологій зі злочинною метою. «Странный характеръ, простая глупость, излишняя талантливость — все это относится к аномаліямъ — по съ какой стати человъкъ, находящійся въ подобномъ состояніи, не долженъ считаться отвътственнымъ за свои поступки», — писав у своїх роботах В. Х. Кандинський [8, 38].
2. Ще у 1979 році проблему обговорювали на 12-й Конференції директорів кримінологічних інститутів ряду європейських держав, де було відзначено, що проблема «білокомірцевої», або економічної злочинності, чи «злочинності у сфері бізнесу» є однією з найважливіших соціальних проблем.
3. Узагальнення проведено на підставі статистичних даних ДІТ МВС України, опрацьованих матеріалів слідчої та судової практики зарубіжних країн, науковців Ю. М. Батуріна, А. М. Жодзишського [13, 5].

Література

1. Ассев В. Г. Мотивации поведения и формирование личности. — М.: Мысль, 1976. — 158 с.
2. Игошев К. Е. Типология личности преступника и мотивация преступного поведения. — Горький, 1974. — 167 с.
3. Нюттен Ж. Мотивация // Экспериментальная психология. — М., 1975. — Вып. 5.
4. Криминалистическая мотивация / Ю. М. Антонян, В. В. Гульдман, Ю. Н. Кудрявцев и др.; Отв. ред. В. П. Кудрявцев; АН СССР. Ин-т госуд. и права. — М.: Наука, 1986. — 304 с.
5. Батурин Ю. М., Жодзишский А. М. Компьютерная преступность и компьютерная безопасность. — М.: Юрид. лит., 1991. — 160 с.
6. Сатерленд Э. Ч. Являются ли преступления людей в белых воротничках преступлениями? // Социология преступности (современные буржуазные теории) / Под ред. Б. С. Никифорова. — М., 1966. — С. 45–59.

7. Kriminalistik. — 1987. — № 5. — S. 265–267.
8. Кандинский В. Х. К вопросу о невменяемости. — М.: Изд-во Е. К. Кандинской, 1890. — 238 с.
9. Некоторые особенности современного кибертерроризма // Борьба с преступностью за рубежом (по материалам зарубежной печати). — М., 2001. — № 9. — С. 3–12.
10. Dalapro Reports on Information Security. — 1990–1993. — Vol. 1–3.
11. Жмыхов А. А. Особенности современной компьютерной преступности за рубежом // Преступное поведение (новые исследования): Сб. науч. тр. / Под общ. ред. Ю. М. Антоняна. — М., 2002.
12. Straub D. W., Widom C. S. Deviancy by bits and bytes: computer abusers and control measures // Computer Security: A Global Challenge. — Netherlands, 1984. — P. 431–441.
13. Батурин Ю. М. Проблемы компьютерного права. — М.: Юрид. лит., 1991. — 268 с.

УДК 343.982.32:343.985

С. П. Чумак

КРИМІНАЛІСТИЧНА ІДЕНТИФІКАЦІЯ У СЛІДЧІЙ ДІЯЛЬНОСТІ

Розкриття й розслідування злочинів тією чи іншою мірою пов'язане з ідентифікацією. Незважаючи на досить широке використання ідентифікації, серед учених-криміналістів дотепер не знайшли остаточного рішення деякі питання, що стосуються її поняття, змісту і значення.

Загальновідомо, що основоположником наукової теорії криміналістичної ідентифікації був видний криміналіст С. М. Потапов, що розглядав ідентифікацію як метод і спеціальну методологію криміналістики. Він вказував, що ідентифікувати можна всілякі матеріальні предмети і явища, їхні роди й види, кількості і якості, ділянки простору й моменти часу, людську особистість у цілому і її окремі ознаки, фізичні властивості людини і її розумові здатності, її зовнішні дії й внутрішні психічні акти [21, 4, 15].

Таке розуміння криміналістичної ідентифікації перетворює її у всеосяжний метод пізнання фактів, що підлягають доказуванню в розслідуванні й судовому розгляді справ. Безмежне поширення процесу криміналістичної ідентифікації на всі пізнавальні акти в судочинстві стикнулося із запереченнями ряду вчених. Так, Н. В. Терзієв, критикуючи погляд С. М. Потапова на криміналістичну ідентифікацію як на всеосяжний спеціальний метод криміналістичного дослідження, відзначав, що криміналістичну ідентифікацію не можна розглядати методом, вона є лише завданням дослідження об'єктів матеріального світу з метою встановлення їхньої тотожності по пам'яті, опису або відображенню, або з об'єктом, що залишив сліди або інші речові докази [26, 36–45]. Надалі Н. В. Терзієв вказував, що ідентифікація в криміналістиці відрізняється від ідентифікації в інших науках по цілях і об'єктах дослідження. До останніх він відносив індивідуально-визначені об'єкти, що служать судовими доказами [17, 37].

С. П. Мітричев, критикуючи позицію С. М. Потапова щодо ідентифікації як загального методу криміналістики, обмежував застосування криміналістичної