УДК 35.078:172.4:316.774

Б. В. ДЗЮНДЗЮК

ОСОБЛИВОСТІ СУБКУЛЬТУРИ КІБЕРЗЛОЧИНЦІВ

***Р**озглянуто основні характеристики кримінальної субкультури, вплив субкультури хакерів на розвиток кіберзлочинності. Визначено характерні ознаки субкультури кіберзлочинців.*

Ключові слова: кіберзлочинність, субкультура кіберзлочинців, субкультура хакерів.

***B**asic descriptions of criminal subculture, influence of subculture of hackers on development of cybercriminality are considered. The characteristic signs of subculture of cybercriminals are defined.*

Key words: cybercriminality, subculture of cybercriminals, subculture of hackers.

Існує значна різниця між субкультурами хакерів та кіберзлочинців, але не існує чіткого розмежування цих понять та ознак вищеназваних субкультур. У суспільстві через низьку поінформованість існує багато кліше стосовно зовнішнього вигляду хакерів, мотивів їх дій. Наслідки дій кіберзлочинців усвідомлюються не в повній мірі.

У ЗМІ висвітлюються лише гучні злочини, скоєні через інтернет або наслідки дій груп хакерів під час політичних виборів. Про "незначні" кіберзлочини, такі як крадіжка фінансової інформації, інтернет-шахрайство взагалі не повідомляється, а правоохоронні органи здебільшого не в силах допомогти жертвам цих злочинів. Люди стають жертвами кіберзлочинців через відсутність елементарної комп'ютерної грамотності та знання правил безпечної поведінки в мережі інтернет.

Ознаки субкультури злочинців і хакерів були висвітлені в роботах та дослідженнях багатьох учених, зокрема М. Денісова, К. Касперськи, І. Смірнової, В. Тулегенова. Однак не розглядались окремо субкультури хакерів і кіберзлочинців, не порівнювались ознаки субкультури кіберзлочинців та злочинців.

Мета статті – визначити характерні ознаки субкультури кіберзлочинців порівняно із субкультурою злочинців та вплив субкультури хакерів на розвиток кіберзлочинності, що допоможе вдосконалити методи боротьби із кіберзлочинністю.

Інтернет на сьогодні є не тільки принципово новим засобом масової комунікації – він охоплює практично всі сфери людської діяльності. Багато процесів успішно переносяться з фізичного світу у віртуальний світ, а сама глобальна мережа інтернет створює умови для формування віртуальних співтовариств, генерує мовні форми нового типу, стирає межі між державами, ігнорує відстані, об'єднуючи людей, і зрештою породжує специфічні форми культури.

При цьому можна стверджувати, що злочинна субкультура в інтернет ідеологічно і зовні дуже схожа на субкультуру хакерів і є її частиною. А, як відомо, субкультура хакерів була спочатку асоціальною, протиставляючи себе державі і суспільству. Тому для сучасного кіберзлочинця ідеал хакера – це не тільки спосіб отримання прибутку, але і виправдання своїх злочинів, а також отримання визнання і пошани у віртуальному просторі.

Деякі дослідники виділяють спільноту користувачів інтернет як своєрідну субкультуру, однією з основ якої є інформаційний лібералізм [7]. У такому випадку хакерів можна назвати "радикальним крилом" даної субкультури, оскільки заради свободи доступу до інформації вони готові до здійснення ряду злочинів.

Можна погодитися з М. Денісовим, який вважає, що субкультура – це сукупність норм і правил поведінки, традицій, звичаїв і зовнішньої атрибутики, які існують усередині певної соціальної мікрогрупи осіб, об'єднаних якимсь загальним інтересом (професійним або іншим); підтримуються всіма членами цієї групи і відрізняються від загальноприйнятих в суспільстві. Вона зазвичай визначається як система сумісних вірувань, відносин і символів, диференціюючих певну мікрогрупу в межах великого культурного співтовариства [2].

Виходячи з цього визначення, в даний час субкультуру хакерів можна вважати такою, що сформувалася. Вони мають специфічний стиль життя; властиві даній соціальній групі своєрідні норми, цінності, моделі поведінки і зовнішні характерні атрибути. При цьому в основі ідейної бази хакерів лежить лібералізація доступу до інформації. "Ми досліджуємо, і ви називаєте нас злочинцями. Ми у пошуках знань і ви називаєте нас злочинцями", – це уривок з відомого маніфесту хакерів (The Hacker Manifesto), написаного хакером під псевдонімом Mentor [9]. Ця теза підтримується більшістю мережевого співтовариства. Так, наприклад, навіть у Китаї, де традиції лібералізму не так поширені, як в інших країнах, можна спостерігати тенденцію до боротьби "жителів мережі" (netizens) за вільне освітлення важливих подій за допомогою Інтернет [10].

При цьому автори в підтримці свободи інформації не голослівні, часто їх гасла підкріплюються серйозними і продуманими аргументами, обґрунтованими філософськи, культурно і логічно. Наприклад, К. Касперські пише: "Ситуація дійшла до логічного абсурду, і в повітрі запахло бунтом. Бунтом проти тоталітаризму демократичного режиму, коли один пролазливий комерсант віднімає у людства те, що належить йому по праву. Інформація – загальнодоступний ресурс, такий же, як вода і повітря. Ми діти своєї культури. Наші думки і думки, які ми щиро вважаємо своїми, насправді вже давно є комбінацією вже давно придуманого і висловленого. Вдалі знахідки, яскраві ідеї – все це результат осмислення або переосмислення. Колись почутого або прочитаного" [4, с. 19].

Для хакера право на свободу інформації є більш очевидним і логічним, ніж патентні, авторські права, право державної таємниці. Тобто в рамках субкультури хакерів право на інформацію просто не діє внаслідок того, що "для функціонування

в рамках певної культури право зобов'язане бути визнано і виправдано як таке" [1], і що право повинне бути сумісне з етичними цінностями людини [5].

Можна виділити також і неприйняття ними споживчої культури. Про це свідчить "Біблія хакера" (cracking notes), написана хакером під псевдонімом "Orc+", яка пронизана ненавистю до існуючого суспільного ладу. Також важливі аспекти ідеології хакерів – це віра у здатність комп'ютера змінити життя до кращого і неприйняття яких-небудь авторитетів поза віртуальним простором і заперечення расових, релігійних, соціальних відмінностей.

Субкультура хакерів істотно відрізняється від інших кримінальних культур, але в той же час можна знайти і деяку схожість. Так, наприклад, В. Тулегенов виділяє декілька відмінностей кримінальних субкультур. Вони відрізняються швидкою мінливістю, оскільки злочинний світ завжди відрізнявся високою адаптивністю і умінням пристосовуватися до умов, що змінюються [8]. Це відноситься і до культури хакерів. У решті, мабуть, субкультура хакерів істотно відрізняється від "типової" кримінальної субкультури.

По-перше, В. Тулегенов стверджує, що кримінальні субкультури не залишають матеріальної спадщини, тобто не мають в своєму розпорядженні яких-небудь матеріальних носіїв, окрім самих злочинців, і передаються з вуст у вуста. У випадку з хакерами це не так.

По-друге, кримінальна субкультура – це закрита система, вона володіє своїми прихованими, найчастіше небезпечними настановами, що суперечать суспільним. Субкультура хакерів теж закрита система, але при цьому цінності хакерів мають добре опрацьовану філософську основу і це додає якусь легітимність ідеям хакерів.

По-третє, практично в усіх кримінальних субкультурах використовуються псевдоніми, псевдоімена, прізвиська. У середовищі хакерів їх називають "ніками" (nick, nickname). Проте псевдоімена прийняті не тільки в злочинній інтернет-субкультурі, але і в усьому інтернет-співтоваристві, причому на відміну від псевдоімен в кримінальному середовищі – "прозвисьок", "нік" кожен вибирає собі сам. Як і в інших кримінальних субкультурах, в "ніках" можуть бути відображені: характерологічні особливості і особливості поведінки; трансформовані прізвища і імена; статус в групі; особливості зовнішності або соціального статусу; переваги, які віддаються в музиці, літературі, мистецтві; специфіка злочинної діяльності і місця здійснення. Але при цьому в середовищі хакерів не зустрічаються прізвиська, аналогічні тюремним або загальнокримінальним, а також такі, які принижують гідність або висміюють недоліки.

По-четверте, як і в усіх субкультурах, у злочинної субкультури хакерів існує свій жаргон. Проте, на відміну від загальнокримінального жаргону, який є похідним від національної мови, сучасна мова хакерів незалежно від країни проживання наповнена англомовними словами, причому часто мова хакерів

недоступна звичайним користувачам, хоча багато слів використовуються і в некримінальному середовищі комп'ютерних професіоналів.

По-п'яте, якщо говорити про решту зовнішніх атрибутів культури хакерів, то необхідно згадати, що на відміну від інших злочинних субкультур, хакери мають власні періодичні видання, художню літературу, кінофільми, відеоролики, постери. Інші категорії злочинців задовольняються тільки спеціалізованими інтернет-сайтами; наприклад, існують інтернет-портали, орієнтовані, на наркозлочинців. Причому значення літератури і кіно для хакерів не варто недооцінювати. Звичайно, для професійних хакерів більшість сюжетів можуть показатися смішними і далекими від реальності, але для основної маси (особливо для підлітків) витвори хакерського мистецтва формують ідеал, до якого треба прагнути, в легкій і доступній формі формують в особистості цінності хакерів, демонструють моделі поведінки, а сам образ хакера при цьому сильно романтизований і тому привабливий.

Відмічене вище свідчить про те, що хоча загальнокримінальна субкультура і культура хакерів мають деяку схожість, але все-таки вони достатньо далекі один від одного. З даним фактом згодні і деякі ідеологи руху хакерів. Так, К. Касперськи, автор книг "Техніка і філософія хакерських атак", "Техніка налагодження програм без початкового коду" і так далі, описує хакерів таким чином: "Існує думка про існування деяких ознак приналежності до хакерів. Це довге (нечесане) волосся, пиво, сигарети, піца в необмежених кількостях і блукаючий в просторі погляд… подібні ознаки є не причиною, а наслідком. Прив'язаність до комп'ютера примушує більш економно відноситися до вільного часу, іноді харчуватись уривками і на ходу. Довге волосся? Так, воно властиве всім комп'ютерникам (і не тільки ним), а зовсім не виключно хакерам, як, до речі, і всі інші ознаки хакерів" [3, с. 65].

Проте це та інші подібні думки не можуть затьмарити той факт, що сучасна субкультура хакерів все ж таки має кримінальну основу, оскільки її можна визначити як сукупність ідей, цінностей, звичаїв, традицій, норм поведінки, направлених на організацію способу життя, метою якого є вчинення комп'ютерних злочинів, їх приховування і ухилення від відповідальності. При цьому ціннісний комплекс даної субкультури служить для легітимації і популяризації ідеї хакерства в суспільстві, саме тому людина, яка розділяє цінності хакери:ів, готова піти на інтернет-злочин, або схвалює злочини, що здійснюються іншими.

Слід зазначити, що субкультура хакерів не була б така важлива для розвитку кіберзлочинності, якби вона не виконувала ряд важливих функцій. У даний час існує низка кримінологічних і соціологічних досліджень [2; 6; 8], що виділяють функції негативних і злочинних субкультур. Найбільш значущими з них для кіберзлочинності є наступні:

1. Об'єднуюча. Той факт, що хакери по всьому світу мають схожі ідеологічні настанови, погляди на життя, способи заробітку, використовують одну і ту ж літературу, терміни і сленг, є серйозним об'єднуючим чинником, завдяки якому

хакери можуть легко об'єднуватися в міжнародні групи для здійснення суспільно небезпечних діянь, обмінюватися професійною інформацією і злочинними інструментами.

2. Легітимаційна. Виправдання в очах оточуючих і відповідність злочинів в інтернеті своїм морально-етичним настановам дають додатковий стимул для вибору кримінального шляху при досягненні мети. Відсутність явного суспільного засудження за подібну протиправну поведінку приводить до ситуації, коли кіберзлочинці не тільки не ховаються, але і виставляють напоказ свої незаконні досягнення, не боячись відповідальності, залишають фірмові знаки або гасла груп хакерів на місцях злочинів (які вони по іронії часто називають "копірайтами" [3]). Окрім цього, як уже вище сказано, самі хакери не вважають свою діяльність злочинною, що створює їм романтичний образ.

3. Інформаційна. Саме в рамках субкультури розповсюджується ідеологічна і інструментальна інформація. У середовищі хакерів передаються нові способи і сучасні засоби здійснення кіберзлочинів. За допомогою своєї субкультури хакери дізнаються, як утекти від правоохоронних органів і як знищити докази, які методи добування грошей злочинним шляхом найбільш безпечні і які засоби найбільш ефективні. Завдяки поширюваній у середовищі хакерів інформації кіберзлочинці часто мають технічну перевагу перед приватними службами безпеки і державними службами протидії кіберзлочинності.

4. Криміногенна. Ця функція виражається в накопиченні, збереженні і передачі традицій злочинного інтернет-середовища, яке здатне протистояти соціальним інститутам, тобто в забезпеченні відтворення і розповсюдження кіберзлочинності.

Таким чином, як можна побачити, субкультура хакерів є одним з головних криміногенних чинників кіберзлочинності, тому нейтралізація негативних наслідків впливу цієї субкультури є найважливішим напрямом боротьби з кіберзлочинністю взагалі і з першим і третім видами кібертероризму зокрема. Даний напрям повинен включати ідеологічні, пропагандистські заходи профілактики, направлені, з одного боку, на усунення в певних групах і у певних індивідів (комп'ютерні фахівці, студенти технічних вузів і тому подібне) антигромадських установок. При цьому пропаганда не повинна обмежуватися констатацією, що так робити не можна і це заборонено законом, а мати під собою серйозну філософсько-ідеологічну базу, що протистоїть субкультурі хакерк:ів.

З іншого боку, слід проводити заходи, що направлені на широку громадськість, дозволяють сформувати негативне суспільне відношення до кіберзлочинців і їх дій. На жаль, певна ідеалізація в суспільній свідомості протиправної діяльності хакерів заважає боротьбі з кіберзлочинністю і створює додаткові стимули для здійснення злочинних дій в кіберпросторі. Тому необхідно поширювати в суспільстві настанову про те, що хакери – це не сучасні Робін Гуди і не "борці за свободу", а злочинці, необхідно широко освітлювати негативні наслідки їх діяльності для окремих індивідів, суспільства і держави. У цьому можуть

допомогти засоби соціальної реклами в різних медіа, в рамках проведення широкомасштабних кампаній, наприклад, під гаслом "Ні кіберзлочинності!" або "Ти хакер? Ти – невдаха!".

У сукупності це дозволило б через якийсь час контролювати формування і розвиток певних груп населення, особливо підлітків і молоді, схильних до злочинної поведінки; привело б до зниження в їх середовищі антигромадських настроїв, поглядів, цінностей, що, врешті-решт, зменшило б базу для кіберзлочинності і кібертероризму.

Розмежування "звичайних" злочинців та кіберзлочинців не повинно стати приводом до зниження відповідальності останніх перед суспільством.

Незважаючи на мотиви хакерів та їх філософську базу, хакерська діяльність повинна попереджатися та повністю не прийматись суспільством через свій криміногенний характер. Запобіжним заходом може стати розповсюдження контр-філософії хакерів.

Формування актуального образу хакерів у суспільній свідомості та висвітлення дій кіберзлочинців у ЗМІ нарівні із діями "звичайних" злодіїв повинно стати одними із задач внутрішньої державної політики. Постійно повинна проводитись інформаційна кампанія по методам захисту своєї власності в кіберпросторі серед усіх прошарків суспільства. Молодь потрібна бути проінформована не лише про наслідки кіберзлочинів, а й про наслідки участі в подібних антисоціальних діях.

Не завжди населення може захиститись від кіберзлочинців і коли трапляється лихо, правоохоронні органи повинні бути готовими до ліквідації його наслідків. На жаль, в Україні відсутні відпрацьовані механізми з боротьби із кіберзлочинцями та наслідками їх дій, тому багато хто із жертв злочинів, скоєних у Всесвітній мережі, вважає за краще не звертатись до правоохоронних органів.

Література:

1. *Данильян О. Г.* Философия права : учебник / О. Г. Данильян, Л. Д. Байрачная, С. И. Максимов и др. ; под. ред. О. Г. Данильяна. – М. : Эксмо, 2006. – 288 с.

2. *Денисов Н. Л.* Влияние криминальной субкультуры на становление личности несовершеннолетнего преступника : дис. … к.ю.н. : спец. 12.00.08. / Н. Л. Денисов. – М., 2002. – 165 с.

3. *Касперски К.* Техника и философия хакерских атак – записки мыщ'а / К. Касперски. – М. : СОЛОН-Пресс, 2004. – 325 с.

4. *Касперски К.* Техника отладки программ без исходных текстов / К. Касперски. – СПб. : БХВ-Петербург, 2005. – 278 с.

5. *Нерсесянц В. С.* Философия права : Учебник для вузов / В. С. Нерсесянц. – М. : НОРМА, 2004. – 621 с.

6. *Павлова А. А.* Субкультура теневой экономической деятельности: сущность и факторы воспроизводства в России : дис. … к.соц.н. : спец. 22.00.03. / А. А. Павлова. – М., 2004. – 179 с.

7. *Смирнова И. А.* Виртуальное пространство культуры: Материалы научной конференции 11–13 апреля 2000 г. – СПб. : Санкт-Петербургское философское общество, 2000. – С. 148–149.

8. *Тулегенов В. В.* Криминальная субкультура и ее криминологическое значение : дис. … к.ю.н. : спец. 12.00.08 / В. В. Тулегенов. – Ростов-н/Д., 2003. – 194 с.

9. Hacker Manifesto, Written on January 8, 1986 [Електронний ресурс]. – Режим доступу : http://project.cyberpunk.ru/idb/hacker_manifesto.html

10. *Xiao Qiang*. Cniha's Virtual Revolution // Project Syndicate [Електронний ресурс]. – Режим доступу : http://www.project-syndicate.org/commentaries/commentary_text.php4?

Надійшла до редколегії 27.05.2013 р.