УДК 343.919:343.533

С. Л. Ємельянов

ДЕЯКІ АСПЕКТИ КРИМІНАЛІСТИЧНОЇ ХАРАКТЕРИСТИКИ СУЧАСНИХ КОМП'ЮТЕРНИХ ЗЛОЧИНЦІВ

Згідно з прогнозами XXI сторіччя стане століттям глобальної інформатизації і комп'ютеризації усього світу і переходом людства до нового інформаційного суспільства, у якому вирішальна роль приділяється інформації, інформаційним системам (ІС), інформаційним ресурсам (ІР) і інформаційно-телекомунікаційним технологіям (ІТТ).

Виходячи зі стратегічного курсу України на інтеграцію у світовий інформаційний простір, виникає об'єктивна потреба в аналізі не тільки позитивних, але і негативних явищ, що супроводжують широкомасштабне впровадження ІС та ІТТ.

Такими є об'єктивний ріст комп'ютерної злочинності (КЗ), розвиток хакерського руху, постійне удосконалювання технологій, способів і засобів здійснення злочинів в інформаційній сфері, збільшення економічного збитку від них і інші, що й обумовлює актуальність розглянутої теми.

Останнім часом з'явилася велика кількість досліджень і публікацій, що торкаються різних аспектів комп'ютерної злочинності [1–7]. Як одну з базових класифікуючих ознак при дослідженні криміналістичних аспектів КЗ багато авторів розглядають мету і сферу (вид) протиправної діяльності [2; 6; 8; 9]. Однак кількість виділених і досліджених за цією ознакою гомогенних груп, на наш погляд, є недостатньою і відстає від сучасного розвитку ІТТ.

Уявляється, що по меті і сфері протиправної діяльності сьогодні вже можна виділити такі групи суб'єктів КЗ (рис. 1).

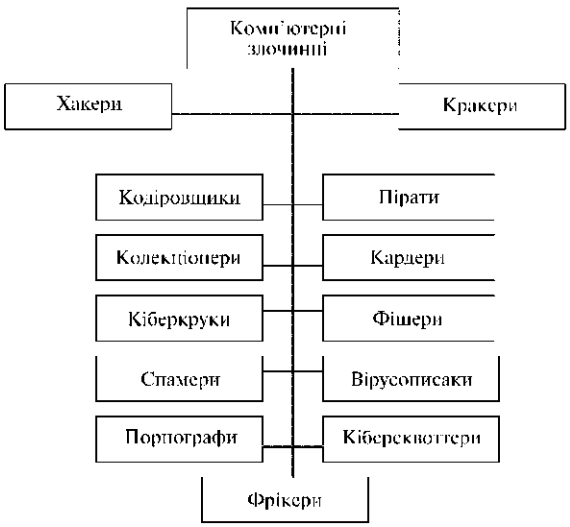

Рис. 1

Слід зазначити, що серед фахівців дотепер відсутнє єдине тлумачення терміна «хакер». Спочатку під хакером (hacker) розумівся високопрофесійний програміст, здатний розробляти і модернізувати комп'ютерні програми, не маючи детальних специфікацій і документації до них. Таке трактування було пануючим на рубежі 70—80-х років минулого сторіччя, коли зародився і розвився світовий хакерський рух.

Пізніше, з ростом масштабів КЗ і перетворення їх в самостійний вид злочинності, цей термін придбав кримінальний відтінок і став означати комп'ютерного зломщика, здатного незаконним способом одержати доступ у ІС чи до захищених ІР.

Однак більшість авторів небезпідставно вважають, що для останньої зазначеної категорії суб'єктів протиправної діяльності більш доцільним є використання терміна «кракер» (cracker) [8–10]. Головна відмінність між зазначеними категоріями полягає, на наш погляд, не у віці чи рівні майстерності (новачок, професіонал, суперпрофесіонал), а в характері впливу на інформацію й у цільовій настанові. Суб'єкти обох зазначених категорій шукають і аналізують уразливі місця («діри», «люки» і т.д.) в апаратно-програмному забезпеченні ІС і здійснюють злом комп'ютерних систем і мереж (КСМ). Хакеры, наприклад, часто мають дослідницькі цілі, не роблять шкідливого впливу на інформацію і повідомляють про результати своїх атак. Напроти, кракеры здійснюють злом КСМ із метою одержання несанкціонованого доступу до чужої інформації, характер впливу на який є набагато більш небезпечним (рис. 2) залежно від їхніх мотивів (рис. 3).

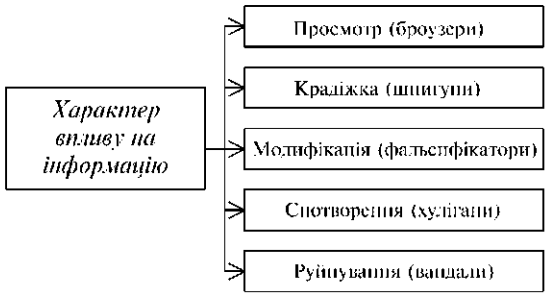

Рис. 2

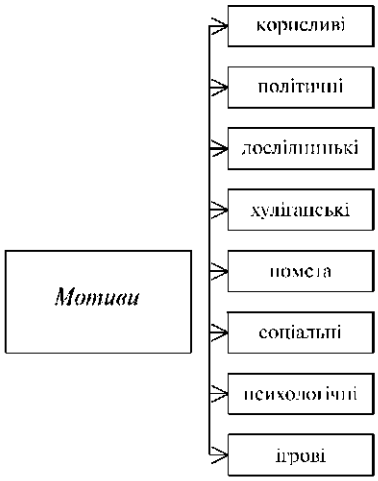

Рис. 3

Статистичне співвідношення різного роду мотивів при здійсненні комп'ютерних злочинів за експертними оцінками становить [7–9]:

– корисливі мотиви — 60—70 %;

– політичні мотиви (тероризм, шпигунство, дисидентство і т.д.) — 15—20 %;

– дослідницький інтерес (любопитство) — 5—7 %;
– хуліганські спонукання і бешкетництво — 8—10 %;
– помста — 4 %.

Інші мотиви здійснення КЗ (виділені на рис. 3) є відносно новими і менш дослідженими.

Так, наприклад, виник термін «хактивізм» із з'єднання двох слів «Hack» і «Activism», що пропонується використовувати для позначення нового явища соціального протесту, який являє собою своєрідний синтез соціальної активності, що переслідує ціль протесту проти чого-небудь, і хакерсьтва. В даний час закордонні аналітики відзначають, що в умовах, коли спостерігається, з одного боку, політизація хакерів, а з іншого — комп'ютеризація і прилучення до Інтернету активістів рухів соціального протесту, зростає число «кіберактивистів», що прагнуть перенести в кіберпростір рух цивільної непокори у формі «електронного протесту» [11].

Психологічні мотиви мають суб'єкти, що страждають новим видом психічних захворюваннь — інформаційно-комп'ютерними фобіями. Цей вид захворювань пов'язаний з порушенням внутрішнього інформаційного балансу людини чи його темпоритму і вивчається в рамках інформаційної психіатрії. З ростом комп'ютеризації суспільства спостерігається й об'єктивний ріст числа таких мотивів [1]. Юристи навіть пропонують внести доповнення в звітність служби у справах неповнолітніх — спеціальну графу для реєстрації дітей з комп'ютерною залежністю [12].

Частка ігрових мотивів також постійно зростає. Всупая в інтелектуальне протиборство з механізмами безпеки КСМ, подібні суб'єкти сприймають свої дії не як протиправні, а як одержання гострих відчуттів чи розвагу [4–6].

Кодіровщики (coders) здійснюють злом програмних продуктів, усуваючи чи обходячи в них програмні механізми захисту. «Трасують» (розкладають) тексти програм, використовуючи для цього мови високого рівня, у тому числі на машинних кодах. «Роздягнені» програми передають (продають) потім, наприклад, комп'ютерним піратам чи колекціонерам. Типовий «крек» — обхід введення реєстраційного чи серійного номеру ліцензійної програми при її інсталяції на ПК.

Комп'ютерні пірати (wares dudes) спеціалізуються на незаконному (без згоди правоволодаря) копіюванні ліцензійних програмних продуктів і їхньому поширенні з метою одержання матеріальної вигоди. Завдають багатомільйонну шкоду розроблювачам програмних продуктів і виявляються в різних формах: «чорного» і «білого» копіювання, завантаження жорстких дисків ПК при їхньому продажі, перекачуванні через Інтернет і ін. [1; 2; 13]. Слід зазначити, що в 2007 р. завдяки успіхам, насамперед, у нормотворчій, правозастосувальній і профілактичній діяльності державних структур з України знято статус пріоритетної країни-порушника авторських прав, і тепер вона прирівняна до країн, за якими ведеться спостереження (рівень піратства менш 90 %) [17].

Колекціонери (codes kids) колекціонують, використовують і обмінюються захищеними комп'ютерними програмними продуктами, що мають коди досту-

пу, паролі й інші вбудовані програмні засоби захисту, а також кодами телефонного виклику і номерами телефонних компаній, що мають вихід до комп'ютерних мереж загального користування, наприклад Інтернет.

Кардери (card) — спеціалізуються на махінаціях із пластиковими картками, сплачуючи свої витрати з чужих кредитних карток. Типова процедура кардинга полягає в копіюванні інформації, що міститься на магнітній смузі кредитної картки (дамп) і виробництві фальшивої картки — «фантома» з нанесенням на неї скопійованого дампа або одержанням індивідуального Pin-кода від власника реальної карти, наприклад методами соціальної інженерії.

Кіберкруки (cybercrooks) — спеціалізуються на несанкціонованому проникненні в КСМ фінансово-банківських установ і закриті КСМ державних силових структур і органів. Використовують КСМ для крадіжки коштів, одержання цінної фінансової інформації. Популярним товаром є кредитна інформація, інформаційні бази даних правоохоронних органів і інших державних і комерційних структур.

Фішинг (phishing — з англ. — рибний лов) — відносно новий вид мережного шахрайства. Його метою є заволодіння оманним шляхом персональними даними клієнтів онлайнових аукціонів, інтернет-магазинів, сервисів грошових переказів і іншою конфіденційною інформацією. Причому бурхливий розвиток Інтернету, мережної комерції і банкінгу обумовлюють перетворення фішинга в один з найпоширеніших видів комп'ютерного шахрайства [14]. Сьогодні вже можна виділити три популярних види фішинга: поштовий, онлайновий і комбінований (фармінг). В останньому випадку змінюється адреса DNS (Domain Name System) таким чином, щоб користувач взаємодіяв з помилковим (фальшивим) сервером-постачальником послуг (товарів).

Спамери (spam, spiced ham — досл. з англ. «шинка зі спеціями») займаються масовим (більш ніж 5 адресатам) розсиланням незапрошених (часто анонімних) оголошень засобами електронних комунікацій, насамперед електронною поштою. За даними [17], частка спама в 2006 р. становила не менш 70 % від загального поштового трафіку і має постійну тенденцію зростання.

Вірусописаки (Virus Writers, вірмейкери) здійснюють протиправне ушкодження КСМ із метою порушення їх функціонування за допомогою програмних (комп'ютерних чи мережних) вірусів. Перші віруси, досить примітивні, з'явилися в 1987 р., і з цього часу їхня кількість росте по експоненті, досягши в 2007 р. кілька десятків тисяч видів [16]. За даними [17], за 2004 р. найбільша кількість заражень викликали мережні хробаки (77,19 %) — шкідливі програми, що мають функції поширення по Інтернет (електронна пошта, Web-сервіси, мережні пейджери, IRC-канали й ін.). На другому місці виявилися комп'ютерні віруси (16,33 %), в основному макровіруси. І на третьому — троянські програми (6,49 %).

Порнографи використовують можливості WWW для платного поширення матеріалів порнографічного характеру, що вчені називають «кокаїном для нового покоління». Більш 75 % усієї дитячої порнографії поширюється в Інтернеті, де, за деякими оцінками, нараховується майже 40 тисяч порносайтів. Мо-

ніторинг українських Інтернет-сайтів показав, що на них міститься приблизно 20 % забороненої порнопродукції, у тому числі і дитяча порнографія. Число користувачів дитячого порно становить, по оцінних данних, 30–40 тисяч чоловік. Педофіли засновують гуртки дитячої порнографії, колекціонують фільми, фотографії, зображення дітей, поєднуються в клуби й обмінюються порнографічною продукцією [18; 19]. Основним об'єктом уваги провоохоронних структур є виготовлювачі матеріалів сексуального характеру за участю дітей,на другому місці — колекціонери таких матеріалів. За даними Управління «К» МВС Росії, близько 92 % міжнародних пошукових доручень Інтерполу по комп'ютерній злочинності присвячені саме цій проблемі [18].

Кіберсквоттінг (cybersquatting) — захоплення доменних імен з метою наживи. Доменні імена найчастіше називають «нерухомістю» онлайнового століття. Добре підібране ім'я може саме по собі забезпечувати досить сильний потік відвідувачів, як наслідок, і потенційних клієнтів: удала назва інтуїтивно знаходиться і легко запам'ятовується. Усвідомлення цінності доменів постійно росте, а слідом росте і їхня ціна. У кіберсквоттінгу також є свої види:

• явне захоплення імен, ідентичних торговим маркам (наприклад, Yandex.com, Kodak.ru);

• регістрація імен, схожих за написанням на імена «розкручених» сайтів-тайпсквоттінг. Пов'язан з тими випадками, коли реєструються імена, що асоціюються в розумах користувачів Мережі з відомими компаніями чи особистостями;

• реєстрація імен «по словнику» — «столбляться» слова, що можуть служити ім'ям, пов'язаним з тематичним змістом сайту. Відсудити такий домен практично неможливо — ці слова, як правило, є загальновживаними.

Фрікери (phreak=phone+break) спеціалізуються на використанні телефонних систем, зломі цифрових АТС телефонних компаній, несанкціонованому одержанні кодів доступу до платних послуг ISDN, крадіжці і підробці телефонних карток і т.д. з метою уникнути оплати за надання послуг у сфері ІТТ. У своїй діяльності використовують не тільки програмне забезпечення, але і спеціальну апаратуру, що генерує імпульсні чи тональні сигнали виклику телефонних систем. Фрікінг є одним з найстаріших видів протиправної діяльності у сфері високих технологій.

На закінчення необхідно відзначити, що з правової точки зору відносити хакерів, кракерів, фрікерів, кардерів і інших суб'єктів з вищерозглянутих категорій до комп'ютерних злочинців може тільки суд. Однак запропонована класифікація комп'ютерних злочинців по меті і сфері протиправної діяльності є, на наш погляд, найбільш повною по зазначеній класифікуючій ознаці і може бути використана для продовження роботи зі створення криміналістичної характеристики злочинності у сфері використання КСМ.

Література

1. Комп'ютерна злочинність : навч. посіб. / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк [та ін.]. — К. : Атіка, 2002.

2. Вехов В. Б. Компьютерные преступления. — М., 1996.
3. Біленчук П. Д. Комп'ютерні злочини / П. Д. Біленчук, О. В. Зубань. — К., 1994.
4. Вехов В. Б. Расследование компьютерных преступлений в странах СНГ : монография / В. Б. Вехов, В. А. Голубев ; под ред. засл. деятеля науки РФ, д-ра юрид. наук, проф. Б. П. Смагоринского. — Волгоград : ВА МВД России, 2004.
5. Голубев В. А. Информационная безопасность: проблемы борьбы с киберпреступлениями : монография. — Запорожье : ГУ «ЗИГМУ», 2003.
6. Голубев В. А. Проблемы борьбы с преступлениями в сфере использования компьютерных технологий : учеб. пособие / В. А. Голубев, В. Д. Гавловский, В. С. Цимбалюк ; под общ. ред. д-ра юрид. наук, проф. Р. А. Калюжного. — Запорожье : ГУ «ЗИГМУ», 2002. — http://www.crime-research.ru/library/book13.html.
7. Осипенко А. Л. Борьба с преступностью в глобальных компьютерных сетях : международный опыт : монография. — М. :Норма, 2004.
8. Голубев В. Хакеры или кракеры, а кто это?//www.crime-research.org.
9. Голубев В. А. Криминалистическая характеристика субъектов преступной деятельности в сфере использования компьютерных технологий // www.crime-research.ru/library.
10. Сабадаш В. Компьютерная преступность: криминологический обзор //www. crime-research.ru, от 13.10.2006.
11. Деннинг Д. «Activism, hacktivism and cyberterrorism» (перевод) //www.kiev-security.org.ua.
12. Ахтырская И. Проблемы юридической психологии лиц, совершающих преступления в сфере информационных технологий // www. crime-research.org.
13. Емельянов С. Л. Некоторые аспекты компьютерного пиратства и борьбы с ним / С. Л. Емельянов, И. А. Яковлев // Бизнес и безопасность. — 2005. — № 5. — С. 17–20.
14. Сабадаш В. Компьютерная преступность-фишинг, как самый распространенный вид мошенничества //www. crime-research.ru, от 25.01.2006.
15. Некоторые аспекты компьютерной преступности и борьбы с нею / С. Л. Емельянов [и др.] // Бизнес и безопасность. — 2006. — № 3. — С.143–145.
16. Емельянов С. Л. Принципы построения комплексной системы антивирусной защиты / С. Л. Емельянов, И. А. Яковлев // Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : наук.-техн. зб. — К., 2004. — Вип. 8. — С. 124–129.
17. Центр исследования проблем компьютерной преступности. — http://www.crime-research.org.ua.
18. Шраго А. Проблема WEB-порнографії та шляхи її подолання //www.crime-research.ru.
19. Голубев В. Компьютерная преступность — проблемы борьбы с Интернет-педофилией и детской порнографией //www.crime-research.ru.
20. Катаев С. Причины вирмейкинга: социологический анализ //www.crime-research.ru.

Анотація

У роботі проведено аналіз сучасної діяльності кіберзлочинців. Наведено їх класифікацію залежно від предметно-рольової діяльності, яка може бути використаною при розслідуванні злочинів.

Ключові слова: кіберзлочинці, розслідування.

Summary

Wide classification of computer criminals depending on their activity's type is given in this article. The author makes efforts for more sofisticated investigation of computer crimes.

Keywords: investigation, cyber criminals.