ISSN 1995-6134

УДК 343.102
О.В. БОЙЧЕНКО, канд. техн. наук, доц., Кримський юридичний інститут Одеського державного університету внутрішніх справ
М.М. НОВІКОВ, Кримський юридичний інститут Одеського державного університету внутрішніх справ

ОСОБЛИВОСТІ ОПЕРАТИВНО-РОЗШУКОВОЇ ПРОТИДІЇ КОМП'ЮТЕРНІЙ ЗЛОЧИННОСТІ

Ключові слова: *інформаційні технології, комп'ютерні злочини, інформаційна злочинність*

З розвитком науково-технічного прогресу забезпечується все більше зростання застосування комп'ютерних технологій в усіх напрямах життєдіяльності суспільства. Поряд із зазначеним все більш нагальною стає потреба в захисті інформаційних даних, які циркулюють у складі інформаційно-телекомунікаційних систем, від несанкціонованого доступу. Це визначено зростанням кількості злочинів у сфері інтелектуальної власності та інформаційних технологій. Визначена обставина вимагає проведення першочергових дій правоохоронними органами щодо розкриття на високому професійному рівні комп'ютерних злочинів [1, 2].

Дослідженню окремих проблем розслідування злочинів у сфері використання комп'ютерних технологій приділялася увага в роботах таких видатних фахівців, як Г.Ю. Маклаков, Е.В. Рижков, С.А. Роганов та інших [3-6].

Але зростання обсягів застосування комп'ютерних технологій на сучасному етапі розвитку суспільства разом із вирішенням проблем оперативно-розшукової протидії комп'ютерній злочинності, потребує проведення подальших наукових досліджень. Метою роботи є комплексне дослідження проблем, пов'язаних з використанням інформаційних технологій оперативними підрозділами ОВС щодо протидії комп'ютерній злочинності та розробка пропозицій для їх вирішення. Наукова новизна статті полягає в формуванні шляхів до визначення якісно нового рівня боротьби зі злочинними діяннями в сфері інформаційних технологій через розуміння психологічних особливостей осіб, схильних до вчинення комп'ютерних злочинів.

Враховуючи невідкладність вирішення завдань щодо протидії злочинам у сфері інформаційних технологій, оперативно-розшукова діяльність, на наш погляд, повинна базуватися на додаткових спеціальних принципах:

- широке застосування сучасних досягнень для розбудови стратегії і тактики ОРД в сфері інформаційних технологій;
- залучення висококваліфікованих фахівців на етапі розробки стратегії і тактики ОРД в сфері високих технологій;
- поповнення сучасними програмно-апаратними засобами арсеналу оперативної техніки;
- організація підготовки особового складу оперативних підрозділів по застосуванню інформаційних систем.

У наш час у діяльності підрозділів органів внутрішніх справ може використовуватися як універсальне, так і спеціальне програмне забезпечення.

Універсальні програми (інформаційно-пошукові системи, редактори, електронні таблиці та ін.) загального призначення не лише підвищують продуктивність праці і ефективність роботи по виявленню, розкриттю і розслідуванню злочинів, але й піднімають її на якісно новий рівень. Спеціалізовані програми можуть бути орієнтовані на безпосереднє застосування при здійсненні оперативно-розшукових заходів щодо боротьби з інформаційною злочинністю.

Сьогодні для протидії комп'ютерній злочинності оперативні підрозділи мають на озброєнні сучасне програмне забезпечення, яке дозволяє контролювати процес спроб злому комп'ютерної системи; визначати індивідуальний почерк роботи програміста і ідентифікаційних характеристик розробле-

ISSN 1995-6134

них ним програм; визначати перелік електронних адрес і сайтів Інтернету, з якими працював користувач; негласно реєструвати перелік програм, з якими працює користувач; визначати шлях, а в деяких випадках і конкретну адресу загрози для комп'ютерних систем; здійснювати негласний контроль над програмістом, визначаючи характер продуктів, що розробляються; виявити латентну і закодовану інформацію в комп'ютерній системі; проводити ідентифікацію комп'ютерних систем за слідами використання на різних матеріальних носіях інформації; здійснювати дослідження слідів діяльності оператора в цілях його ідентифікації; здійснювати діагностику пристроїв і систем телекомунікацій на можливість здійснення несанкціонованого доступу до них; досліджувати матеріальні носії з метою пошуку заданої інформації; здійснювати дослідження комп'ютерних технологій для встановлення можливості вирішення конкретних злочинних завдань (крекінг, хакінг, фрикінг і т. ін.); досліджувати програми і бази даних для визначення їх можливого призначення для злочинних дій (наявність програмних закладок, підпрограм класу «троянський кінь» та ін.).

Такі пошукові програмні засоби можуть знайти широке застосування в оперативно-розшуковій діяльності (не процесуальна форма), а також до порушення кримінальної справи щодо фактів виявлення об'єктів (програм закладок, програмного забезпечення для виготовлення вірусів або для здійснення злому комп'ютерних мереж тощо). Це може у майбутньому служити підставою для збудження кримінальної справи та провадження розслідування.

Одним із напрямів оперативно-розшукової діяльності щодо протидії комп'ютерній злочинності доцільно застосовувати кримінологічне прогнозування індивідуальної та групової злочинної поведінки фігурантів.

Так, певну інформацію можна одержувати аналізуючи мережевий трафік локальних і регіональних комп'ютерних мереж. Корисну інформацію можуть дати й аналіз платежів клієнтів за телефонні послуги. Прогнозування може успішно здійснюватися в основі первинних матеріалів оперативного обліку, оскільки банки інформації створюються на основі прогнозу вірогідності злочинної поведінки певних криміногенних контингентів. Саме аналіз їх установчих даних (судимість; правопорушення, антигромадські вчинки, досягнення у сфері програмування), дають підстави для прогностичних висновків про вірогідну протиправну поведінку в майбутньому. Крім того, беруться до уваги соціальні оцінки особи, яка представляє оперативний інтерес, а також її авторитет у криміногенному середовищі.

Суттєвою складовою інформаційних злочинів є мотивація поведінки. Злочинні мотиви є по суті модифікацією звичайних людських мотивів, але направлені на цілі, заборонені законом або пов'язані з використанням протиправних засобів. Тому для здійснення ОРД в сфері інформаційних технологій певний інтерес представляють соціологічні та психологічні дослідження молоді, яка навчається комп'ютерним наукам.

Для профілактичної діяльності по запобіганню комп'ютерним злочинам важливо проводити вивчення мотивів вчинків людини. Особливий інтерес представляє визначення рівня ціннісно-орієнтаційної єдності в молодіжній аудиторії, за яким можна визначити чинники, що впливають на поведінку людини в групах і спрогнозувати його прагнення до протиправних дій [3].

При виявленні та розкритті злочинів, здійснених з використанням обчислювальних систем або іншої електронної техніки, оперативний співробітник стикається з нетрадиційними слідами злочинної діяльності або речовими доказами. Тому для грамотного використання фактичних даних, отриманих в ході здійснення оперативно-розшукових заходів щодо таких злочинів, базової юридичної підготовки може бути недостатньо.

Для успішного здійснення ОРД співробітникам необхідні добрі знання психології хакера, знати тактику проведення ним атак на

ISSN 1995-6134

комп'ютерні системи, рівень його знань і можливість їх поповнення.

Важливою обставиною, врахування якої є необхідним для підвищення ефективності оперативно-розшукової протидії комп'ютерній злочинності, являється проведення оперативними підрозділами заходів щодо запобігання так званій «інформаційній наркоманії» («internet-addiction», «pathological internet use»). Поширення «інформаційних» наркотиків за допомогою Інтернет є діями, за які може бути порушена кримінальна справа за відповідними статтями Кримінального кодексу. Проблемою є те, що більшість співробітників правоохоронних органів навіть не знають про можливості деструктивної інформації. А ряд сект (наприклад «Біле Братство») уміло користуються можливостями сучасних інформаційних технологій впливати на свідомість і підсвідомість людини [4].

Проблема інтернет-наркоманії стала реальністю. Інтернет-наркоманія подібно до хронічного алкоголізму або азартної гри має руйнівні наслідки на людину, його сім'ю, роботу, навчання, а в деяких випадках провокує на злочин. На думку професора Пітсбургського університету Кимберлі Янг, проблема інтернет-наркоманії в США досягла епідемічних розмірів, причому число наркоманів («мережеголіков») продовжує зростати. До міжнародної класифікації психічних розладів (Diagnostic and Statisticai Manuai of Mental Disorders - Fourth Edition «DSM-IV», American Psychiatric Association, 1995) внесено захворювання «кібернетичні розлади».

Власне кажучи, в мережі Інтернет є практично відкрита інформація по виготовленню синтетичних наркотиків. Зокрема, в дослідженнях С.А. Роганова, які направлені на аналіз розслідування кримінальних справ, пов'язаних з незаконним обігом наркотичних речовин, зазначено, що методи синтезу наркотиків часто беруться з Інтернету [6].

Слід зазначити також, що сьогодні Інтернет представляє велику можливість для проведення розвідувальних заходів (операцій), про що видно з аналізу відповідних сайтів.

Саме поняття «комп'ютерна розвідка» існує доволі давно. Так, ще на початку 90-х років аналітики спецслужб США звернули увагу на те, що велика частина необхідної інформації без особливих зусиль може бути отримана через Інтернет. Це дозволило переглянути структуру фінансування спецслужб у бік значного збільшення засобів, що виділяються на «комп'ютерну розвідку». Підрозділи по дослідженню і використанню Інтернет потужно працюють в ЦРУ, ФБР, МОССАД і інших спецслужбах розвинених держав. Сферою їх діяльності є легальна розвідка в глобальній мережі, організація каналів зв'язку з агентурою, збір матеріалів по оперативно значимим ситуаціям, проведення акцій «інформаційної війни», вивчення особових характеристик політиків, учених, військових, а також найважливіших носіїв секретів у якості можливих кандидатів на вербування.

Підсумовуючи зазначимо, що здобуття будь-якої інформації про злочинну діяльність вимагає певних тактичних зусиль і організаційних форм: дій негласних співробітників, оперативно-пошукових груп, оперативних контактів з громадянами. Особливо це стосується злочинів у сфері інформаційних технологій, інформацію про які можна отримати лише вивченням стосунків (глибинних явищ), що часто ніяк не фіксуються візуально.

Тому підвищення ефективності роботи правоохоронних органів по розкриттю і розслідуванню злочинів у сфері високих технологій в даний час неможливе без інтеграції в діяльність міліції нових інформаційних технологій.

ЛІТЕРАТУРА

1. Наказ МВС України «Про створення у структурі ДСБЕЗ підрозділів по боротьбі з правопорушенням у сфері інтелектуальної власності та високих технологій» : від 31.05.2001 р., № 429.

2. Наказ МВС України «Про затвердження Типового положення про підрозділи ДСБЕЗ по боротьбі з правопорушенням у сфері інтелектуальної власності та високих техноло-

ISSN 1995-6134

гій» : від 19.08.2001 р., № 737.

3. Маклаков Г. Ю. Методологічні підходи, до вдосконалення підготовки кадрів з ОВС з урахуванням розвитку інформаційних технологій / Г. Ю. Маклаков, Е. В. Рижков // Проблеми правознавства та правоохоронної діяльності : зб. наук. ст. – 2001. – № 2. – С. 121-131.

4. Маклаков Г. Ю. Анализ сплоченности студенческой группы в работе куратора / Маклаков Г. Ю. // Структурно-системный подход в обучении и воспитании. – Днепропетровск : ДГУ, 1984. – С. 129-131.

5. Рыжков Э. В. Энергоинформационная безопасность общества и государства с позиции деятельности правоохранительных органов / Рыжков Э. В. // Злочини проти особистої волі людини : збірник матеріалів міжнародного науково-практичного семінару (19-20 вересня 2000 р.). – Х., 2002. – С. 83-88.

6. Роганов С. А. Синтетические наркотики: вопросы расследования преступлений : монографія / С. А. Роганов. – СПб., 2001. – 224 с.

Бойченко О. В. Особливості оперативно-розшукової протидії комп'ютерній злочинності / О. В. Бойченко, М. М. Новиков // Форум права. – 2010. – № 1. – С. 34–37 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2010-1/10bovpkz.pdf

Проведено аналіз проблем оперативно-розшукової протидії злочинам у сфері інформаційних технологій. Визначено зростання комп'ютерної злочинності з застосуванням Інтернет; запропоновано комплексне застосування програмних засобів у поєднанні з профілактичними заходами по протидії комп'ютерній злочинності.

***

Бойченко О.В., Новиков М.М. Особенности оперативно-розыскного противодействия компьютерной преступности

Проведен анализ проблем оперативно-розыскного противодействия преступлениям в сфере информационных технологий. Определен рост компьютерной преступности с применением Интернет; предложено комплексное применение программных средств в сочетании с профилактическими мероприятиями по противодействию компьютерной преступности.

***

Boychenko O.V., Novikov M.M. Features of Operatively-Search Counteraction Computer Criminality

The analysis of problems of operatively-search counteraction crimes is conducted in the field of information technologies. Growth of computer criminality is certain with application the Internet; ccomplex application of programmatic facilities is offered in combination with prophylactic measures on counteraction computer criminality.