УДК 376:379
К.В.Тарасюк
аспірант Східноєвропейського національного університету імені Лесі Українки

ПРОКУРОРСЬКИЙ НАГЛЯД ПРИ РОЗСЛІДУВАННІ КОМПЮТЕРНИХ ЗЛОЧИНІВ

В даній статті досліджуються актуальні питання сутності та методики розслідування комп'ютерних злочинів. Розглянуто роль прокурорського нагляду у попередженні комп'ютерних злочинів.
Ключові слова: *комп'ютерна злочинність, прокурорський нагляд*

Тарасюк К.В. A directorate of public prosecutions is at investigation of computer crimes. *The pressing questions of essence and methodology of investigation of computer crimes are investigated in this article. The role of directorate of public prosecutions is considered in warning of computer crimes.*
Keywords: computer criminality, directorate of public prosecutions

Як свідчить історія розвитку світового науково-технічного прогресу, будь-яка технічна новація, зокрема в галузі засобів комунікації, неминуче притягувала до себе людей, які намагалися і намагаються використати її для вчинення правопорушення, злочину.

Комп'ютеризація породила новий вид злочинів, які в теорії та практиці кримінології одержали умовну назву "комп'ютерні злочини". Це в свою чергу викликало потребу осмислення комп'ютерної злочинності як соціального явища і напрацювання відповідних методик боротьби з нею, в тому числі виявлення та розслідування злочинів, що вчиняються з використанням комп'ютерних технологій [2].

"Комп'ютерна злочинність", особливо її транснаціональна складова, стала однією з міжнародних проблем, що зумовлено широким впровадженням глобальних інформаційних мереж.

Комп'ютерні злочини характеризуються наступними особливостями:

високою латентністю;

складністю їх виявлення та розслідування;

складністю доказу в суді подібних справ;

транснаціональною складовою в основному з використанням інформаційної мережі Internet;

високим збитком навіть від одиничного злочину.

Висока латентність таких злочинів пояснюється, насамперед тим, що державні комерційні структури, які зазнали нападу, особливо в банківській діяльності не дуже довіряють можливості розкриття таких злочинів правоохоронними органами. На наш погляд, однією з основних причин високої латентності та низького рівня розкриття злочинів у сфері комп'ютерної інформації є проблеми, які виникають перед правоохоронними органами на стадії порушення кримінальної справи внаслідок складності кваліфікації злочинних діянь та особливостей проведення окремих слідчих дій.

Розглядаючи труднощі, які виникають при розслідуванні таких злочинів треба мати на увазі, що існує багато особливостей, які повинні враховуватися при проведенні таких дій, як огляд місця події, обшук та вилучення речових доказів, допит потерпілих і свідків, призначення експертизи. Для того, щоб фактичні дані були визначені доказами, вони повинні бути отримані з джерел і з дотриманням правил, які встановлені кримінально - процесуальним кодексом [1,132].

Вивчення кримінальних справ цієї категорії злочинів дає можливість зрозуміти те, що одна із основних причин низької якості слідства є відсутність систематизованих та відпрацьованих методик розслідування комп'ютерних злочинів, а також помилки , які вчиняються при проведенні слідчих дій відносно комп'ютерної інформації чи комп'ютерів.

Особливістю комп'ютерних злочинів, що вчиняються групою осіб, є обов'язкова присутність учасника злочинної групи як хакер. Цим жаргонним терміном називають особу, яка володіє знаннями і навичками несанкціонованого проникнення до комп'ютерної системи.

Переважно безпосередніх виконавців, причетних до вчинення комп'ютерного злочину, встановлюють у момент одержання ними готівки чи товарів. При їх допиті насамперед слід з'ясувати : хто разом з ними використовував комп'ютерну техніку в корисливих цілях; скільки разів і з рахунків яких організацій знімалися гроші, в який спосіб; кому передавалися і як розподілялися гроші між співучасниками злочину.

У разі, коли підозрювані або обвинувачені не бажають називати співучасників, рекомендується використовувати поліграф за допомогою спеціаліста. Це дає можливість одержати орієнтовну інформацію для планування наступних слідчих дій з метою одержання на цій основі офіційних процесуальних доказів. Висновок про наявність наміру на заволодіння чужим майном, заздалегідь обдуманого наміру вчинити розкрадання коштів через використання комп'ютерної системи може бути зроблений на основі аналізу всієї множини доказів [3,140].

Факт неправомірного доступу до інформації в автоматизованій(комп'ютерній) системі чи мережі, як правило виявляється: користувачами автоматизованої інформаційної системи , що стали жертвою цього правопорушення; в результаті оперативно-розшукової діяльності правоохоронних органів; при проведенні ревізій, інвентаризацій та перевірок; при проведенні судових експертиз та слідчих дій з кримінальних справ по інших злочинах; за інших обставин.

Ознаками несанкціонованого доступу або підготовки до нього можуть бути такі обставини: поява у комп'ютері неправдивих даних; не оновлення тривалий час в автоматизованій інформаційній системі кодів, паролів та інших захисних засобів; часті збої в процесі роботи комп'ютерів; часті скарги користувачів комп'ютерної системи чи мережі на збої і її роботи; робота декого з персоналу понад норми робочого часу без поважних на те причин; немотивовані відмови від відпусток окремих співробітників, які обслуговують комп'ютерні системи чи мережі; раптове придбання співробітником у власність дорогого комп'ютера чи іншого дорогого майна; часті випадки перезапису окремих даних без поважних на те підстав; надмірна зацікавленість окремих співробітників змістом документів (листингів) , що виходять з принтерів, роздруковуються на папері після комп'ютерної обробки тощо.

Вирішення завдання встановлення місця несанкціонованого доступу до комп'ютерної системи чи мережі викликає певні труднощі, бо таких місць може бути декілька. При встановленні факту неправомірного доступу до інформації у комп'ютерній системі чи мережі слід виявити місця , де розміщені комп'ютери, що мають єдиний комунікаційний зв'язок.

Простіше це завдання вирішується у разі несанкціонованого доступу до окремих комп'ютерів, що знаходяться в одному приміщенні. Однак, при цьому необхідно врахувати, що інформація на машинних носіях може знаходитися в іншому приміщенні, що слід також встановлювати.

Складніше встановити місце безпосереднього застосування технічних засобів несанкціонованого доступу, який був здійснений за межами організації, через систему електронної комунікації тощо. Для цього необхідно залучати фахівців, що мають спеціальні прилади та комп'ютерні програмні засоби виявлення несанкціонованого доступу. Встановленню підлягає також місце зберігання інформації на машинних носіях або у вигляді роздруківок, одержаних в результаті, одержаних у результаті неправомірного доступу до комп'ютерної мережі або системи [3,142].

У розслідуванні комп'ютерних злочинів велику роль відіграє прокурорський нагляд, який спрямований на додержання та застосування в області комп'ютерної інформації, попередження комп'ютерної злочинності.

Успіх профілактичної діяльності органів прокуратури значною мірою залежить від того, наскільки прокурор проінформований про фактичний стан комп'ютерної злочинності, обставини, що їй сприяють.

Для організації профілактичної роботи прокурору необхідно мати повні відомості про комп'ютерну злочинність: її стан та динаміку в цілому по місту, району, області; на конкретних об'єктах; види комп'ютерної злочинності; фактори, що впливають на її стан, дані про осіб, які скоїли комп'ютерні злочини та ін.[6].

Для детального вивчення комп'ютерної злочинності прокурорам доцільно використовувати різні методи, у тому числі: аналіз статистичних даних про злочинність у сфері інформаційних технологій і обставини, що їй сприяють.

На вказані обставини звертається увага прокурорів у Наказі Генерального прокурора України №1/1 від 19 січня 2004 року "Про організацію аналітичної і методичної роботи в органах прокуратури". У ньому передбачається планувати аналітичні заходи з урахуванням стану злочинності та боротьби з нею, додержання та виконання законів, рівня ефективності прокурорського нагляду та об'єктивних підстав для цього.

Плануючи аналітичні заходи, у тому числі аналіз стану злочинності, умов і причин, що сприяють вчиненню злочину, прокурор визначає напрямки наглядової діяльності.

Відповідно до законодавства про прокуратуру України одною із основних галузей прокурорського нагляду є нагляд за додержанням і застосуванням законів. Тому є підстави стверджувати, що першочергове значення в плані попередження злочинності й інших правопорушень має наглядова діяльність органів прокуратури [7,34].

Нагляд за додержанням законодавства про інформацію значною мірою попереджує злочини у сфері інформаційних технологій.

Повноваження прокурора з виявлення порушень законів у сфері інформаційних технологійреалізуються в процесі перевірок. Виявивши порушення законів у вищезазначеній сфері, прокурор добивається їх усунення, поновлення порушених прав і притягнення у встановленому порядку до відповідальності осіб, які допустили ці порушення. Такі перевірки і прийняті за їх результатами заходи прокурорського реагування можна розглядати як прикладні кримінологічні дослідження , оскільки вони за замістом спрямовані на виявлення порушень інформаційного законодавства, прав громадян. Якщо зазначені порушення своєчасно не будуть припинені, то вони можуть сприяти вчиненню злочинів.

Важливим фактором підвищення рівня прокурорського нагляду за додержанням і застосуванням законів у сфері інформаційних технологій є ефективність дій актів прокурорського реагування на виявлені порушення.

Передбачені Законом України « Про прокуратуру» акти прокурорського реагування: подання, протест, припис, постанова про порушення кримінальної справи, дисциплінарне провадження або провадження про адміністративне правопорушення - є найбільш дієвими засобами реагування на виявлені в процесі перевірок правопорушення, у тому числі й криміногенні фактори. У даному випадку юридичних і фізичних осіб спрямовується в правове русло, реально поновлюються порушені права, притягуються до відповідальності винні особи.

Прокурорське втручання у формі протесту попереджує дію криміногенних факторів, несприятливий розвиток подій, які можуть закінчитися злочином.

Особливе значення у попередженні злочинних проявів має такий акт прокурорського реагування , як подання. Антикриміногенна роль подань визначається тим, що в цьому акті відповідно до вимог ст.23 Закону України « Про прокуратуру» прокурор не тільки констатує порушення закону, але й аналізує їх причини та умови, а також вимагає усунути порушення закону, причини цих порушень і умови, що їм сприяють.

Дуже важливо, щоб прокурор кримінологічно обґрунтував подання і націлив його на усунення причин і умов правопорушення. При цьому кримінологічно грамотний аналіз обставин, які сприяли правопорушенням, правильно визначити адресата цих документів.

Як загальний висновок треба зазначити, що використання і впровадження сучасних інформаційних технологій привело до появи нових видів злочинів, зокрема до порушень роботи автоматизованих систем і несанкціонованого доступу до комп'ютерної інформації. По своєму механізму, способам вчинення і приховання цей злочин має визначену специфіку, яка характеризується високим рівнем латентності і низьким рівнем розкриття, а окремі види таких злочинів мають транснаціональний характер [8,65].

Аналіз діяльності органів прокуратури з нагляду за додержанням законодавства у сфері інформаційного законодавства дозволяє зробити висновок, що вона сприяє стабілізації, упорядкуванню, приведенню в законні рамки відносини у сфері комп'ютеризації, усуненню кримінально небезпечних ситуацій, причин і умов, які сприяють кримінально караним діянням, що посягають на права і свободи громадян, захисту охоронюваних законом інтересів суспільства і держави.

Відносна новизна виниклих проблем, стрімке нарощування процесів комп'ютеризації суспільства ставлять перед правоохоронними органами складні питання боротьби з цим новим соціально- правовим явищем і зокрема проблему виявлення та розслідування таких злочинів.

Сьогодні « комп'ютерна злочинність» вийшла зі сфери контролю правоохоронних органів і прокурорського нагляду і загрожує перерости у серйозну державну та міжнародну проблему.

1.Батурин Ю.М., Жодзинський А.М . Компьютернаяпреступность и компьютернаябезопасность.- М: Юрид. література, 1999.- 158 с.

2.Біленчук П.Д. Організована транснаціональна комп'ютерна злочинність: глобальна проблема третього тисячоліття.- К.: Національна академія внутрішніх справ України.-2002

3.Вехов Б.В. Компютерниепреступления : способи совершения и раскрития.- М.:Право и закон, 1996.-182 с.

4.Какоткин А.Компьютерниевзломщики// Аиф.-1997.- №8

5.Кримінальний кодекс України.- К.: ВЕЛЕС, 2006.-152 с.

6.Кримінальне право України: Особлива частина: Підручник /М.І.Бажанов, Ю.В. Баулін, В.І. Борисов та ін.; За ред..проф. М.І.Бажанова, В.В.Сташиса, В.Я. Тація.- 2-е вид., перероб. І доп.- К.: Юрінком Інтер, 2005.- 544 с.

7.Максимюк А Особливості прокурорського нагляду//Вісник прокуратури.-2009.-№1.-С.33-41.

8. Руденко М Проблеми та перспективи прокурорського нагляду за додержанням законів в Україні//Право України.-2002.-№6.-С65