УДК 343.296:004

А.І. ЖУРБА, Донецький юридичний інститут Луганського державного університету внутрішніх справ

ДЕЯКІ ОСОБЛИВОСТІ ВИЯВЛЕННЯ ПРИЧИН І УМОВ, ЩО СПРИЯЛИ СКОЄННЮ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Ключові слова: *комп'ютерні злочини, причини, умови, виявлення*

У кримінальній справі можливе досягнення істини лише тоді, коли об'єктивно, всебічно і повно встановлено всі обставини, які входять до предмета доказування. До необхідних елементів законодавець відніс причини і умови, які сприяють скоєнню злочину. Під час розслідування кримінальної справи встановлення вказаних обставин має велику практичну, профілактичну і соціальну значущість. Органи розслідування зобов'язані виявляти причини і умови, що сприяють скоєнню злочину. На цьому ґрунті виникають серйозні практичні труднощі в застосуванні цієї норми до конкретних діянь, і це має особливе значення для розслідування комп'ютерних злочинів.

Причини й умови, що сприяють скоєнню злочину, постійно дискутувалися в наукових колах щодо повноти дослідження, необхідності доказування або виявлення, стосовно окремих категорій кримінальних справ тощо. Цим проблемам присвячено праці вітчизняних і зарубіжних учених, а саме: Т.В. Аверьянової, В.А. Баніна, Р.С. Бєлкіна, С.І. Данілова, Ю.Г. Корухова, Г.М. Міньковського, П.П. Михайленко, А.І. Михайлова, Р.Д. Рахунова, А.Д. Соловйова та ін. Комп'ютерним злочинам, причинам і умовам, що сприяють скоєнню цього роду діянь, приділяється увага в роботах П.Д. Біленчука, В.Б. Вєхова, В.Д. Гавловського, В.О. Голубєва, М.А. Зубаня, В.Е. Козлова, В.В. Попова, С.Н. Рогозіна, В.С. Цимбалюка, Н.Г. Шурухнова та ін. У той же час, незважаючи на значущість проведених досліджень, залишаються аспекти, досліджені неповною мірою. Тому метою цієї статті є аналіз і виявлення особливостей причин і умов, що сприяють скоєнню комп'ютерних злочинів. Її новизна полягає у висновку про потребу вивчення зовнішніх елементів, що також можуть сприяти скоєнню комп'ютерного злочину, й їх подальшому усуненню на загальних підставах.

Встановлення зазначених причин і умов є найчастіше невчасною профілактикою злочинів, направленою на запобігання аналогічним діянням, скоєння яких можливе на тому ж ґрунті. Ці елементи повинні встановлюватися в ході всього розслідування і виявлятися неодмінно у стадії досудового слідства. Це зумовлено, перш за все, можливістю безпосереднього дослідження слідчим, органом дізнання місця події, що зберегла сліди злочину, спілкування з учасниками події тощо. Часовий чинник впливає на усунення причин і умов у зв'язку з яскравістю негативних емоцій. Наприклад, виявлені обставини більш доцільно усувати відразу ж після скоєння злочину, ніж через два місяці, відведені для досудового слідства. У стадії судового розгляду суд повинен перевірити зібрані докази, пов'язані з причинами й умовами скоєння злочину, і, крім того, упевнитися у вживанні заходів для усунення доведених обставин. Ця умова є невід'ємною частиною профілактичного завдання судочинства.

Аналіз наукової літератури свідчить, що предмет доказування у встановленні причин і умов, що сприяють скоєнню злочину, складається з трьох фактичних даних, що характеризують:

1) причини формування антигромадської установки обвинуваченого і пояснюють виникнення його антигромадських поглядів;

2) перетворення антигромадської установки на конкретний злочинний намір (приводи для скоєння злочину);

3) об'єктивні умови, які сприяли настанню злочинного результату [1, с.22].

Деякі вчені до умов, які сприяли скоєнню злочину, відносять і обставини, що сприяли приховуванню його слідів і наслідків [2, с.101]. На нашу думку, вказані умови не входять до

предмета доказування, а мають бути віднесені до загальної профілактики злочинів. У цьому випадку мова повинна йти про умови діяння, які спричинили виникнення злочину.

Отже, слідчий, виявляючи причини й умови скоєння злочину і усуваючи їх, завжди має справу з умовами формування причин і скоєння злочинів. Аналогічний висновок можна зробити, наприклад, із твердження, зробленого С.С. Степчевим, про те, що матеріальне становище обвинуваченого й умови, в яких протікало його особисте життя і трудова діяльність, будучи всебічно вивченими і проаналізованими, можуть пояснити причини, що сприяли скоєнню злочину [3, с.111].

Умови, що сприяють скоєнню комп'ютерних злочинів, можна поділити на три види. До першого необхідно віднести умови, в яких функціонує комп'ютерна техніка потерпілого. До другого – умови технічного росту особи, що скоїла комп'ютерний злочин. До третього слід віднести умови морального розвитку особи комп'ютерного правопорушника. Межа між цими видами є достатньо умовною і залежить від сфери діяльності особи, що скоїла комп'ютерний злочин, і виду останнього.

До першого типу слід віднести:

- порушення правил роботи з інформацією. Це може виражатися в порушенні конфіденційності даних, залишення працюючої системи без нагляду або в авторизованому режимі тощо;

- застосування виробничого комп'ютера для невідповідних цілей. Зокрема, установка програмного забезпечення або використання інших ресурсів (наприклад, Інтернету), не потрібних для виконання службових функцій;

- недостатнє застосування програмних і технічних засобів захисту інформації. Використання слабких або таких, що не відповідають виду діяльності, мережевих фільтрів, криптографічних систем;

- ігнорування вимог, направлених на збереження конфіденційності інформації в Інтернеті. Відправка відкритої електронної пошти, зокрема з вкладеними даними авторизації без застосування криптографічних засобів тощо;

- відсутність необхідного контролю за здійсненням операцій над інформацією. Недосконаліть системи статистики роботи програмного забезпечення. Може виражатися в обмеженні статистичних файлів у розмірі або в кількості фіксуючих операцій. З іншого боку, цей чинник може виражатися в недостатності кадрових ресурсів;

- відсутність або недостатнє використання антивірусних систем. Наприклад, виставлянння низького режиму стеження за системою.

До другого типу належать:

- недостатність уваги правовим аспектам, що приділяється в технічних навчальних закладах;

- відкритість в середовищі Інтернету технічних аспектів скоєння злочинів. Виражається у відсутності заборон на розміщення інформаційних ресурсів в Інтернеті, які пояснюють способи скоєння комп'ютерних злочинів, отримання вигоди від них, поширюють спеціальне програмне забезпечення тощо;

- специфічне негативне середовище спілкування. Наприклад, рухи хакерів, клани та ін.

До третього типу можна віднести такі чинники:

- негативний вплив з боку колективу, в якому працює особа, що скоїла комп'ютерний злочин. Це може бути аморальна поведінка членів сім'ї, робочого колективу або навчальної групи. Крім того, сюди слід віднести недостатність уваги з боку керівництва до злочинних умов;

- фінансове становище обвинуваченого, відсутність у нього стабільного доходу тощо;

- недостатність загальної профілактики злочинності з боку правоохоронних органів.

У кримінальних справах у сфері комп'ютерних злочинів встановлення умов, що сприяють скоєнню злочинів, проводиться стандартними методами, які необхідно позначити з урахуванням специфіки цього виду діянь:

- допит підозрюваного на предмет встановлення інформації про те, що викликало не-

обхідність у скоєнні злочину, яким чином було досягнуто рівня, потрібного для здійснення злочинних намірів та ін.;

- допит потерпілих про особливості роботи комп'ютерної системи, засоби захисту (антивірус, міжмережевий екран, застосування криптографії) тощо;

- допит розробників і обслуговуючого персоналу програмного забезпечення, яке було використано для скоєння злочину і захисту інформації;

- допит осіб, які надали інформативну допомогу в скоєнні злочину;

- виїмка і огляд документації програмного забезпечення у вказаному розумінні;

- проведення експертизи з питання співвідношення особливостей програмного забезпечення і способу скоєння комп'ютерного злочину;

- проведення відтворення обстановки й обставин події.

Досліджуючи програмне забезпечення, що є в комп'ютері потерпілого, слід враховувати, що розробники професійного програмного продукту гарантують надійність і за необхідності враховують претензії з приводу відхилення функціонування системи від норми. Цей аспект потрібно врахувати з тієї позиції, що, можливо, буде необхідно направити подання і виробникам програми.

Значну допомогу у встановленні причин і умов, що сприяють скоєнню злочинів, надає внутрішнє (службове) розслідування. Часто у висновках службових розслідувань є дані про порушення захисту інформації, недостатність уваги до цих питань з боку персоналу та ін. Отримані відомості не можна розглядати як догму і вважати достатніми для встановлення зазначених причин і умов. Будь-який висновок повинен бути ретельно перевірений в кримінально-процесуальному порядку і відбитися в поданні слідчого про усунення причин і умов, що сприяли скоєнню злочину. Якщо висновки службового розслідування і вжиті заходи на підприємстві, що зазнало інформаційної шкоди, повністю відбивають причини й умови скоєння злочину і усувають їх, на нашу думку, виносити подання в порядку 23-1 КПК України недоцільно.

У науковій літературі наголошувалося на тому, що важливу роль у профілактиці злочинів мають відігравати заходи соціального запобігання [4, с.177]. Цим заходам у літературі, присвяченій комп'ютерній злочинності, приділено недостатньо уваги. Основний акцент робиться на методах захисту інформації. На наш погляд, захист інформації повинен бути другорядним. Будь-яке комп'ютерне злочинне діяння, яке було припинено внаслідок активності систем захисту інформації, може містити ознаки незакінченого злочину. Такі дії також можуть заподіювати шкоду, яка в комп'ютерних злочинах може виражатися в розголошуванні інформації із закритим доступом, порушенні в роботі систем захисту тощо. Наприклад, особа зробила спробу несанкціонованого доступу до інформації підприємства, після чого, не справившись із системою захисту, розмістила відомі їй дані про особливості захисту та інші елементи в електронному форумі Інтернету.

На підставі викладеного виділимо заходи, що впливають на умови соціального характеру комп'ютерної злочинності:

1. Обмеження роботи ресурсів Інтернету, зміст яких був використаний або послужив стимулом обвинуваченому у скоєнні комп'ютерного злочину. Необхідно направити подання в порядку ст.23-1 КПК України власникові ресурсу Інтернету про видалення із сайту інформації (що описує спосіб здійснення або програмний продукт), яку було використано під час скоєння злочину.

2. Вимагати належного рівня уваги правовим аспектам у технічних закладах, де навчався обвинувачений.

3. Вимагати від технічного керівництва підприємства, де працює обвинувачений, приділяти увагу профілактиці комп'ютерної злочинності серед робочого колективу, якщо подія злочину пов'язана з професійною діяльністю.

4. Встановлювати середовище спілкування обвинуваченого, а саме: дії з боку родичів, кола знайомих, у тому числі з використанням віртуального спілкування.

5. Усувати конфліктні ситуації, які спонукали до скоєння злочину.

Методам захисту інформації приділяється значна увага в літературі як правового, так і технічного спрямування. Гарантувати безпеку комп'ютерних систем від шкідливих програм і решти погроз практично неможливо. Розглядаючи питання, пов'язані із захистом інформації, учені стверджують, що захисту від копіювання програмного забезпечення ніколи не було і ніколи не буде. Це неможливо навіть теоретично [5, с.30]. Те саме можна сказати і відносно решти умов, пов'язаних із несанкціонованим доступом до системи, розповсюдженням вірусів, зміною інформації тощо. Слід враховувати, що розробники програм ще на стадії проектування передбачають різноманітні засоби захисту. З іншого боку, їм протистоять особи, що скоюють комп'ютерні злочини, знаходячи недоліки в цій сфері, порушуючи захист тощо. Отже, ставити завдання досягти універсальності систем захисту марно, проте сприяти цьому органи розслідування, виявляючи умови, що сприяли скоєнню злочину, і усуваючи їх, зобов'язані.

Відповідно до ст.23-1 КПК України орган дізнання, слідчий, прокурор, встановивши причини й умови, які сприяли скоєнню злочину, вносять до відповідного державного органу або громадської організації подання про застосування заходів щодо усунення цих умов. Не можна погодитися з думкою В.Т. Очередіна, що в поданні немає необхідності детально описувати обставини скоєння злочину, достатньо вказати час, місце і характер протиправних дій. Основну увагу, на думку дослідника, слід приділити детальному відображенню причин, що сприяли скоєнню злочину [6, с.30]. Такий виклад, на наш погляд, може порушити повноту реалізації цієї вимоги. Обсяг причин і умов скоєння злочину повинен бути доведений і усунений у якомога більш повному вигляді. Слід враховувати те, що особа, яку буде задіяно в їх усуненні, за умови правильного ставлення до цього питання, зможе більш повно виконати поставлені завдання.

Закономірно виникає питання про те, чи зобов'язаний слідчий безпосередньо вимагати усунення причин і умов, чи він повинен обмежуватися перекладанням рішення на інші органи і стежити за виконання винесеного подання? Наприклад, у відповіді на подання може бути вказано, що проведеним службовим розслідуванням виявлено, що персонал підприємства порушень не допускав, захисні засоби інформації працювали відповідно до технічних вимог. На наш погляд, для успішної профілактики й усунення причин і умов, що сприяли скоєнню злочину, органи розслідування необхідно наділити відповідними повноваженнями щодо можливої заборони на використання певного устаткування, наприклад до виконання вимог, вказаних у поданні. Крім того, чи можуть бути виконані вимоги особою, що провадить розслідування, виявляти повну картину причин і умов, наскільки це можливо зробити в межах повноважень і доступних матеріалів кримінальної справи? Будь-яка умова або причина повинні виявлятися з достатньою глибиною. Наприклад, вимога до підприємства усунути уразливість у захисті комп'ютерної системи має містити, якщо це можливо, конкретний номер порту, через який відбувся несанкціонований доступ. Вимога усунути уразливість решти портів, які не використовувалися в злочинній діяльності підозрюваного (обвинуваченого), але через які можливе здійснення несанкціонованого доступу, повинна здійснюватися у межах загальної профілактичної діяльності (наприклад, п.2 ст.10 Закону України «Про міліцію»). Деякі автори стосовно обставин, виявлених, але не пов'язаних із розслідуваною кримінальною справою, зазначають, що «питання про них повинне вирішуватися самостійно» [1, с.30].

Після усунення причин і умов, що сприяли скоєнню злочину, може виникнути необхідність підтримання негативних умов для скоєння злочину. Наприклад, проникнення в комп'ютерну систему відбулося унаслідок порушення розкладу зміни паролів. Умови було усунено цій частині шляхом чергової заміни кодів паролів. На наш погляд, подальше підтримання негативності цих умов для злочинів, зокрема подальші зміни паролів

відповідно до розкладу, має здійснюватися в контексті загальної профілактичної діяльності. Крім того, наприклад, у разі зміни паролів необхідно стежити за якістю вжитих заходів відповідно до встановлених вимог. Безумовно, усунення умов скоєння злочину має проводиться на відповідному якісному рівні. Цей аспект проблеми вимагає дослідження як на теоретичному, так і на практичному рівні.

Таким чином, установлюючи причини й умови, що сприяли скоєнню комп'ютерного злочину, слід акцентувати увагу на соціальних умовах, що стали стимулом до скоєння злочину. Причини й умови скоєння злочину мають бути доведені в максимально повному і точному обсязі. В іншому випадку мета усунення умов може вважатися не досягнутою. Зовнішні елементи, які також можуть сприяти скоєнню комп'ютерного злочину, повинні піддаватися виявленню й усуненню на загальних підставах, як і необхідність, що стосується підтримання негативних умов для скоєння злочину після їх усунення.

ЛІТЕРАТУРА

1. Звирбуль В., Кудрявцев В., Михайлов А., Рахунов Р., Якубович Н. Выявление причин преступления и принятие предупредительных мер по уголовному делу. –М.: Юрид. лит., 1967. –152 с.

2. Савонюк Р. Щодо термінів і понять Кримінально-процесуального кодексу України // Право України. –2004 . –№ 2. –С.99-101.

3. Руководство для следователей /Под ред. Н.В. Жогина. –М.: Юрид. лит., 1971. –752 с.

4. Бородин С.В. Рассмотрение судом уголовных дел об убийствах. –М.: Юрид. лит., 1964. –212 с.

5. Хогланд Г. Мак-Гроу Г. Взлом программного обеспечения: анализ и использование кода. –М.: Вильяме, 2005. –400 с.

6. Очередин В.Т. Изучение личности несовершеннолетнего обвиняемого на предварительном следствии: Учебное пособие. – Волгоград: ВСШ МВД СССР, 1985. –40 с.

Журба А.І. Деякі особливості виявлення причин і умов, що сприяли скоєнню комп'ютерних злочинів // Форум права. -2007. -№ 1. –С.59-63 [Електронний ресурс]. – Режим доступу: http://www.nbuv.gov.ua/e-journals/FP/2007-1/07gaickz.pdf

Розглянуто аспекти застосування ст.23 КПК України щодо виявлення причин і умов, які сприяють скоєнню комп'ютерних злочинів. Акцентується увага на необхідності враховувати соціальні умови скоєння комп'ютерних злочинів, обсяг їх доказування та усунення під час розслідування.

***

Журба А.И. Некоторые особенности выявления причин и условий, которые оказывали содействие в совершении компьютерных преступлений

Рассмотрены аспекты применения ст.23 УПК Украины относительно выявления причин и условий, которые оказывают содействие в совершении компьютерных преступлений. Акцентируется внимание на необходимости учитывать социальные условия совершения компьютерных преступлений, объем их доказывания и устранение во время расследования.

***

ZHurba A.I. Some of feature in revealing of the reasons and conditions which assisted in fulfillment of computer crimes

Aspects of application of clause 23 Criminal-remedial code of Ukraine concerning revealing the reasons and conditions which assist in fulfillment of computer crimes are considered. The attention to necessities to take into account social conditions of fulfillment of computer crimes, volume their substantiation and elimination is accented during investigation.