Ученые записки Таврического национального университета им. В. И. Вернадского
Серия «Юридические науки». Том 22 (61). № 1. 2009 г. С. 229-235.

УДК 343.98

Пашнєв Д.В., Рудик М.В.

ОСОБЛИВОСТІ ВИЯВЛЕННЯ ТА КРИМІНАЛЬНО-ПРАВОВА КВАЛІФІКАЦІЯ ЗЛОЧИНІВ, ЩО ПОСЯГАЮТЬ НА КОМП'ЮТЕРНУ ІНФОРМАЦІЮ З ОБМЕЖЕНИМ ДОСТУПОМ

Стаття присвячена питанням застосування спеціальних знань при перевірці інформації про комп'ютерний злочин, чіткої його кваліфікації на початковому етапі розслідування стосовно окремого складу комп'ютерного злочину – несанкціонованого розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (ст. 3622 КК України).

Ключові слова: комп'ютер, злочин, кваліфікація, спеціальні знання, несанкціоноване розповсюдження, несанкціонований збут, інформація, обмежений доступ.

Сьогодні в Україні дуже важливим є питання комп'ютерної безпеки, зараз існує безліч персональних комп'ютерів, ними обладнані практично всі установи, як державної так і приватної форми власності вони є майже в кожному будинку. Їхні потенційні можливості величезні, але нажаль вони використовуються не тільки з правомірною метою.

За останні п'ять років динаміка зростання злочинів у сфері високих технологій становить приблизно 13-15% щорічно, що говорить про існуючі сьогодні тенденції розвитку злочинних посягань у сфері інформаційно-телекомунікаційних відносин в Україні. Це, на наш погляд, дає підстави говорити про необхідність подальшого вдосконалення діяльності правоохоронних органів в цій сфері.

На шляху від виявлення злочину до притягнення особи до кримінальної відповідальності та покарання органи дізнання і досудового слідства здійснюють велику роботу по встановленню обставин вчиненого злочину, викриттю особи, яка його вчинила, збиранню доказів її вини. Успіх цієї роботи багато в чому визначається на початковому етапі розслідування. Первинні дії, що здійснюються при отриманні відомостей про злочин, нерідко дозволяють запобігти або своєчасно присікти злочин, розкрити його за гарячими слідами, захопити злочинців на місці злочину, одержати і зафіксувати цінну в доказовому відношенні інформацію. Зволікання або некваліфіковане проведення первинних дій може привести до переховування злочинця, втрати важливих доказів і створити додаткові, деколи нездоланні труднощі у викритті винного.

Але щоб ефективно діяти на початковому етапі розслідування необхідно як можливо ближче до істини уявляти суть та механізм події і давати їм правильну правову оцінку, а отже одну з ключових ролей грає найбільш наближена до реальності кваліфікація скоєного злочину.

Все вказане стосується і комп'ютерних злочинів. З нашої точки зору, найважливішим фактором своєчасного встановлення ознак злочину та розкриття його по гарячих слідах є ефективне застосування спеціальних знань при перевірці інформації про комп'ютерний злочин, а також чітка його кваліфікація вже на початковому етапі розслідування. Метою даної статті є дослідження вказаних питань щодо окремого складу комп'ютерного злочину – несанкціонованого розповсюдження або збуту комп'ютерної інформації з обмеженим доступом (ст. 3622 КК України).

Кримінально-процесуальним законодавством України не встановлено обов'язковості перевірки заяв і повідомлень про злочини. Якщо ознаки злочину є очевидними, кримінальна справа порушується негайно. Коли ознаки злочину неочевидні, відповідно до ч. 4 ст. 97 КПК України необхідно перевірити заяву або повідомлення про злочин до порушення справи. Така перевірка здійснюється прокурором, слідчим або органом дізнання в строк не більше десяти днів шляхом відібрання пояснень від окремих громадян чи посадових осіб або витребування необхідних документів. Крім того, з метою перевірки чинне кримінально-процесуальне законодавство України дозволяє до порушення кримінальної справи проводити такі слідчі дії, як огляд місця події у невідкладних випадках (ч. 2 ст. 190 КПК України), накладення арешту на кореспонденцію і зняття інформації з каналів зв'язку з метою запобігти злочину (ч. 3 ст. 187 КПК України).

У тексті ст. 97 КПК України цілі попередньої перевірки не роз'ясняються. Вони випливають зі змісту ст.ст. 94, 98, 99 КПК України, що встановлюють основні правові вимоги законності й обґрунтованості рішення про порушення кримінальної справи. Зі змісту статей випливає, що перевірка може мати такі цілі:

– встановлення даних, що вказують на ознаки злочину;

– з'ясування наявності обставин, що виключають провадження у справі.

Аналіз слідчої практики показує, що по деяких категоріях злочинів вказана вище інформація може бути одержана з матеріальних джерел тільки в результаті застосування спеціальних знань відповідних фахівців. Так, в ході попередньої перевірки матеріалів згідно ст. 97 КПК України необхідно встановити приналежність об'єктів до отруйних, сильнодіючих, психотропних речовин, наркотичних засобів або прекурсорів, вогнепальної або холодної зброї, боєприпасів, вибухових речовин; визначити наявність матеріальної підробки документів, грошей, цінних паперів, ступінь тяжкості нанесених тілесних пошкоджень, відповідність якості товарів і продукції нормативам тощо. Така ж ситуація складається і при виявленні ознак комп'ютерного злочину.

У Настанові, що регулює діяльність експертно-криміналістичної служби МВС України вказано, що одною з виконуваних нею функцій, крім експертних криміналістичних досліджень, є проведення досліджень за завданнями оперативно-розшукових підрозділів [1, п.5.3]. Мета цих досліджень не уточнюється. На думку М.Г. Щербаковського та І.І. Золотухина, для відмежування досліджень, що проводяться на стадії порушення кримінальної справи, від інших видів використання спеціальних знань і з урахуванням того, що вони здійснюються з метою перевірки припущення про вчинений злочин, ці дослідження слід іменувати «перевірочними» [2]. Єдина кінцева задача перевірочних досліджень - виявлення матеріальних ознак злочину, прямо

вказаних в нормі кримінального закону. Встановлення таких ознак служить підставою для порушення кримінальної справи.

Таке перевірочне дослідження може бути виконано як в рамках огляду місця події з участю спеціаліста, так і окремо, після огляду, у лабораторних умовах [3, с. 27].

Злочини, вчинені з використанням комп'ютерних технологій, також відносяться до вказаних категорій справ. У більшості випадків ознаки комп'ютерного злочину неочевидні, тому що зберігаються, як нами було вказано вище, на носіях комп'ютерної інформації в недоступному для звичайного сприйняття вигляді та потребують застосування спеціальних знань для їх виявлення та інтерпретації. Тільки за допомогою досліджень носіїв комп'ютерної інформації удається достовірно судити про наявність матеріальних ознак комп'ютерного злочину.

Більшість опитаних слідчих, які спеціалізуються на розслідуванні комп'ютерних злочинів (58,3 %) вказало на те, що під час огляду місця події вони стикалися з ситуаціями, коли достатні дані, які вказували б на наявність ознак злочину, необхідні для порушення кримінальної справи, знаходилися на носії комп'ютерної інформації, а інших підстав для порушення кримінальної справи не було.

Кримінально-процесуальним законом не врегульована процедура застосування спеціальних знань у стадії порушення кримінальної справи. В роз'ясненнях до ст. 196 КПК України наголошується, якщо виникне потреба у використанні спеціальних знань для встановлення обставин, що є підставою для порушення кримінальної справи, слідчий може по письмовому запиту одержати від компетентної установи або обізнаної особи довідку з питань, що його в цьому плані інтересують [4, с. 475].

На практиці результати цих досліджень відображаються в документах, які в НДЕКЦ МВС України іменуються «Довідкою», НДІСЕ Міністерства юстиції – «Висновком спеціаліста» і підписуються обізнаною особою, що проводила дослідження. Від установ інших відомств відповідь поступає у формі листа, підписаного керівником.

Суб'єктами перевірочних досліджень є фахівці в області комп'ютерних технологій. Предмет перевірочних досліджень повністю поглинається предметом судової комп'ютерно-технічної експертизи. Крім того, в обох видах досліджень вивчаються одні і ті ж об'єкти – елементи комп'ютерних технологій: технічні засоби або програмне забезпечення. Збіг предмету і об'єктів дослідження двох форм застосування спеціальних знань обумовлює застосовування однакових методів, прийомів і технічних засобів, тобто всього того, що визначає методику дослідження. Проте до методів, що використовуються в ході перевірочних досліджень, пред'являються жорсткіші вимоги, пов'язані з необхідністю збереження в незмінному вигляді складових комп'ютерних технологій та інших об'єктів для їх подальшого експертного дослідження.

Вказані співпадаючі ознаки свідчать про схожість двох видів застосування спеціальних знань для визначення обставин злочину. Проте єдиною і вирішальною їх відмінністю є непроцесуальний режим проведення перевірочних досліджень, відсутність доказового значення результатів такого дослідження. Одержані фактичні дані, поза сумнівом, відносяться до справи, але не мають такої властивості доказів, як допустимість. Документ, в якому відображені перевірочні дослідження, не є процесуальним, оскільки отриманий до порушення кримінальної справи. Дані

документи, таким чином, використовуються як довідкові, містять відомості оперативно-розшукового характеру. Проте основна мета цих досліджень - встановлення підстав прийняття процесуального рішення про порушення (відмову в порушенні) кримінальної справи.

У процесі дослідчої перевірки при наявності повідомлення про комп'ютерний злочин перевірочні дослідження застосовуються для встановлення таких необхідних для порушення кримінальної справи даних, як:

ознаки злочину;

способи і місце здійснення неправомірного доступу (копіювання, модифікація, знищення інформації, внесення шкідливих програм; зсередини організації або ззовні) і його ознаки;

засоби, використані при вчиненні злочину (технічні, програмні, носії інформації);

способи подолання захисту (підбір ключів і паролів, викрадання паролів, відключення засобів захисту тощо).

На етапі перевірки під час проведення досліджень необхідна тісна взаємодія особи, що здійснює перевірку інформації про злочин, та фахівця, яка направлена на виявлення всіх комп'ютерних слідів. Це пов'язано з завданням своєчасного вжиття необхідних дій по виявленню, вилученню, закріпленню і дослідженню слідів злочину, що є умовою успішного розслідування і розкриття злочинів. Невідкладність дій по отриманню доказової та орієнтуючої (розшукової) інформації є запорукою успіху розслідування. Отже, метою такої взаємодії є негайне отримання орієнтуючої інформації від фахівця. Отримані дані використовуються для висунення розшукових версій про напрями пошуку злочинця за гарячими слідами, виявлення носіїв комп'ютерних слідів, що знаходяться поза місцем події, з'ясування механізму і обставин вчиненого злочину тощо.

Проведення перевірочних досліджень елементів комп'ютерних технологій у взаємодії з суб'єктом дослідчої перевірки набуває великого значення при збиранні комп'ютерних слідів. Адже іноді неможливо без дослідження інформації на комп'ютерному носії виявити сліди підключень з віддаленого доступу до комп'ютерної системи, під час яких було вчинено злочин, на їх основі прослідити мережний маршрут між елементами комп'ютерних технологій, що були засобом та предметом злочину, і зібрати всі сліди цього злочину на всіх точках маршруту.

Можна рекомендувати розпочати пошук слідів комп'ютерного злочину з виявлення мережних підключень засобів комп'ютерної техніки, що знаходяться на місці події і в яких виявлені сліди злочину, та дослідження інформації, що пов'язана з цими підключеннями. А далі діяти наступним чином:

Ситуація 1. Якщо ЕОМ апаратно не підключена до мережі, або в інформації про мережні підключення не містяться ознаки, що вказують на віддалений доступ до неї під час вчинення злочину, то, скоріш за все, ця ЕОМ є і предметом злочинного посягання і засобом вчинення злочину.

Ситуація 2. Якщо ЕОМ має підключення до мережі і в інформації про мережні підключення містяться ознаки, що вказують на віддалений доступ до неї під час вчинення злочину, то залежно від інформації, що міститься в записах підключень, слід

визначити наступну точку пошуку слідів та діяти в ній згідно ситуації 1. В результаті пошук приведе до ЕОМ, які є кінцевими точками маршруту.

Всі сліди на точках маршруту фіксуються, при потребі досліджуються та вилучаються за допомогою фахівця.

Зауважимо, що у випадку вчинення конкретного комп'ютерного злочину мову треба вести про індивідуальну слідову картину. Але все ж таки можна виділити певну специфіку слідової картина цього виду комп'ютерних злочинів. Вона в основному буде характеризуватися наявністю на носії комп'ютерної інформації зловмисника файлів, що вміщують інформацію з обмеженим доступом, що стала предметом злочину, програмні та технічні засоби подолання захисту, отримання інформації шляхом перехвату активного чи пасивного, її декодування, а також іншого спеціального обладнання та програмного забезпечення для отримання комп'ютерної інформації та виготовлення її носіїв, а також розповсюдження і збуту: сканерів, цифрових фотоапаратів, принтерів, записуючих пристроїв для компакт-дисків, відповідних заготовок, чистих носіїв інформації, засобів підключення до мережі локальної і глобальної (Інтернет) тощо.

На етапі дослідчої перевірки також необхідно правильно оцінити отриману інформацію та кваліфікувати діяння, що, як показує практика, викликає деякі труднощі.

Проаналізувавши диспозицію ст. 361² КК України, можна стверджувати що це є норма загальної дії, тому, що у кримінальному кодексі України вже є самостійні склади злочинів, що передбачають незаконний збут, розповсюдження інформації з обмеженим доступом за допомогою комп'ютерних систем. Зокрема, аналіз Особливої частини КК України, дає підстави виділити ряд складів злочинів, що мають на меті охорону всілякого роду таємниць (конфіденційної інформації), що є власністю, як окремих осіб, (приватних підприємств), так і держави в цілому. Так в п'ятому розділі Особливої частини КК України є наступні склади злочинів, що передбачають кримінальну відповідальність за розголошення таємниць: ст. 159 - порушення таємниці голосування, ст. 163 - порушення таємниці листування, телефонних розмов, телеграфної чи іншої кореспонденції, що передаються засобами зв'язку або через комп'ютер, ст. 168 - розголошення таємниці усиновлення (удочеріння), ст. 182 - порушення недоторканності приватного життя. У сьомому розділі: ст. 231 - незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю, ст. 232 - Розголошення комерційної або банківської таємниці. В чотирнадцятому розділі: ст. 328 - розголошення державної таємниці, ст. 329 - втрата документів, що містять державну таємницю. Слід зазначити, що вище зазначені склади злочинів були введені до Кримінального кодексу ще у 2001 році, та вже мали практику застосування [5]. Однак наприкінці 2004 року законодавець прийняв рішення щодо суттєвого розширення розділу шістнадцятого КК України, зокрема розширивши цей розділ такими складами: ст. 361¹, що встановлює кримінальну відповідальність за створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут, та ст. 361² - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації [6, с. 6]. З одного боку це був значний крок вперед, який суттєво «розвантажив» диспозицію статті 361 КК України

редакції 2001 року. З іншого - створив деякі складнощі при практичному застосуванні даного складу злочину. Так, наприклад, при навмисному розголошені комерційної або банківської таємниці злочинець, використавши перевагу електронних носіїв інформації та глобальної мережі Інтернет, оприлюднив відомості, які їх власник вважав комерційною таємницею підприємства, внаслідок чого власник зазнав відчутної шкоди. Як в цьому випадку повинен діяти правоохоронний орган відносно кваліфікації дій злочинця? З одного боку тут присутні об'єктивні ознаки дій передбачених ст. 361². З іншого є сенс стверджувати, що злочин повинен бути кваліфікований за ст. 232 КК України, бо предмет цього злочину повністю співпадає з предметом злочину, передбаченим цією статтею. Це є дуже складним завданням, яке потребує законодавчого вирішення та роз'яснення.

Для вирішення цієї ситуації можливі два підходи: перший - необхідно виключити з XVI розділу КК України ст. 3612, як таку, що ускладнює кваліфікацію злочинних дій, спрямованих на незаконне заволодіння, розповсюдження та збут комп'ютерної інформації з обмеженим доступом, а в існуючих складах злочинів, які охороняють таємницю приватного життя, комерційну, банківську, та державну необхідно доповнити диспозиції ще однією альтернативною дією - незаконний збут або розповсюдження зазначених відомостей за допомогою комп'ютеру; другим варіантом вирішення є удосконалення диспозиції ст. 3612, а саме конкретизувати та перелічити види інформації з обмеженим доступом. При даному підході незаконний збут, розповсюдження комерційної та банківської таємниці, вчинене за допомогою комп'ютеру слід кваліфікувати лише за ст. 3612 КК України. У підтвердження цього можна навести позицію Коржанського М.Й., який вважає, що кваліфікація може бути правильною лише тоді, якщо буде застосовано саме ту норму, яка передбачає це діяння, тобто застосовано лише одну і лише певну, конкретну норму. Інакше кажучи, кваліфікувати злочин - означає надати йому кримінально-правову оцінку і застосувати до нього ту кримінально-правову норму, яка найбільш повно описує його ознаки [6, с. 6]. Те, що для правильної кваліфікації діяння необхідно вибрати і застосувати лише одну, конкретну кримінально-правову норму з декількох суміжних, подібних, яка найбільш повно описує ознаки вчиненого діяння, має суттєве практичне значення, оскільки змушує правозастосовників шукати саме ту норму, яка є єдино правильною. Така певна конкретизація кримінально-правової норми, що підлягає застосуванню, допомагає вирішенню багатьох питань кваліфікації злочинів при конкуренції кримінально-правових норм, що підлягають застосуванню. Таким чином, кваліфікація злочину і способу його вчинення підкоряється загальному правилу: діяння, при якому певні дії є способом, складовою частиною об'єктивної сторони іншого, більш тяжкого злочину, кваліфікується як один злочин. Останній варіант здається нам більш вдалим, оскільки за такою кваліфікацією ми охоплюємо як предмет злочину так і спосіб вчинення злочинних дій.

З огляду на вище зазначене необхідно зробити наголос на тому, що колізія норм Особливої частини КК України неприпустима. Вважаємо, що необхідно на законодавчому рівні розрішити цю проблему, та внести відповідні доповнення до диспозицій статей Особливої частини КК України, які передбачають кримінальну

відповідальність за розповсюдження та збут конфіденційної інформації з обмеженим доступом.

Список використаних джерел та література:

1. Настанова про діяльність експертно-криміналістичної служби МВС України // Затверджена Наказом МВС України від 30.08.99 № 682.
2. Щербаковський М.Г. Використання спеціальних знань в стадії порушення кримінальної справи / Щербаковський М.Г., Золотухін І.І. // Вісник Університету внутрішніх справ. - 1997. - №2. - с. 36-44.
3. Лавров В.П. Расследование преступлений по горячим следам: Учеб. пособие / В.П. Лавров, В.Е. Сидоров. - М.: ВЮЗШ МВД СССР, 1989. - 56 с.
4. Уголовно-процессуальный кодекс Украины: науч.-практ. коммент. / Ю.П. Аленин, Е.Н. Гидулянова, Ю.А. Гурджи и др.; под общ. ред.: В.Т. Маляренко, Ю.П. Аленин. - Х.: Одиссей, 2005. - 967 с.
5. Науково-практичний коментар Кримінального кодексу України від 5 квітня 2001 року / [М.Л. Мельник, М.І. Хавронюк та ін.]. - К. : Каннон, 2003. – 1056 с. - (Нормативні документи та коментарі).
6. Коржанський М.Й. Кваліфікація злочинів : монографія / Коржанський Микола Йосипович. - К. : Атіка, 2002. - 640 с.

Пашнев Д.В., Рудик М.В. Особенности выявления и уголовно-правовая квалификация преступлений, которые посягают на компьютерную информацию с ограниченным доступом.

Статья посвящена вопросам применения специальных знаний в ходе проверки информации о компьютерном преступлении, четкой его квалификации на первичном этапе расследования относительно отдельного состава преступления – несанкционированного распространения или сбыта компьютерной информации с ограниченным доступом (ст. 3622 УК Украины).

Ключевые слова: компьютер, преступление, квалификация, специальные знания, несанкционированное распространение, несанкционированный сбыт, информация, ограниченный доступ.

Pashnev D.V., Rudik M.V. Features of revealing and criminally-legal qualification of crimes which encroach on the computer information with the restricted access.

The article is devoted to the questions of special knowledge application while looking into information on computer crime, its precise qualification at the primary stage of investigation as to the separate corpus delicti - not authorized distribution or selling of the computer information with restricted access (art. 3612 Criminal Code of Ukraine).

Key words: a computer, a crime, the qualification, special knowledge, not authorized distribution, not authorized selling, information, restricted access.

Надійшла до редакції 11.03.2009 р.