УДК 343.98

Б.М. Дердюк
кандидат юридичних наук,
старший викладач
кафедри кримінального права,
процесу та криміналістики
Прикарпатського юридичного
інституту Національного
університету «Одеська юридична
академія»

ПОНЯТТЯ ТА ТЕОРЕТИЧНІ ОСНОВИ КРИМІНАЛІСТИЧНОЇ КЛАСИФІКАЦІЇ КОМП'ЮТЕРНИХ ЗЛОЧИНІВ

Пошуки шляхів підвищення ефективності боротьби зі злочинами, що вчиняються у сфері використання комп'ютерних технологій, ведуться в різних напрямках. Один з них – наукова розробка проблеми. Інтерес учених до цих питань останнім часом зріс. Більш детальне вивчення комп'ютерної злочинності (КЗ) виявляє ряд аспектів цієї проблеми, які найважче піддаються дослідженню. Як правило, вони знаходяться в так званих суміжних галузях науки, на стикові різних наукових дисциплін. Для визначення генезису та механізму розвитку феномена КЗ немаловажне значення має аналіз поняття та видів комп'ютерних злочинів.

Значний вклад у вивчення, розслідування та протидії цим злочинам зробили такі провідні науковці: Т. В. Авер'янова, Б. В. Андрєєв, Ю. М. Батурін, Р. С. Бєлкін, П. Д. Біленчук, О. А. Баранов, М. С. Вертузаєв, Т. В. Варфоломеєва, О. Г. Волєводз, В. О. Голубєв, В. Г. Гончаренко, М. В. Гуцалюк та ін.

Однак комплексна розробка даної проблематики в криміналістичній науці не проводилася. Існує ще багато питань, які потребують більш детального та комплексного вирішення.

Мета нашого дослідження полягає в тому, щоб з огляду на сучасні потреби практики розслідування комп'ютерних злочинів, на основі криміналістичних знань дати кримінально-правову та криміналістичну характеристику поняття та теоретичних основ криміналістичної класифікації комп'ютерних злочинів.

Завдання нашого дослідження полягає у проведенні комплексного аналізу особливостей поняття та теоретичних основ криміналістичної класифікації комп'ютерних злочинів.

Протягом 1990–1997 років науковцями вивчались проблеми, пов'язані з бурхливим розвитком феномена, відомого в усьому світі під назвою «комп'ютерна злочинність». На сьогоднішній день це поняття включає всі протизаконні дії, при яких електронне опрацювання інформації було знаряддям їх учинення або їх об'єктом. Таким чином, у це коло проблем потрапили не лише злочини, безпосередньо пов'язані з комп'ютерами, але й такі як шахрайство з магнітними кредитними картками, злочини у галузі телекомунікацій (шахрайство з оплатою міжнародних телефонних переговорів), незаконне використання банківської мережі електронних платежів, програмне «піратство», шахрайство з використанням ігрових автоматів та багато інших злочинів [1, с. 29].

В науковій літературі виділяють характерні риси комп'ютерної злочинності:

1) має міжнародний характер злочину (виходить за рамки кордону однієї держави);

2) труднощі у визначенні «місцезнаходження злочину»;

3) слабкість зв'язку між ланками в системі доказів;

4) неможливість спостерігати і фіксувати докази візуально;

5) широке використання злочинцями засобів шифрованої інформації [2, с. 4].

У нашій країні комп'ютерна злочинність – поняття досить маловідоме і маловивчене. Але світовій практиці (кримінальній статистиці) це явище знайоме вже близько 50 років. Практично із застосуванням комп'ютерної техніки в різних сферах діяльності людини з'явилась фальсифікація даних, які вводились в ЕОМ. За даними

американського криміналіста О.Б. Паркера злочинність, «пов'язана з системою електронної обробки даних, виникла одночасно з появою комп'ютерної техніки близько 1940 року». Поки що не має єдиної згоди у визначенні цього нового міжнародного явища, назва якого – комп'ютерна злочинність [3, с. 31].

У системі кримінальної поліції ФРН за декілька останніх років було запропоновано ряд кримінально-правових визначень комп'ютерної злочинності.

Наприклад, деякі фахівці вважають, що комп'ютерні злочини – це всі злочинні дії, при яких комп'ютер є знаряддям, засобом чи метою їх здійснення [3, с. 31].

Друге визначення об'єднує під цим терміном всі протизаконні дії, які завдають збитки майну і пов'язані з електронним опрацюванням даних [4, с. 12].

Третє визначення комп'ютерної злочинності окреслює три основні види протизаконних дій: 1) комп'ютерні майнові злочини (наприклад, комп'ютерне шахрайство, саботаж, промисловий шпіонаж); 2) комп'ютерні злочини проти прав особи; 3) правопорушення проти громадських і суспільних правових цінностей (наприклад, проти національної безпеки) [5, с. 18].

Таким чином, під комп'ютерною злочинністю слід розуміти суспільно небезпечну діяльність чи бездіяльність, яка здійснюється з використанням сучасних інформаційних технологій і засобів комп'ютерної техніки з метою спричинити збитки майновим або суспільним інтересам держави, підприємствам, відомствам, організаціям, кооперативам і громадянам, а також правам окремої особи.

Сформульоване визначення комп'ютерної злочинності дозволяє зробити висновок, що це складне нове явище в кримінально-правовій практиці, яке потребує більш досконалого спеціального і систематичного вивчення.

Комп'ютерні злочини – це якісно новий вид злочинності в нашій країні, їх діапазон у світовій практиці надзвичайно широкий. Практично навіть злочинці дилетанти, як і досвідчені злочинці, сьогодні можуть

проникати в різноманітні комп'ютерні системи і автоматизовані банки даних. Цей вид суспільно небезпечного діяння поки що залишається недостатньо вивченим. Тому попереду велика науково-дослідна робота з вивчення цього явища і розробка на цьому ґрунті відповідних законодавчих положень.

Неважко прогнозувати подальше зростання залежності життєдіяльності національної інфраструктури від процесів інформатизації та входження України в єдиний інформаційний простір, поширення криміногенних процесів, пов'язаних з протиправним використанням комп'ютерних технологій або так званими «кіберзлочинами».

Кіберзлочинність (cyber crime) – це явище міжнародного значення, рівень якого знаходиться у прямій залежності від рівня розвитку та впровадження сучасних комп'ютерних технологій, Україні несе за собою мереж та доступу до них. Таким чином, стрімкий розвиток інформатизації в Україні дає можливість використовувати комп'ютерні технології з корисливих та інших мотивів, що певною мірою ставить під загрозу інформаційну безпеку держави.

Згідно з даними щорічного дослідження проблем КЗ, які проводяться Інститутом комп'ютерної безпеки США (Computer Security Institute), сукупний збиток злочинів у сфері використання комп'ютерних технологій за 5 років, з 2005 р. по 2011 р., становить уже більше ніж 1 млрд. дол. США [6, с. 14]. Відповідно до статистичних даних ГУБОЗ Міністерства внутрішніх справ України, на вересень 2011 р. в Україні було порушено 18 кримінальних справ, матеріальний збиток лише по одній з них становить 249 млн. грн. [4, с. 12].

Розділ XVI Кримінального кодексу України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» містить ряд норм, які передбачають кримінальну відповідальність за вчинення злочинів у сфері використання комп'ютерних технологій. До них, зокрема, належить ст. 361 «Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку», ст. 361-1 «Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а

також їх розповсюдження або збут», ст. 361-2 «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», ст. 361-3 «Несанкціоноване втручання в роботу державних електронних інформаційних ресурсів або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних систем, критичних об'єктів національної інформаційної інфраструктури», ст. 361-4 «Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, що оброблюється в державних електронних інформаційних ресурсах», ст. 362 «Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї», ст. 362-1 «Несанкціоновані дії з інформацією, що оброблюється в державних електронних інформаційних ресурсах або інформаційних, телекомунікаційних, інформаційно-телекомунікаційних системах критичних об'єктів національної інформаційної інфраструктури, вчинені особою, яка має право доступу до такої інформації», ст. 363 «Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється», ст. 363-1 «Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку».

Застосування цих спеціальних норм при кваліфікації комп'ютерних злочинів виконує не тільки кримінально-правову функцію, але й здійснює ряд кримінологічних та криміналістичних функцій, у тому числі – забезпечення об'єктивності кримінальної статистики, наукових досліджень, формування емпіричної бази для напрацювання методик виявлення та розкриття злочинів, їх профілактики тощо.

Ефективність боротьби зі злочинами у сфері використання

комп'ютерних систем значною мірою визначається розумінням криміналістичної сутності окремих видів цього злочинного посягання, що зумовлює необхідність їх наукової класифікації.

Більшість фахівців поділяють комп'ютерні злочини на два типи:

1) злочини, в яких об'єктом їх здійснення є ЕОМ: знешкодження або заміна даних, програмного забезпечення та обладнання; розкрадання вхідних, вихідних даних, програмного забезпечення та обладнання; економічне шпигунство та розголошення відомостей, які складають державну чи комерційну таємницю (придбання протиправними засобами або відкриття, переміщення чи використання торгової, комерційної, промислової таємниці без дозволу або інших законних підстав з метою нанесення економічної шкоди особою, яка допущена до таємниці, або одержання протизаконної економічної переваги для інших осіб); інші злочинні діяння цього виду.

2) протизаконні акції, для здійснення яких ЕОМ використовується як знаряддя в досягненні злочинної мети: комп'ютерний саботаж (стирання, приведення у непридатний стан або фальсифікація інформації, інформації, пошкодження засобів інформаційної техніки шляхом втручання до комп'ютерних мереж з метою перешкоджання функціонуванню комп'ютерів чи телекомунікаційних систем); вимагання та шантаж; розтрата; розкрадання коштів; обман споживачів, інвесторів чи користувачів; інші злочини [6, с. 26; 2, с. 4; 3, с. 31; 5, с. 19].

Досить значний досвід криміналістичної класифікації злочинів у сфері комп'ютерної інформації накопичений у ведучих промислово розвинутих державах світу, що вилився в появу так званих «Мінімального списку порушень» і «Необов'язкового списку порушень», розроблених державами-учасниками Європейського співтовариства й офіційно оформлених як «Керівництво Інтерполу по комп'ютерній злочинності» [7, с. 16].

«Мінімальний список порушень» містить вісім основних видів комп'ютерних злочинів: комп'ютерне шахрайство, підробка комп'ютерної інформації, ушкодження даних ЕОМ або програм ЕОМ, комп'ютерний саботаж, несанкціонований доступ, несанкціоноване перехоплення даних, несанкціоноване використання захищених

комп'ютерних програм, несанкціоноване відтворення схем.

«Необов'язковий список» містить у собі чотири види комп'ютерних злочинів: зміна даних ЕОМ або програм ЕОМ, комп'ютерне шпигунство, несанкціоноване використання ЕОМ, несанкціоноване використання захищеної програми ЕОМ.

Однією з найбільш розповсюджених існуючих класифікацій злочинів у сфері комп'ютерної інформації є кодифікатор робочої групи Інтерполу, що був покладений в основу автоматизованої інформаційно-пошукової системи, створеної на початку 90-х рр. Відповідно до названого кодифікатора всі комп'ютерні злочини мають таку класифікацію [3, с. 16]:

Несанкціонований доступ і перехоплення: 1) комп'ютерний абордаж; 2) перехоплення; 3) крадіжка часу; 4) інші види несанкціонованого доступу і перехоплення.

Зміна комп'ютерних даних: 1) логічна бомба; 2) троянський кінь; 3) комп'ютерний вірус; 4) комп'ютерний черв'як; 5) інші види зміни даних.

Комп'ютерне шахрайство: 1) шахрайство з банкоматами; 2) комп'ютерна підробка; 3) шахрайство з ігровими автоматами; 4) маніпуляції з програмами вводу-виводу; 5) шахрайства з платіжними коштами; 6) телефонне шахрайство; 7) інші комп'ютерні шахрайства.

Незаконне копіювання: 1**)** комп'ютерні ігри; 2) інше програмне забезпечення; 3) топологія напівпровідникових пристроїв; 4) інше незаконне копіювання.

Комп'ютерний саботаж: 1) з апаратним забезпеченням; 2) з програмним забезпеченням; 3) інші види саботажу.

Інші комп'ютерні злочини: 1) з використанням комп'ютерних табло оголошень; 2) розкрадання інформації, що складає комерційну таємницю; 3) передача інформації, що підлягає судовому розглядові; 4) інші комп'ютерні злочини.

Виходячи з цієї класифікації можна зрозуміти обґрунтовану позицію багатьох криміналістів, про те, що криміналістична класифікація є основою побудови не тільки криміналістичної характеристики, але і системи криміналістичних методик розслідування злочинів [8, 38].

Виходячи з усього викладеного, криміналістична класифікація комп'ютерних злочинів має такий вигляд:

1) знищення (руйнування) інформації;

2) неправомірне заволодіння інформацією чи порушення права її використання: а) неправомірне заволодіння інформацією як сукупністю відомостей, документів – порушення права володіння; б) неправомірне заволодіння інформацією як алгоритмом (методом перетворення); в) неправомірне заволодіння інформацією як товаром;

3) дія або бездіяльність щодо створення (генерації) інформації з заданими властивостями: а) поширення по телекомунікаційних каналах інформаційно-обчислювальних мереж інформації, що наносить збиток абонентам; б) розробка і поширення комп'ютерних вірусів і інших шкідливих програм для ЕОМ;

4) неправомірна модифікація інформації: а) неправомірна модифікація інформації як сукупності фактів, відомостей; б) неправомірна модифікація інформації як алгоритму; в) неправомірна модифікація інформації як товару з метою скористатися її корисними властивостями.

Розглянутий підхід до побудови класифікації злочинів допомагає більш чітко зрозуміти механізм вчинення комп'ютерних злочинів, а також буде відображати винятково криміналістичні особливості, тому що в його основі лежать особливості здійснення злочинних дій, механізм слідоутворення, тобто усе те, що визначає напрями розслідування комп'ютерних злочинів.

Література

1. Біленчук П. Д. Комп'ютерна злочинність. Навч. посіб. / П. Д. Біленчук. – К.: Атіка, 2012. – 240 с.

2. Голубєв В. Комп'ютерна злочинність / В. Голубєв // Юридичний вісник України. – 2012. – № 6 (9). – С. 1-4.

3. Комп'ютерна злочинність: Навчальний посібник / П. Д. Біленчук, Б. В. Романюк, В. С. Цимбалюк та ін. – К.: Атіка, 2012. – 240 с.

4. Селюк А. В. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. / А. В. Селюк. – К.: Вид-во НА СБУ, 2010. – 124 с.

5. Тищенко Є. Ф. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. / Є. Ф. Тищенко. – К.: Вид-во НА СБУ, 2010. – 124 с.

6. Баранов О. Цифрове законодавство / О. Баранов // Дзеркало тижня. – 2012. – № 20. – 7 черв. – С. 12-17.

7. Колесник В. А. Розслідування комп'ютерних злочинів. Наук.-метод. посіб. / В. А. Колесник. – К.: Вид-во НА СБУ, 2012. – 124 с.

8. Баулін О. В. Спрощене досудове провадження в Україні: історія, сучасність, перспективи: Навч. посіб. / О. В. Баулін, Н. С. Карпов, О. І. Поповченко, Д. О. Савицький. – К., 2008. – 151 с.

Анотація

Дердюк Б.М. **Поняття та теоретичні основи криміналістичної класифікації комп'ютерних злочинів. –** Стаття.

У статті розглядаються питання визначення поняття та теоретичних основ криміналістичної класифікації комп'ютерних злочинів. Автором визначено, що комп'ютерні злочини – це якісно новий вид злочинності в нашій країні, їх діапазон у світовій практиці надзвичайно широкий.

Ефективність боротьби зі злочинами у сфері використання комп'ютерних систем значною мірою визначається розумінням криміналістичної сутності окремих видів цього злочинного посягання, що зумовлює необхідність їх наукової класифікації.

Ключові слова: комп'ютерні злочини, кіберзлочинність, комп'ютерна інформація, комп'ютерні технології, комп'ютер.

Аннотация

Дердюк Б.М. **Понятие и теоретические основы криминалистической классификации компьютерных преступлений. –** Статья.

В статье рассматриваются вопросы определения понятия и теоретических основ криминалистической классификации компьютерных преступлений. Автором определено, что компьютерные преступления – это качественно новый вид преступности в нашей стране, их диапазон в мировой практике неимоверно широк.

Эффективность борьбы с преступлениями в сфере использования компьютерных систем в наибольшей степени определяется пониманием криминалистической сущности отдельных видов этого преступного посягательства, что обуславливает необходимость их научной классификации.

Ключевые слова: компьютерные преступления, киберпреступность, компьютерная информация, компьютерные технологии, компьютер.

Summary

Derdyuk B.M. **The Notion and Theoretical Basis of Forensic Classification of Computer Crimes.** – Article.

This article studies issues concerning the definition of the notion and theoretical basis of forensic classification of computer crimes. The author defines computer crimes to be qualitatively a new type of crime in our country, their range in the world practice is extremely wide.

The effectiveness of combating crimes in the sphere of the use of computer systems is largely determined by understanding of forensic essence of certain types of this crime, which makes it necessary to provide their scientific classification.

Keywords: computer crime, cybercrime, computer information, computer technology, computer.

УДК 343.112

Н.С. Кисляк
здобувач кафедри кримінального права, процесу та криміналістики Прикарпатського юридичного інституту Національного університету «Одеська юридична академія»

ПРАВОВЕ РЕГУЛЮВАННЯ ДІЙ СУДУ З ПЕРЕВІРКИ ЯВКИ УЧАСНИКІВ СУДОВОГО ПРОВАДЖЕННЯ: ПИТАННЯ ТЕОРІЇ ТА ПРАКТИКИ

Постановка проблеми. Як вбачається зі змісту ч. 2 ст. 342 КПК України секретар судового засідання доповідає суду, хто з учасників судового провадження, викликаних та повідомлених осіб прибув у судове засідання, встановлює їх особи, перевіряє повноваження захисників і представників, з'ясовує, чи вручено судові виклики та повідомлення тим, хто не прибув, і повідомляє причини їх неприбуття, якщо вони відомі [1].

Неухильне дотримання вимог кримінального процесуального закону щодо проведення зазначених дій на початку підготовчої частини судового розгляду має важливе значення для провадження наступних його етапів, захисту прав та законних інтересів його учасників.