УДК 343.973:343.72(681.142)

Шапочка Сергій Володимирович –
заступник начальника Спеціального миротворчого центру Національної академії внутрішніх справ

Кримінологічна характеристика шахрайства, що вчиняється з використанням комп'ютерних мереж

Розглядається комплекс взаємопов'язаних чинників, що характеризують шахрайство з використанням комп'ютерних мереж.

Ключові слова: шахрайство з використанням комп'ютерних мереж, комп'ютерне шахрайство, економічне шахрайство.

Постановка проблеми. Система забезпечення інформаційної безпеки є складовою частиною забезпечення національної безпеки держави та однією з найважливіших її функцій. Інформаційна безпека – це стан захищеності людини, суспільства і держави, за якого забезпечується охорона і захист інформаційних ресурсів, мінімізація шкоди від негативних інформаційних впливів, небажаних наслідків використання інформаційних продуктів та інформаційних технологій [1, с. 328].

Комп'ютери та об'єднані інформаційні системи набувають усе більшого значення, суттєво збільшуються й можливості для злочинної діяльності, що здійснюється за допомогою комп'ютерних мереж, із використанням обману чи зловживання довірою.

Стан дослідження. Проблемам вивчення детермінант злочинності присвячено праці Г. М. Горшенкова, О. М. Джужі, А. І. Долгової, І. В. Ільїна, І. І. Рогова, В. С. Устинова, С. С. Чернявського, В. І. Шакуна. Детермінанти шахрайств, що вчиняються з використанням комп'ютерних мереж, на жаль, у кримінології ще не знайшли свого відображення.

В результаті стрімкого розвитку телекомунікацій та інформаційних технологій ми живемо в інформаційному суспільстві, збираємо, систематизуємо, накопичуємо та використовуємо інформацію для важливих соціальних, економічних, культурних, навчально-наукових та інших потреб людства. Важливим інструментом використання досяг-

нень інформаційного суспільства є комп'ютер-комунікатор у всіх його можливих варіаціях. Існує загальновідома класифікація комп'ютерів:

1. за класом виконуваних завдань: універсальні, спеціалізовані;

2. за способом внутрішнього надання даних: аналогові обчислювальні машини (ОМ), гібридні ОМ, цифрові ОМ;

3. за видом робочого середовища: квантовий, оптичний, електронний, біологічний комп'ютер;

4. за призначенням: а) настольні (сервер, робоча станція, персональний, домашній комп'ютер, ігрова приставка); б) інтернет-комп'ютери (нетбук, інтернет-планшет Tablet PC, планшетний нетбук, неттоп); в) консольний комп'ютер;

5. суперкомп'ютери: мейнфрейм, мінісуперкомп'ютер, персональний суперкомп'ютер;

6. за розміром: інтернет-планшет, смартфон, кишеньковий КПК, Handheld, UMPC, ноутбук, субноутбук (ультрабук McBook, iPad, нетбук, смартбук) [2], а також інші високотехнологічні пристрої, що знаходяться у стані розробки та вдосконалення, такі як нанокомп'ютер, розумний пил та ін.

Як бачимо, кількість електронно-технічних засобів, за допомогою яких у широкого загалу є можливість вільно користуватись величезним масивом інформації, маючи при цьому як вибір інструменту, так і відсутність обмеження у просторі й способі виходу у всесвітню мережу Інтернет.

Наш час характеризується становленням інформаційного суспільства, входженням високих технологій у життєдіяльність людей, визначенням векторів розвитку всіх галузей суспільного життя. Комп'ютери, Інтернет, стільниковий зв'язок перебувають у постійному вдосконаленні, стали доступними широким верствам населення, з'явилися нові види послуг, у тому числі електронне листування, електронна торгівля, безготівкові розрахунки за допомогою електронних платіжних систем, проведення Інтернет-аукціонів, лотерей, Інтернет-конференцій тощо [3].

Кількість користувачів всесвітньої мережі Інтернет збільшилася настільки, що стала сягати двохмільярдної позначки, а кількість абонентів стільникового зв'язку досягла п'яти мільярдів абонентів, про це зазначив Генеральний секретар Міжнародного союзу електрозв'язку (ITU) ООН Хамадун Туре (Hamadoun Toure) [4].

Об'єднання комп'ютерних мереж і комунікацій створило умови для виникнення нових, народжених інформаційним суспільством, видів злочинних посягань проти власності – шахрайств, що вчиняються з використанням комп'ютерних мереж. Даному виду злочинів притаманні такі характеристики як велика суспільна небезпека, слабкий контроль з боку суспільства і правоохоронних органів, інтелектуальність, висока

латентність, низький ризик для злочинця і, при цьому, порівняно легкий успіх, конфіденційність дій, анонімність будь-якого користувача.

Боротьба з шахрайствами даного виду повинна включати комплекс соціальних, технологічних і кримінально-правових заходів протидії.

Чезаре Беккаріа, якого недаремно знані науковці вважають одним із основоположників кримінології взагалі й профілактики злочинів зокрема, у своїй книзі "Про злочини і покарання" § XLI Як запобігати злочинам зазначає, що краще попереджувати злочини, аніж карати за них [5, с. 230]. Із розвитком людства діяльність, яка здійснюється у сфері охорони правопорядку, зазнавала значних змін. Заходи кримінального покарання почали співвідноситися із профілактичними заходами, причому в багатьох країнах світу, зокрема і в Україні, саме профілактичним заходам надається пріоритетний напрям [6, с. 11].

Треба відмітити, що в юридичній науці розрізняються наступні кримінологічні групи комп'ютерних злочинів: економічні комп'ютерні злочини; комп'ютерні злочини проти особистих прав і недоторканності приватної сфери; комп'ютерні злочини проти суспільних і державних інтересів.

До комп'ютерних злочинів у сфері економіки відносяться різні форми розкрадання шляхом неправомірного доступу в автоматизовані системи забезпечення діяльності різних установ [7, с. 679].

На думку А. М. Медвєдєва, комп'ютерні злочини у сфері економіки – це кримінально карані діяння, що мають одним із об'єктів злочинного посягання економічні відносини і, як правило, з корисливою спрямованістю [8].

Ми відносимо комп'ютерне шахрайство до економічних комп'ютерних злочинів.

На сьогоднішній день у світовій, а також вітчизняній літературі і практиці не склалось точних визначень "економічної злочинності" та "економічного злочину" [9, с. 25.].

В українському кримінальному законодавстві також немає легального" визначення економічного злочину.

Існують лише кримінологічні визначення економічного злочину та економічної злочинності. Наразі спостерігається плюралізм думок по відношенню до даної проблеми.

Так, наприклад, А. М. Яковлєв вражає, що підставою для включення злочинів до категорії "економічних" є зв'язок із конкретними особливостями економічного, господарського механізму [10, с. 50]. При цьому він зазначає, що суб'єкт злочину в цьому випадку повинен займати конкретне положення в сфері народного господарства, бути учасником економічних відносин чи володіти соціальною роллю, соціальною позицією і ситуацією, які характерні для функціонування пев-

них елементів господарського механізму [10]. Такої точки зору притримується і В. Е. Мельникова [12, с. 4].

І. І. Рогов розуміє економічні злочини, як сукупність кримінологічно однорідних суспільно небезпечних діянь, що посягають на економічну систему держави, вчинені особами, які виконують економічні, господарські функції в державних або суспільних підприємствах, організаціях або у відносинах між громадянами [13, с. 91].

В. В. Колесніков вважає, що економічні злочини – два види злочинів. Це, по-перше, ті, котрі вчиняються у сфері виробництва і зачіпають економічні відносини, пов'язані безпосередньо з виробничою функцією (діяльністю) бізнесу. По-друге, ті, що вчиняються в сфері розподілу, обміну і споживання товарів і послуг [9, с. 64–65].

Приблизно тієї ж точки зору притримуються інші вчені: Г. М. Горшенков [14, с. 3–12], А. Х. Казаріна [15, с. 316], В. Д. Пахомов, П. Г. Пономарьов, А. Н. Чеботарьов [16], В. С. Устінов [11].

Б. Свенсон, шведський кримінолог, визначає економічними злочинами ті, котрі мають у якості мотиву економічну вигоду, повинні носити продовжуваний характер, здійснюватись систематично у рамках легальної господарської діяльності. Також він вважає, що економічні злочини важко виявляються, завдають великих збитків суспільству або групам осіб, мають великий розмах, відносяться до господарської діяльності та вчиняються лише спеціальними суб'єктами, наприклад, підприємцями, комерційними агентами і т. ін. [17, с. 25–26].

Поряд із поняттям економічного злочину в США використовується поняття "білокомірцевий злочин" (white color crime (WCC)). Такий термін уперше у 1939 році ввів американський кримінолог Едвін Сазерленд (Edwin Hardin Sutherland), що розуміє білокомірцевий злочин як злочин, що вчиняється особою, яка заслуговує на довіру, займає високе суспільне положення в процесі здійснення ним своєї професійної діяльності [18].

Г. Маннхейм визначає "білокомірцевий злочин" як правопорушення, вчинене особою не нижче середнього класу, яка займає високе положення, в процесі своєї професійної діяльності з використанням зловживання довірою [19].

За даними вивчення публікацій про Інциденти у Національній Системі Повідомлень (NIRBS), білокомірцеві злочини складають 42 % від загальної кількості всіх правопорушень, пов'язаних із використанням комп'ютера. З таких правопорушень, злочини, пов'язані з розкраданнями, складають найбільшу кількість – близько 31 % [20].

І. В. Ільїн вважає, що комп'ютерне шахрайство є видом економічного шахрайства. Під економічним шахрайством він розуміє: шахрайство, що вчиняється по відношенню до підприємств, установ, орга-

нізацій та інших структур, що є юридичними особами, незалежно від форм власності, організаційно-правової форми, об'єднань (громадян, юридичних осіб), що не є юридичними особами, фізичних осіб, які здійснюють підприємницьку діяльність та офіційно зареєстрованих у якості підприємців, або шахрайство, що вчиняється у процесі економічної діяльності по відношенню до великої групи людей [21, с. 40].

Комп'ютерне шахрайство в більшості випадків є видом економічного шахрайства. Однак, воно може бути і проявом загальнокримінального (звичного) шахрайства.

Під комп'ютерним шахрайством ми розуміємо – заволодіння грошовими коштами або завдання майнової шкоди шляхом використання банкоматів, мережі Інтернет, гральних автоматів, кредитних карт (кардінг) та інших платіжних засобів, а також шляхом маніпуляцій з програмами вводу-виводу і з використанням стільникового телефонного зв'язку.

Комп'ютерне шахрайство, як і комп'ютерні злочини, має дуже високу латентність. Відомими стають лише 10 %–15 % злочинів із усіх учинених. Ми виділяємо кілька причин такої високої латентності даного виду злочину. По-перше, багато організацій намагаються вирішити конфлікт своїми силами, оскільки втрати від розслідування можуть виявитися більшими за суму завданих збитків. Наприклад, вилучення ЕОМ і масиву важливих даних на них може призвести до зупинки роботи підприємства на невизначений час, що є неприйнятним для жодної організації.

По-друге, співробітники служб безпеки різних фінансових установ чи великих компаній приховують прикрі факти злочинних посягань, як доказ власної непрофесійності, а в наслідок цього і неспроможності забезпечити безпеку компанії в повному обсязі, включаючи інформаційну її складову. Цим не лише завдаються збитки компанії, а й створюється прецедент безкарності, приховування факту вчинення злочину самим персоналом, службою, що покликана її забезпечувати і " запрошуються " злочинці до дій знову і знову. Від цього страждають, насамперед, банківські установи, кредитні спілки, відомі компанії із солідним ім'ям і високим рівнем довіри з боку акціонерів, інвесторів, клієнтів, втрата довіри до яких може призвести до втрат, що значно перевищують збитки від шахрайських дій з використанням комп'ютерних мереж аж до втрати позицій у сфері своєї діяльності та банкрутства. Також у ході розслідування може бути виявлена незаконна діяльність підприємства.

По-третє, часто потерпілі просто не здогадуються, що стали жертвою, оскільки відсутні звичні елементи доказової бази – сліди. Виникає запитання, чи мав місце факт вилучення інформації, адже після копіювання все залишилося на місці, а оригінал не пошкоджено, не змі-

нено і т. ін. В іншому випадку виявлені помилки роботи комп'ютерних програм сприймаються як сліди злочинних посягань і навпаки. А тому однією з найбільших складнощів протидії вказаним злочинам є встановлення самого факту вчинення злочину [22].

Сфери діяльності, в яких вчиняються комп'ютерні злочини, різноманітні. Найбільша частина комп'ютерних шахрайств учиняється в кредитно-банківській сфері – близько 70 %. Далі йдуть: злочини в сфері стільникового зв'язку – 20 % і сфера електронної комерції – близько 5 %. Причому, остання сфера діяльності стає все більш привабливою для злочинців завдяки стрімкому розвитку даного ринку, і введення в обіг електронної готівки.

Останнім часом, як свідчить статистика, різко збільшується кількість злочинів, що вчиняються у складі організованих злочинних груп і злочинних організацій.

В кримінологічних дослідженнях останніх років відмічається, що в Україні, як і за кордоном, відбувається активний процес розмивання граней між різними видами злочинів. Злочинці загально-кримінальної спрямованості, організовані злочинні групи та злочинні організації починають використовувати методи, що традиційно використовуються в сфері економіки, нерідко застосовуючи при цьому засоби комп'ютерної техніки, зв'язку і телекомунікацій [23].

Організована злочинність в Україні за короткий період зуміла пройти шлях від розрізнених груп до інтелектуально і технічно забезпечених, добре законспірованих злочинних спільнот. Організована злочинність останнім часом поряд із учиненням загальнокримінальних злочинів інтенсивно інтегрується в економічну сферу з метою отримання високих незаконних доходів, зливаючись при цьому з конгломератом економічної злочинності [23, с. 33.].

Комп'ютерне шахрайство, виходячи з його специфіки, – може бути вчинене з будь-якої точки світу, на нашу думку, є одним із видів транснаціональної організованої злочинності.

Транснаціональна організована злочинність – це добре організовані злочинні співтовариства, що базуються в одній державі, та діють в інших іноземних державах з найбільш сприятливою ринковою кон'юнктурою [24].

Отже, шахрайство, що вчиняється з використанням комп'ютерних мереж, є порівняно новим видом злочину, з високим рівнем латентності, величезною кількістю способів учинення, необмеженими часом і простором можливостями щодо вчинення, використанням специфіки мережі Інтернет – неможливості забезпечення стовідсоткового контролю за користувачами, які мають статус анонімності, несуть мінімальну відповідальність за свої дії та можуть з будь-якого місця, використовуючи комп'ютерно-телекомунікаційні пристрої, вчинити злочин у будь-якій

точці світу, в будь-який час доби. Шахрайство з використанням комп'ютерних мереж – це злочин третього тисячоліття.

Список використаних джерел

1. Правова інформатика : підручник : [у 2-х т.] / Авт. кол. : М. Швець, В. Брижко, Л. Задорожня, В. Цимбалюк та ін. ; [За ред. В. Я. Тація, М. Я. Швеця, Я. Ю. Кондратьєва. – К. : Парламентське видавництво, 2004. – Т. 1. – 416 с.

2. Классификация компьютеров / [Електронний ресурс]. – Режим доступу : http://ru. wikipedia. org/wiki/Шаблон: Виды_компьютеров.

3. Шапочка С. В. Шахрайство у сфері використання всесвітньої мережі Інтернет / С. В. Шапочка // Спеціальна техніка у правоохоронній діяльності : Тези доп. V Міжн. наук.-практ. конф. (Київ, 25 листоп. 2011 р.) – К. : НАВС, 2011. – С. 31–35.

4. Five billion people to use mobile phones in 2010: UN February 15, 2010 / [Електронний ресурс]. – Режим доступу : http://www. physorg. com/news185467439. html.

5. Беккариа Ч. О преступлениях и наказаниях / Ч. Беккариа ; [сост. и предисл. В. С. Овчинского]. – М. : Инфра-М. 2004. – 303 с.

6. Профілактика злочинів : підручник / О. М. Джужа, В. В. Василевич, О. Ф. Гіда та ін. ; [за заг. ред. докт. юрид. наук, проф. О. М. Джужи]. – К. : Атіка, 2011. – 718 с.

7. Криминология / Под ред. А. И. Долговой. – М. : НОРМА, 2002. – 848 с.

8. Медведев А. М. Экономические преступления: понятие и система / А. М. Медведев // Сов. гос-во и право. – 1992. – № 1. – С. 78–87.

9. Колесников В. В. Экономическая преступность и рыночные реформы: политико-экономические аспекты / В. В. Колесников. – СПб. : УЭФ, 1994. – 172 с.

10. Яковлев А. М. Социология экономической преступности / А. М. Яковлев. – М., 1988. – 256 с.

11. Устинов В. С. Криминологические аспекты экономической преступности / Устинов В. С., Арефьев А. Ю. – Н. Новгород, НЮИ МВД РФ, 2000. – 145 с.

12. Мельникова В. Е. Причины и условия хозяйственных преступлений, совершаемых должностными лицами с использованием своего служебного положення : [учеб. пособ.] // В. Е. Мельникова. – М., 1990. – 93 с.

13. Рогов И. И. Экономика и преступность / И. И. Рогов. – Алма-Ата, 1991. – 160 с.

14. Горшенков Г. Н. Экономическая преступность как криминологическая категория : лекция / Г. Н. Горшенков. – Н. Новгород, 1994. – 34 с.

15. Казарина А. Х. Преступность в экономике и её предупреждение / А. Х. Казарина // Криминология : учебник / Под ред. В. Н. Кудрявцева и В. Е. Эминова. – М. : Юристъ, 1997. – 512 с.

16. Пахомов В. Д. Экономическая преступность / Пахомов В. Д., Пономарёв П. Г., Чеботарёв А. Н. // Криминология / Под ред. А. И. Долговой. – М., 1997. – С. 482–485.

17. Свенсон Б. Экономическая преступность : пер. со шведск. / Б. Свенсон. – М., 1987. – 160 с.

18. They Cooked The Books": A Humorous Look at the World of White-Collar Crime / [Електронний ресурс]. – Режим доступу :
http://www. securityinfowatch. ru/view. php? section=books.
19. Mannheim H. Comparative criminology / H. Mannheim. – Boston – New-York – Atlanta – Geneva – Paloalto, 1965. – Vol. II. – P. 491.
20. FBI – WHITE Collar Crimes / [Електронний ресурс]. – Режим доступу :
http://www. fbi. gov.
21. Ильин И. В. Виктимологическая профилактика экономического мошенничества : дис. … канд. юрид. наук / И. В. Ильин. – Н. Новгород, НА МВД РФ, 2000. – 213 с.
22. Шапочка С. В. Кримінологічна характеристика і кримінально-правові заходи боротьби з шахрайствами, що вчиняються з використанням комп'ютерних мереж / С. В. Шапочка // Співпраця поліції/міліції зі службами інтернет-сайтів (аукціонів, соціальних мереж тощо) у боротьбі з інтернет-злочинністю на підставі національного законодавства та законодавства, яке діє у Європейському Союзі : тези доп. Міжн. наук.-практ. конф. (Хмельницький, 16–17 листоп. 2010 р.). – Хм. УМВС України в Хмельницькій обл., 2010. – С. 60–64.
23. Бражник С. Д. Преступления в сфере компьютерной информации : учебно-методическая разработка по спецкурсу / С. Д. Бражник. – Ярославль, 2000. – 54 с.
24. Яблоков Н. П. Транснациональная преступность и некоторые формы международного сотрудничества в борьбе с ней / Н. П. Яблоков // Вестник МГУ : сер. Право. – 2000. – № 4. – С. 17–26.

Рассматривается комплекс взаимосвязанных факторов, которые характеризуют мошенничество с использованием компьютерных сетей.

The complex of the interconnected factors which characterize fraud with the use of computer networks is examined.

Стаття надійшла до редакції журналу 5 грудня 2011 року.