УДК 343.9
DOI https://doi.org/10.32841/2307-1745.2021.54.2.20

Завидняк І. О.,
кандидат юридичних наук, доцент,
докторант кафедри кримінальної юстиції
Державного податкового університету

УЧИНЕННЯ ЕКОНОМІЧНИХ ТРАНСНАЦІОНАЛЬНИХ ЗЛОЧИНІВ ШЛЯХОМ НЕЗАКОННИХ ОПЕРАЦІЙ, ПОВ'ЯЗАНИХ ІЗ НЕПРАВОМІРНИМ ДОСТУПОМ ДО КОМП'ЮТЕРНОЇ МЕРЕЖІ

Анотація. У статті досліджено одну з груп способів учинення економічних транснаціональних злочинів із використанням комп'ютерних технологій, а саме незаконні операції, пов'язані з неправомірним доступом до комп'ютерної мережі. Зазначено, що однією з особливостей способів скоєння економічних транснаціональних злочинів із використанням сучасних комп'ютерних технологій є комплексний характер таких злочинів, тобто основний злочин спрямований проти нормальної економічної діяльності, а підпорядкований злочин – проти засобів комп'ютерної техніки.

Запропоновано таку класифікацію способів учинення неправомірного доступу до комп'ютерної мережі у світлі економічних транснаціональних злочинів: 1) учинення за допомогою комп'ютерних технологій і відповідної техніки економічних злочинів, включаючи злочини, спрямовані на незаконне привласнення або пошкодження самої цієї техніки; 2) незаконне отримання товарів та послуг; 3) несанкціоноване перехоплення інформації; 4) неправомірний доступ до комп'ютерної інформації суб'єктів господарювання та її розкрадання: посягання на комп'ютерну інформацію, що перебуває на одному із серверів глобальної комп'ютерної мережі; посягання на інформацію, що міститься в апаратних засобах некомп'ютерного типу; 5) розкрадання, пов'язані з переказом електронної готівки; 6) шахрайство у сфері електронної торгівлі та інвестування; 7) електронні способи легалізації злочинних доходів; 8) ухилення від оподаткування.

Акцентовано увагу на тому, що наведена класифікація способів неправомірного доступу до комп'ютерної мережі не є вичерпною, що пояснюється доволі стрімким розвитком інформаційної сфери та комп'ютерних технологій зокрема.

Своєю чергою, перераховані способи неправомірного доступу до комп'ютерної мережі поділено на три групи залежно від форми контакту з комп'ютерною технікою, а саме: 1) способи безпосереднього впливу на комп'ютерну інформацію (здійснюються шляхом видачі відповідних команд із того комп'ютера, на якому інформація перебуває); 2) способи опосередкованого доступу до комп'ютера та інформації (проникнення в чужі інформаційні мережі, проникнення в комп'ютерну систему з використанням паролів, підключення до лінії зв'язку законного користувача й отримання тим самим доступу до його системи, використання шкідливих програм для віддаленого доступу до інформації); 3) змішані способи (здійснюються за допомогою і безпосереднього контакту, і віддаленого доступу до комп'ютерної мережі).

Зазначено, що в процесі розслідування економічних транснаціональних злочинів, учинених шляхом проведення незаконних операцій, пов'язаних із неправомірним доступом до комп'ютерної мережі, однією з проблем є виявлення слідів несанкціонованого втручання до комп'ютерних мереж та комп'ютерної інформації.

Ключові слова: економічні злочини транснаціонального характеру, способи вчинення злочинів, сучасні комп'ютерні технології, незаконні операції, неправомірний доступ до комп'ютерної мережі, розслідування злочинів, професійна підготовка злочинців.

Постановка проблеми. Під час розслідування злочинів будь-яких категорій особливо важливим є визначення їх способів учинення. Спосіб учинення злочину є однією з основних категорій як у науці кримінального права, так і в криміналістиці. Разом із тим, як справедливо відзначається в науковій літературі, криміналістичне розуміння способу вчинення злочину набагато ширше, ніж кримінально-правове, оскільки криміналістика покликана надати найбільш ефективні рекомендації щодо розкриття та розслідування злочинів, виявлення в кожному конкретному випадку слідів злочину, встановлення злочинців, забезпечення повноти розслідування та попередження злочинних дій.

Способи вчинення економічних транснаціональних злочинів, скоєних із використанням сучасних комп'ютерних технологій, мають велике значення для розслідування цих протиправних діянь, оскільки вони безпосередньо пов'язані з іншими елементами їх криміналістичної характеристики та відіграють важливу роль як джерело фактичної інформації, що має організаційне й тактичне значення в процесі розслідування та міжнародного співробітництва зокрема. У зв'язку із цим способам учинення економічних транснаціональних злочинів із використанням сучасних комп'ютерних технологій постійно приділяється увага вчених-криміналістів. Але, незважаючи на загальний інтерес до цієї категорії, існує багато розбіжностей у цьому питанні. Так, основні розбіжності стосуються структури та змісту способів учинення злочинів досліджуваної категорії.

Аналіз останніх досліджень і публікацій. Структуру, зміст та сутність способів учинення економічних злочинів, скоєних із використанням сучасних комп'ютерних технологій, досліджували: В.М. Біленчук, В.Б. Вехов, В.О. Голубєв, М.А.Зубань, В.М. Кичак, С.І. Ніколаюк, Д.Й. Никифорчук, Ю.В. Оніщик, Д.В. Пашнєв, М.В. Салтевський, О.О. Семенова, О.В. Тихонова, В.О. Фінагеєв. Але попри значне зацікавлення науковців проблематикою способів учинення економічних транснаціональних злочинів, скоєних із використанням

сучасних комп'ютерних технологій, єдиного розподілу способів учинення даної категорії злочинів на групи не існує.

Мета статті. Визначення сутності, особливостей та специфіки виявлення способів учинення незаконних операцій, пов'язаних із неправомірним доступом до комп'ютерної мережі; визначення класифікації способів учинення даної категорії економічних транснаціональних злочинів.

Виклад основного матеріалу. Способи вчинення економічних транснаціональних злочинів, скоєних із використанням сучасних комп'ютерних технологій, як окремий об'єкт дослідження є малодослідженою сферою криміналістичної методики, оскільки більшість авторів відокремлює способи вчинення економічних злочинів від способів учинення комп'ютерних злочинів. Також уважаємо, що класифікація способів учинення досліджуваних транснаціональних злочинів постійно потребує вдосконалення, тому що пов'язана з видозміною існуючих способів учинення таких протиправних дій відповідно до сучасного стану розвитку комп'ютерних технологій.

Уважаємо, що однією з найважливіших особливостей способів скоєння економічних транснаціональних злочинів із використанням сучасних комп'ютерних технологій є комплексний характер таких злочинів, який убачається у тому, що основний злочин спрямований проти нормальної економічної діяльності (такої, що відповідає інтересам держави, громадян, фінансів, торгівлі), а підпорядкований злочин – проти засобів комп'ютерної техніки. Тож особливості основного предмета злочинного посягання й зумовлюють відповідний спосіб учинення економічних транснаціональних злочинів, зокрема наявність у розпорядженні злочинців певного засобу комп'ютерної техніки.

Так, однією з груп способів учинення економічних транснаціональних злочинів із використанням комп'ютерних технологі, є незаконні операції, пов'язані з неправомірним доступом до комп'ютерної мережі.

У криміналістичній літературі виділяється безліч класифікацій способів учинення злочинів, пов'язаних із неправомірним доступом до комп'ютерної мережі, комп'ютерної інформації зокрема, та пропонуються різноманітні підстави для їх виокремлення.

Проаналізувавши юридичну літературу та матеріали кримінальних проваджень, уважаємо, що більш ґрунтовною та повною є класифікація способів скоєння злочинів, пов'язаних із неправомірним доступом до комп'ютерної мережі, В.Б. Вєхова, яку також в основних аспектах підтримали П.Д. Біленчук, М.А. Зубань, В.О. Голубєв та В.С. Цимбалюк [1, с. 24–25].

Сам автор зазначає, що способи вчинення економічних злочинів, пов'язаних із неправомірним доступом до комп'ютерної мережі, слід класифікувати за роллю комп'ютерної техніки в механізмі такого злочинного діяння: по-перше, коли комп'ютерна техніка виступає в ролі предмета посягання; по-друге, коли зазначена техніка виступає в ролі знаряддя й засобу вчинення злочину. Таким чином, стосовно даної групи діянь предметом посягання буде інформація, що міститься в комп'ютерній мережі, а знаряддям злочину виступає комп'ютерна техніка. Також учений справедливо вважає, що використання зазначених апаратних засобів може здійснюватися не тільки для несанкціонованого доступу, перехоплення і прослуховування, а й для зберігання злочинної інформації.

З огляду на специфіку цієї групи злочинів способи їх учинення умовно можна поділити на три групи, а саме: а) способи, які застосовуються для отримання несанкціонованого доступу до інформації, що перебуває на машинних носіях інформації; б) способи, у яких комп'ютерна техніка і засоби комунікації використовуються як знаряддя і засоби вчинення злочину; в) способи, у яких застосовуються високотехнологічні пристрої з метою незаконного доступу до комп'ютерної інформації, її модифікації або блокування.

Зазначимо, що всі перераховані способи вчинення злочинів, пов'язаних із неправомірним доступом до комп'ютерної мережі, можуть поєднуватися між собою в різноманітних варіаціях. Тому, незважаючи на різноманіття економічних транснаціональних злочинів, учинених із використанням комп'ютерних технологій, практично всі способи їх учинення мають свої індивідуальні ознаки.

Відповідно до цього, пропонуємо таку класифікацію способів учинення неправомірного доступу до комп'ютерної мережі у світлі економічних транснаціональних злочинів, учинених із використанням сучасних комп'ютерних технологій:

1) учинення за допомогою комп'ютерних технологій і відповідної техніки економічних злочинів, включаючи злочини, спрямовані на незаконне привласнення або пошкодження самої цієї техніки;

2) незаконне отримання товарів та послуг;

3) несанкціоноване перехоплення інформації;

4) неправомірний доступ до комп'ютерної інформації суб'єктів господарювання та її розкрадання: посягання на комп'ютерну інформацію, що перебуває на одному із серверів глобальної комп'ютерної мережі; посягання на інформацію, що міститься в апаратних засобах некомп'ютерного типу;

5) розкрадання, пов'язані з переказом електронної готівки;

6) шахрайство у сфері електронної торгівлі та інвестування;

7) електронні способи легалізації злочинних доходів;

8) ухилення від оподаткування.

Хочемо звернути увагу на те, що знищення, блокування, модифікація та копіювання комп'ютерної інформації не виключають здійснення певних самостійних дій, тобто коли несанкціонований доступ до інформації є не лише способом учинення злочину, а й коли ці дії є підготовчими до інших протиправних дій.

Наведена класифікація способів неправомірного доступу до комп'ютерної мережі не є вичерпною, що пояснюється доволі стрімким розвитком інформаційної сфери та комп'ютерних технологій зокрема.

У цілому перераховані способи неправомірного доступу до комп'ютерної мережі можна також поділити на три групи залежно від форми контакту з комп'ютерною технікою, а саме: способи безпосереднього впливу на комп'ютерну інформацію; способи опосередкованого (віддаленого) доступу до комп'ютера та інформації; змішані способи.

Спосіб безпосереднього впливу на комп'ютерну техніку та інформацію здійснюється шляхом видачі відповідних команд із того комп'ютера, на якому інформація перебуває. При цьому можливо проникнення в закриті зони приміщення, у яких провадиться обробка інформації [2, с. 693]. Застосовуючи такий спосіб неправомірного доступу до комп'ютерної мережі, сліди вчинення економічного транснаціонального злочину перебуватимуть тільки в комп'ютерній системі, у пам'яті якої зберігається інформація, яка є предметом протиправного посягання.

Безпосередній доступ до комп'ютерної техніки та інформації може здійснюватися як особами, що мають право доступу до засобів обчислювальної техніки, так й особами, які спеціально проникають у зони з обмеженнями щодо допуску.

Способи опосередкованого (віддаленого) доступу до комп'ютера та інформації, що в ньому зберігається, реалізуються через комп'ютерні мережі з іншого комп'ютера, який перебуває на певній відстані [3, с. 41]. Така група способів включає у себе:

– проникнення в чужі інформаційні мережі шляхом автоматичного перебору абонентських номерів із подальшим з'єднанням із певним комп'ютером (перебирання здійснюється доти, доки на протилежному кінці лінії не «відізветься чужий» комп'ютер) [4, с. 93];

– проникнення в комп'ютерну систему з використанням паролів;

– підключення до лінії зв'язку законного користувача й отримання тим самим доступу до його системи;

– використання шкідливих програм для віддаленого доступу до інформації.

Такий спосіб віддаленого несанкціонованого доступу до комп'ютерної техніки та інформації як протиправний доступ до програмного та технічного захисту можна легко виявити, тому подібний «електронний злам» здійснюється з декількох робочих місць: у зазначений час декілька (більше десяти) персональних комп'ютерів одночасно роблять спробу несанкціонованого доступу. Це може призвести до того, що декілька «атакуючих» комп'ютерів відсікаються системою захисту, а інші – отримують потрібний доступ [4, с. 93].

Доволі цікавим способом віддаленого впливу на комп'ютерну техніку є протиправне проникнення в комп'ютерну систему з використанням чужих паролів. Застосовуючи такий спосіб, зловмисники здійснюють доступ до комп'ютерної системи, використовуючи логін і пароль користувача.

Виокремлюють три прийоми формування паролів, які найчастіше застосовують злочинці. Так, зловмисники можуть використовувати спеціальні технічні або програмні засоби для зчитування пароля; можуть застосовувати «інтелектуальний» підбір необхідного пароля, використовуючи наявні «словники» найпоширеніших паролів; можуть уводити в оману власника з метою схилити його до повідомлення пароля.

Такий спосіб віддаленого доступу до комп'ютерної системи та комп'ютерної інформації, як перехоплення, поділяється на безпосереднє та електромагнітне перехоплення.

Безпосереднє перехоплення здійснюється шляхом фізичного підключення до телекомунікаційного обладнання, каналів зв'язку, комп'ютерної системи законного користувача й одержання тим самим доступу до його системи [4, с. 95]. Використовуючи такий спосіб протиправного посягання, злочинець має можливість впливати на засоби комп'ютерної техніки у цілому, носіїв комп'ютерної інформації, систему санкціонування доступу до них, телекомунікаційне обладнання, канали зв'язку і на саму комп'ютерну інформацію. Безпосереднє підключення до каналу зв'язку здійснюється злочинцем за допомогою технічних засобів та спеціального обладнання, після чого вся інформація фіксується на матеріальному носії та переводиться у загальну форму будь-якими доступними програмними засобами [5, с. 45].

Електромагнітне перехоплення відбувається за допомогою сучасних технічних засобів, які дають змогу отримати інформацію, перебуваючи на достатній відстані від об'єкта перехоплення. Воно полягає у відновленні інформації, що розповсюджується за рахунок фізичних явищ, котрі виникають у процесі функціонування технічних засобів обробки інформації (телекомунікаційних каналів, центрального процесора, принтера) [5, с. 46].

Третьою групою способів неправомірного доступу до комп'ютерної мережі залежно від форми контакту з комп'ютерною технікою є змішаний спосіб учинення злочину, який може здійснюватися за допомогою і безпосереднього контакту, і віддаленого доступу до комп'ютерної мережі.

До змішаних способів можна віднести:

а) несанкціоноване введення до чужої програми команд, за допомогою яких здійснюються нові, незаплановані функції, зберігаючи при цьому її працездатність (програма виконує копіювання файлів, але одночасно знищує дані про фінансову діяльність суб'єкта господарювання) [4, с. 96];

б) протиправну зміну програм у результаті таємного розміщення в програмі набору команд, які спрацьовують за певних умов через будь-який час (як тільки програма незаконно перерахує грошові кошти на так званий підставний рахунок, вона самознищиться і знищить усю інформацію про цю операцію) [4, с. 96];

в) здійснення протиправного доступу до баз даних законного користувача через слабкі місця в системах захисту. У разі їх виявлення з'являється можливість читати й аналізувати інформацію, що міститься в системі, копіювати її, повертатися до неї за необхідності [30, с. 97];

г) використання помилок логіки побудови програми та знаходження «прогалин». При цьому програма «розривається», і до неї вводиться необхідна кількість певних команд, які допомагають їй здійснювати нові, незаплановані функції, одночасно зберігаючи при цьому її попередню працездатність. Таким чином, злочинці переказують кошти на підставні рахунки та отримують інформацію про нерухомість та персональні дані особи тощо [6, с. 17].

Як бачимо, під час виявлення, розкриття та розслідування економічних транснаціональних злочинів, учинених шляхом проведення незаконних операцій, пов'язаних із неправомірним доступом до комп'ютерної мережі, актуальною є проблема виявлення слідів несанкціонованого втручання до комп'ютерних мереж та комп'ютерної інформації. У зв'язку із цим під час розслідування таких злочинів особливо важливим є виявлення не лише фізичних слідів, а й нетрадиційних слідів комп'ютерних злочинів, які несуть необхідну доказову інформацію.

Висновки. Ураховуючи вищевикладене, зауважимо, що вчинення економічних транснаціональних злочинів, скоєних із використанням сучасних комп'ютерних технологій, неможливе без ретельної попередньої підготовки до вчинення злочину, вивчення обстановки, створення передумов для його вчинення та приховування слідів злочину.

Особливістю початкового етапу цієї категорії злочинів є невразливість від переслідування правоохоронних органів, служб безпеки та фінансової розвідки, оскільки такий етап злочинної діяльності зазвичай маскується під правовідносини за участю суб'єктів господарювання, правомірні дії громадян або ж виконання своїх обов'язків працівниками банку [7, с. 74].

Також важливим елементом у процесі вчинення економічних транснаціональних злочинів даної категорії є рівень

професійної підготовки злочинців, а саме: навички у підробці документів, навички у застосуванні комп'ютерних та інформаційних технологій, знання в економічній, фінансово-кредитній або податковій сферах [8, с. 181].

Література:

1. Біленчук П.Д., Зубань М.А. Комп'ютерні злочини: соціально-правові і кримінолого-криміналістичні аспекти : навчальний посібник. Київ : Українська академія внутрішніх справ, 1994. 72 с.
2. Справочник следователя / В.Н. Григорьев, А.В. Победкин, В.Н. Яшин, Ю.В. Гаврилин. Москва : ЭКСМО, 2008. 752 с.
3. Козак Н.С. Криміналістичні прийоми, способи і засоби виявлення, розкриття та розслідування комп'ютерних злочинів : дис. … канд. юрид. наук : 12.00.09. Ірпінь, 2011. 229 с.
4. Голубєв В.О. Розслідування комп'ютерних злочинів : монографія. Запоріжжя : ЗІДМУ, 2003. 296 с.
5. Пашнєв Д.В. Використання спеціальних знань при розслідуванні злочинів, вчинених із застосуванням комп'ютерних технологій : дис. … канд. юрид. наук : 12.00.09. Харків, 2007. 228 с.
6. Протидія злочинам, що вчиняються у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж : науково-практичний посібник / С.І. Ніколаюк, Д.Й. Никифорчук, О.В. Тихонова, С.В. Шутенко та ін. Київ : КНТ, 2007. 196 с.
7. Фінагеєв В.О. Способи вчинення злочинів, пов'язаних із використанням засобів доступу до банківських рахунків. *Науковий вісник Національної академії внутрішніх справ*. 2016. № 1(98). С. 63–82.
8. Завидняк І.О. Особливості криміналістичної характеристики економічних транснаціональних злочинів, вчинених із використанням сучасних комп'ютерних технологій. *Аналітично-порівняльне правознавство*. 2021. № 3. С. 178–183.

Zavydnyak I. Committing economic transnational crimes through illegal operations involving unauthorized access to a computer network

Summary. The article explores one of the groups of methods for committing economic transnational crimes using computer technologies, namely: illegal operations associated with illegal access to a computer network. It is noted that one of the features of the methods of committing economic transnational crimes using modern computer technologies is the complex nature of such crimes, that is, the main crime is directed against normal economic activity, and the subordinate crime is directed against computer equipment.

The following classification of ways of committing illegal access to a computer network in the light of economic transnational crimes is proposed: 1) commission of economic crimes using computer technologies and related equipment, including crimes aimed at misappropriation or damage to this equipment itself; 2) illegal receipt of goods and services; 3) unauthorized interception of information; 4) illegal access to computer information of business entities and its theft: encroachment on computer information located on one of the servers of the global computer network; infringement of information contained in non-computer type hardware; 5) theft associated with the transfer of electronic cash; 6) fraud in the field of electronic commerce and investment; 7) electronic methods of money laundering; 8) tax evasion.

Emphasis is placed on the fact that the classification of methods of unauthorized access to the computer network is not exhaustive, due to the rather rapid development of the information sphere and computer technology in particular.

In turn, these methods of unauthorized access to the computer network are divided into three groups depending on the form of contact with computer technology, namely: 1) ways to directly influence computer information by issuing appropriate commands from that computer. the user on which the information is located); 2) methods of indirect (remote) access to computers and information (intrusion into other people's information networks, intrusion into a computer system using passwords, connecting to a legitimate user's communication line and thus gaining access to his system, use of malicious programs for remote access to information); 3) mixed methods (carried out by direct contact and remote access to a computer network).

It is noted that in the process of investigating economic transnational crimes committed through illegal operations related to illegal access to the computer network, one of the problems is the problem of identifying traces of unauthorized interference with computer networks and computer information.

Key words: economic crimes of a transnational nature, methods of committing crimes, modern computer technology, illegal operations, illegal access to a computer network, investigation of crimes, professional training of criminals.