Дмитрук М. М.
доцент кафедри кримінального права
Національного університету «Одеська юридична академія»,
кандидат юридичних наук, доцент

ТИПОВІ НАСЛІДКИ «НЕСАНКЦІОНОВАНОГО ВТРУЧАННЯ В РОБОТУ ЕОМ, АВТОМАТИЗОВАНИХ СИСТЕМ, КОМП'ЮТЕРНИХ МЕРЕЖ ЧИ МЕРЕЖ ЕЛЕКТРОЗВ'ЯЗКУ»

За останні декілька десятиліть життя більшості людей та суспільства, в цілому, було настільки автоматизовано, що будь-яка звичайна діяльність людини не уявляється без персональних комп'ютерів, комп'ютерних мереж, мереж електрозв'язку.

Тотальна опосередкованість всіх суспільних відносин інформаційними технологіями призвела до збільшення кількості злочинів, які вчиняються за допомогою ЕОМ, автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку, а також — до збільшення кількості суспільно небезпечних діянь, які вчиняються як за допомогою ЕОМ, автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку так і щодо суспільних відносин, які виникають у сфері використання ЕОМ, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку.

В теорії кримінального права існує дискусія щодо термінів та понять («комп'ютерні злочини», «злочини у сфері ІТ», «кіберзлочини») у визначенні системи діянь, які вчиняються за допомогою ЕОМ, автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку та інших понять, які використовуються для визначення ознак злочинів у сфері ІТ (Карчевский Н. Киберпреступление или преступление в сфере использование информационных технологий? // Кібербезпека в Україні: правові та організаційні питання : матер. всеукр. наук.-практ. конф., м. Одеса, 21.10.2016 р. — О.: ОДУВС, 2016. — С. 10-15.). Інші вчені, наприклад, В. М. Бутузов, звертають увагу на необхідність системно-структурної протидії комп'ютерним злочинам, виділяючи два основних аспекти: 1) як множинності взаємодіючих складових (об'єктів, суб'єктів, заходів протидії тощо); 2) у рамках системи протидії загальній злочинності шляхом визначення особливостей протидії комп'ютерній злочинності (Бутузов В. М. Системно-структурний аналіз як метод дослідження комп'ютерної злочинності // Правова інформатика 2011. — № 1. — С. 67-71). Зазначена проблематика є актуальною, проте стан узагальнення судової практики та постійні зміни в інформаційному законодавстві України вимагають приділення більшої уваги ознакам окремих злочинів у сфері ІТ, зокрема, несанк-

ціонованому втручанню в роботу ЕОМ. Розглянемо деякі проблеми у визначенні ознак об'єктивної сторони вказаного злочину.

Поширеною є думка, що об'єктивна сторона несанкціонованого втручання в роботу ЕОМ, автоматизованих систем та комп'ютерних мереж, мереж електрозв'язку характеризується такими наслідками, як: 1) витік; 2) втрата; 3) підробка; 4) блокування інформації; 5) спотворення процесу обробки інформації; 6) порушення встановленого порядку її маршрутизації. Зміст вказаних наслідків полягає у наступному.

1. *Витік* визначається як результат дій, внаслідок яких інформація в системі стає відомою чи доступною фізичним та/або юридичним особам, що не мають права доступу до неї (ст. 1 Закону України «Про захист інформації в інформаційно-телекомунікаційних системах»). Наприклад, Особа 3 з метою незаконного отримання та подальшого використання інформації з банківських карток громадян, несанкціоновано втрутилась в роботу ЕОМ, встановивши на банкоматі, несанкціоновані зчитувальні пристрої для зняття інформації з банківських платіжних карток (вирок Приморського райсуду м. Одеса від 27.06.2013 р., кримінальне провадження № 522/14602/13-к, N 1-кп/522/374/13) тобто витік у судовій практиці трактується як зняття та зчитування інформації. Проте «зняття» та «зчитування» це дії, а «витік» у більшості навчальній та науковій літературі трактується як «наслідок» несанкціонованого втручання (Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. — [2-ге вид.] — К. : «ВД «Дакор», 2013. — 606 с.).

2. *Втрата* інформації визначається як «дія, внаслідок якої інформація в автоматизованій системі перестає існувати для фізичних або юридичних осіб, які мають право власності на неї в повному чи обмеженому обсязі» (ст. 1 Закону України «Про захист інформації в автоматизованих системах» в редакції до 27.03.2014 р.).

Наприклад, Особа С. працюючи інженером програмного забезпечення банку маючи намір «знищити» інформацію на його сервері розмістила шкідливе програмне забезпечення в активному стані у каталогах операційної системи серверу банку, але реалізувати до кінця свій умисел не змігла, оскільки в день подання заяви про звільнення їй було відмовлено в допуску до робочого місця і сервера (Судова практика розгляду справ про злочини у сфері використання ЕОМ ...: Узагальнення опрацьовано суддею ВС України М. І. Грицівим та головним консультантом В. В. Антощуком). Вказане діяння є закінченим замахом, вчинене у сукупності із діянням передбаченим ст. 361-1 КК України, а тлумачення «втрати» як «знищення» свідчить, що вказана ознака в судовій практиці дійсно відіграє роль «злочинного наслідку».

3. *Підробкою* є вплив на носій інформації, що передається мережею електрозв'язку у результаті якого абонент отримує відомості, які не збігаються з тими, що було йому надіслано (Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. — [2-ге вид.] — К.: «ВД «Дакор», 2013. — с. 607). Наприклад, Особа 1 несанкціоновано втрутилась у роботу автоматизованої системи комп'ютерного програмного комплексу «Єдина система статистики та аналізу роботи органів прокуратури України» шляхом надання незаконних вказівок чим підробила відомості про своєчасне подання апеляційної скарги (Вирок Печерського райсуду м. Києва від 4.03.2015 р. по справі N 757/3752/15-к). При цьому, підробка згідно ч. 1 ст. 358 КК України у цьому ж навчальному підручнику визнано як злочин із формальним складом, який є закінченим з моменту вчинення дій, які альтернативно становлять його об'єктивну сторону (Кримінальне право (Особлива частина) : підручник / за ред. О. О. Дудорова, Є. О. Письменського. — [2-ге вид.] — К.: «ВД «Дакор», 2013. — с. 590). Незрозуміло чому в одному випадку підробка — це злочинний наслідок, а в іншому випадку характеристика дій винуватої особи.

4. *Блокування інформації в системі* визначається як «дії, внаслідок яких унеможливлюється доступ до інформації в системі» (Закон України «Про захист інформації в інформаційно-телекомунікаційних системах»). Громадянин Ч., використовуючи телефонний пристрій для здійснення несанкціонованого втручання в роботу мереж електрозв'язку, через електрощитові, що розташовані в під'їздах багатоповерхових будинків, не маючи на це дозволу, підключився до мережі електрозв'язку чим блокував доступ громадянину Г. як абоненту до мережі електрозв'язку (Узаг. судової практики розгляду місцевими судами м. Харкова та Харківської обл. кримінальних справ та проваджень про злочини у сфері використання ЕОМ, систем та КМ і МЕ за період 2012-2014 рр.: http://clc.to/S7EKDg). Вказана ознака більше характеризує діяння, а ніж злочинний наслідок.

5. *Спотворення процесу обробки комп'ютерної інформації.* Поняття вказаного наслідку у інформаційному законодавстві відсутнє. Проте в судовій практиці цей злочинний наслідок «несанкціонованого втручанні в роботу мереж електрозв'язку» розкривається через поняття «порушення встановленого порядку обробки інформації» у вигляді «монтажу» шкідливих програмних пристроїв.

Особа В. за матеріальну винагороду встановила громадянину З. обладнання (супутникову антену), яке призначене для прийому супутникового радіосигналу, до якого підключила технічні засоби (модифікований роутер, конвертор), що дозволяли здійснити несанкціоноване декодування та послідуючий перегляд кодованих телепрограм

з обмеженим доступом (Узаг. судової практики розгляду місцевими судами м. Харкова та Харківської обл. з кримінальних справ та проваджень про злочини у сфері використання ЕОМ, систем та КМ і МЕ за період 2012-2014 рр.: https://hra.court.gov.ua/sud2090/inf_court/generalization/uzag15/).

6. *Порушення встановленого порядку маршрутизації комп'ютерної інформації.* Маршрутизацію є обмін даними при виконанні операцій, у тому числі щодо переказу коштів, між учасниками платіжної системи. (ст. 1.18-2 Закону України «Про платіжні системи та переказ коштів в Україні»), а порушення роботи автоматизованої системи — це «дії або обставини, які призводять до спотворення процесу обробки інформації». Вказані визначення щодо порушення встановленого порядку маршрутизації комп'ютерної інформації свідчать, що «спотворення» і є «порушенням порядку обробки комп'ютерної інформації». Щодо відображення в судовій практиці цього «злочинного наслідку» можна навести наступний приклад. Особа 2 будучи відповідальною за побудову та налаштування каналів зв'язку для ДМС України і ДП «Документ» не санкціоновано змінила налаштування та конфігурацію маршрутизатора шляхом підключення Центру обробки даних Єдиного державного демографічного реєстру ДМС України через мережу Інтернет «напряму» в обхід Національної системи конфіденційного зв'язку, чим вчинила несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж та мереж електрозв'язку ДМС України, що призвело до спотворення процесу обробки інформації та до порушення встановленого порядку маршрутизації інформації (вирок Солом'янського райсуду м. Києва від 22.01.2018 р., по справі № 760/1167/18). Таке формулювання ознак об'єктивної сторони досліджуваного злочину свідчить, що «порушення встановленого порядку маршрутизації комп'ютерної інформації» характеризує те яким чином здійснюється «несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку» тобто є способом вчинення діяння, а не його «злочинним наслідком».

Отже, дослідження типових наслідків несанкціоноване втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, на нашу думку, вказує на помилкове визначення значення «витоку», «підробки», «блокування інформації», «спотворення процесу обробки інформації», «порушення встановленого порядку маршрутизації інформації»: вказані ознаки характеризують спосіб вчинення діяння, а не його злочинний наслідок.

«Втрата комп'ютерної інформації» є злочинним наслідком несанкціонованого втручання в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України).