

УДК 343.3/.7

Віта Петрівна СОЛОГУБ,

*студент групи ПБП-16-6 навчально-наукового інституту права
Національного університету державної фіскальної служби України;*

Тарас Валерійович ШВОРАК,

*студент групи ПБП-16-6 навчально-наукового інституту права
Національного університету державної фіскальної служби України;*

Микола Васильович КОВАЛЬ,

*кандидат юридичних наук, професор,
професор кафедри адміністративного права і процесу та митної справи
Національного університету державної фіскальної служби України*

ОСОБЛИВОСТІ КІБЕЗЛОЧИННОСТІ В УКРАЇНІ

Одним з досягнень науково-технічної думки людини стало впровадження в управлінський процес та інші сфери життя суспільства електронно-обчислювальної техніки, без якої зберігання, обробка та використання величезної кількості найрізноманітнішої інформації не було неможливим. Це досягнення принесло неоціненну користь у розвиток науки, техніки та інших галузей знань.

Однак вигоди, які можна отримати завдяки використанню цієї техніки, стали використовуватися і в злочинних цілях. Так, з'явився новий вид злочинної діяльності – кіберзлочини – суспільно небезпечні наслідки від вчинення яких не йшли в порівняння зі шкодою від інших злочинів. За оцінками експертів правоохоронних органів країн Центральної та Східної Європи з питань боротьби з комп'ютерною злочинністю, прибутки злочинців від злочинів у сфері використання електронно-обчислювальних приладів посідають третє місце після доходів наркоторговців та від продажу зброї, а завдані збитки вже зараз оцінюються мільярдами доларів.

Під кіберзлочинністю слід розуміти сукупність злочинів, що вчинюються у віртуальному просторі за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Криміналістична особливість кіберзлочинів становить в тому, що розслідування та розкриття цих злочинів неможливе без застосування та використання комп'ютерних технологій. Це пов'язано з необхідністю відшукування, фіксування, вилучення та збирання доказів в електронній формі. Також комп'ютерні технології широко використовуються для проведення оперативно-розшукових заходів.

Термін «кіберзлочинність» часто вживається поряд з терміном «комп'ютерна злочинність», причому нерідко ці поняття використовуються як синоніми. Дійсно, ці терміни дуже близькі один одному, але все-таки, не синонімічні. Поняття «кіберзлочинність» (в

англомовному варіанті – *cybercrime*) ширше, ніж «комп'ютерна злочинність» (*computer crime*), і більш точно відображає природу такого явища, як злочинність в інформаційному просторі.

Так, Оксфордський тлумачний словник визначає приставку «*cyber*» як компонент складного слова. Її значення – що відноситься до інформаційних технологій, мережі Інтернет, віртуальної реальності. Практично таке ж визначення дає Кембриджський словник. Таким чином, «*cybercrime*» – це злочинність, пов'язана як із використанням комп'ютерів, так і з використанням інформаційних технологій і глобальних мереж. У той же час термін «*computer crime*» в основному стосується злочинів, які скоєні щодо комп'ютерів або комп'ютерних даних. Ідея поділу термінів «кіберзлочинність» і «комп'ютерна злочинність» й використанню саме першого терміну і закріплена в міжнародному праві. Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність, вживши саме термін «*cybercrime*», а не «*computer crime*» [2]. В даний же час офіційне визначення кіберзлочинності на міжнародному рівні відсутнє.

Хоча аналіз національного законодавства України, що регулює суспільні інформаційні відносини, дозволяє стверджувати, що наша держава вживає необхідних заходів, спрямованих на профілактику та протидію комп'ютерної злочинності. Прикладом цьому може служити Указ Президента від 31 липня 2000 року «Про заходи розвитку національної складової глобальної інформаційної мережі Internet та забезпечення широкого доступу до цієї мережі в Україні», а також Розділ 16 «Злочини у сфері використання ЕОМ, систем та комп'ютерних мереж» чинного Кримінального кодексу України. Але цього виявляється не достатньо для протидії кіберзлочинності в нашій державі.

Тому, однією з проблем, на яких доцільно акцентувати увагу є проблема понятійно-категорійного апарату. Термін «кіберзлочин», яким зараз у наукових колах прийнято позначати специфічні види злочинів, віднесених до так званої «кібернетичної сфери» набув на пострадянському просторі достатньо широкого вжитку, не маючи сформованого загальноновизнаного юридичного наповнення. Залишається не вирішеною проблема не тільки встановлення співвідношення «кіберзлочину» з такими правовими категоріями як «комп'ютерний злочин», «злочин у сфері комп'ютерної інформації», «злочин у сфері використання комп'ютерів», «злочин у сфері використання інформаційних технологій», або із законодавчим в Україні поняттям «злочин у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», а й концептуального визначення місця «кіберзлочину» в системі протиправних діянь передбачених національним законодавством: як окремого виду цих діянь, як специфічної форми їх скоєння, як того і іншого. Все це ставить під великий сумнів доцільність і можливість нормативного визначення

кіберзлочину і впровадження його як окремого виду злочинів кримінальним правом [3, с. 189].

Проблема профілактики кіберзлочинності в Україні – це комплексна проблема. Сьогодні закони мають відповідати сучасним реаліям, а не рівню розвитку чи то науки, чи то розумінняправляючої групи щодо пріоритетності тих чи інших національних інтересів. Розвиток технологій, кіборгізація та подальше впровадження штучного інтелекту в наше життя це вже не майбутнє, а сьогодення. Тому будь-які подальші рефлексії з цього питання лишень затягуватимуть час тоді, коли відносини у кіберпросторі розвиваються швидкоплинно і нелінійно.

Пріоритетним напрямком є також організація взаємодії і координація зусиль правоохоронних органів, спецслужб, судової системи, забезпечення їх не лише найсучаснішою матеріально-технічною базою, а й розвиток акмеологічних засад кібербезпекової освіти, підготовка відповідних фахівців. Жодна держава сьогодні не в змозі самотужки протистояти кіберзлочинності самотійно. Нагальною є необхідність активізації участі України в інтересах національної безпеки в різноманітних системах міжнародної та глобальної інформаційної безпеки, посилення співпраці з всесвітніми інформаційними гігантами: Facebook, Apple, Google із залученням широкого кола аналітичних центрів, в тому числі недержавних та інститутів громадянського суспільства.

Боротьба з кіберзлочинністю неможлива без глибокого розуміння і правових проблем регулювання інформаційних мереж. Саме аналіз взаємозв'язку між технічними характеристиками мережі і зумовленими цими характеристиками правовими і соціальними труднощами, з якими стикаються законодавці та правоохоронні органи, є першим кроком до можливого вироблення механізмів адекватного реагування на розвиток і зростання кіберзлочинності. Механізми контролю, запобігання та розслідування посягань у кіберпросторі дуже обмежені як соціально, так і технологічно.

Тому, можна зробити висновок, що відсутність уніфікованого визначення «кіберзлочинності» створює сприятливі умови для виникнення та неможливості вирішення низки проблем. Невідповідність існуючого законодавства сучасним загрозам та небезпекам у кібернетичній сфері також сприяють виникненню та розвитку кіберзлочинності. Суб'єктом даного виду злочинів є фізична осудна людина, об'єктом є, перш за все, кібербезпека. Кіберзлочини найчастіше ставлять під загрозу життєво важливу інфраструктуру. Кіберзлочини вчиняються за допомогою комп'ютерних систем або шляхом використання комп'ютерних мереж та інших засобів доступу до віртуального простору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних.

Список бібліографічних посилань

1. Бельський Ю. Щодо визначення поняття кіберзлочину. *Юридичний вісник*. 2014. № 6. С. 414-418.
2. Аль-мзіраві Н. А., Мисливий В. А. Поняття та сутність кібернетичної злочинності // Науково-практична інтернет-конференція. 08.12.2016. URL: http://legalactivity.com.ua/index.php?option=com_content&view=article&id=1425%3A091216-07&catid=170%3A5-1216&Itemid=211&lang=en (дата звернення: 31.10.2018).
3. Тихомиров О. О. Кіберзлочин: теоретико-правові проблеми // 36. матеріалів наук.-практ. конф. «Інформаційна безпека: виклики і загрози сучасності»; 5 квітня 2013 р. К. : Наук.-вид. центр НА СБ України. 2013. С. 179-182
4. Бугузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : монографія. К. : КИТ, 2010. 148 с.

Одержано 01.11.2018

УДК 004.056.53

Микола Олександрович УДЯНСЬКИЙ,

магістр факультету № 6

Харківського національного університету внутрішніх справ

ДЕЯКІ ТЕНДЕНЦІЇ ПОШИРЕННЯ ЗЛОЧИНІВ З ВИКОРИСТАННЯМ КРИПТОВАЛЮТ

Інформаційні технології стали постійним супутником сучасної людини не тільки на робочому місці, вони увійшли майже в усі сфери людського життя. Поширення нових інформаційних технологій, в основі яких лежить широке використання комп'ютерної техніки і засобів комунікацій, оптимізації та автоматизації процесів у всіх без винятку сферах життєдіяльності, призвело разом з цим до нівелювання меж і переплетення національних економік і національних інфраструктур країн світу.

Більш того, зазначені тенденції привели до формування єдиного світового інформаційного простору, де кожен може отримати доступ до будь-якої інформації в будь-якій точці планети, здійснювати дистанційно управління власними активами і активами компанії, укладати господарські договори з іноземними суб'єктами господарювання без необхідності особистого контакту і т.д.

Все це призводить до зростання такого явища як кіберзлочинність, а поява такого інструменту для анонімних розрахунків як криптовалюта ще більш загострило і так не просту ситуацію в боротьбі з цим видом злочинів.

Упродовж останнього року, велика кількість інтернет-видань стала отримувати скарги від користувачів, що їх сторінки стали дуже повільними. З'ясувалося, що винен у цьому скрипт-майнер, який було вбудовано в сайти цих відань для видобутку криптовалюти