Бура Тетяна Вадимівна
Миколаївський інститут права
Національного університету «Одеська юридична академія»
Білик Наталя Михайлівна
Кандидат технічний наук, доцент
Миколаївський інститут права
Національного університету «Одеська юридична академія»

ПОНЯТТЯ ТА КРИМІНОЛОГІЧНА ХАРАКТЕРИСТИКА КІБЕРЗЛОЧИННОСТІ

Під кіберзлочинністю треба розуміти сукупність злочинів, які вчинюються у віртуальному просторі за допомогою різних 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.

Поняття «кіберзлочинність» часто вживається поряд з поняттями «комп'ютерна злочинність», «злочинність у сфері високих (інформаційних) технологій», «високотехнологічна злочинність». Кримінальний кодекс України оперує терміном «злочини у сфері використання електронно-обчислюваних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку». Серед вищезазначених, поняття «кіберзлочинність» є найширшим поняттям та охоплює найбільше коло злочинних посягань у віртуальному середовищі, а також його використання передбачає міжнародне законодавство. Так, Рада Європи в листопаді 2001 року прийняла Конвенцію про кіберзлочинність. Тому слід вважати обґрунтованим вживання саме цього терміну для кримінологічного дослідження цього різновиду злочинності [1].

Слід звернути увагу перш за все на те, що засобом для здійснення кіберзлочину є комп'ютер, а саме комп'ютерні мережі чи комп'ютерні системи. З кримінально-правової точки зору він характеризується прямим умислом, майже виключається можливість недбалості. Також суб'єктом виступає осудна фізична особа. Даний вид злочину спрямований на порушення діяльності інформаційних та комп'ютерних систем, порушення авторських і суміжних прав, незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення та інші [2].

Наслідки кіберзлочинності зачіпають не лише інтереси окремих осіб, що стали жертвами, але й компанії, організації, уряди і суспільство в цілому. Кіберзлочини найчастіше ставлять під загрозу життєво важливу як інформаційну, так і взагалі критичну інфраструктуру, яка в багатьох країнах не контролюється публічним сектором, і такі злочини можуть вчиняти дестабілізуючий вплив на всі верстви суспільства. Таким чином кіберзлочинність виступає загрозою національній безпеці в кібернетичній сфері.

Проаналізувавши теоретичні та практичні дослідження в галузі визначення поняття кіберзлочину, можна висновувати, що серед сучасних українських науковців немає єдиного підходу до визначення поняття кіберзлочину.

Отже, кіберзлочинність – це дії, а саме: незаконний доступ; нелегальне перехоплення; втручання у дані або у систему; зловживання пристроям; шахрайство; правопорушення, пов'язані з дитячою порнографією; порушення авторських і суміжних прав; правопорушення, спрямовані проти конфіденційності, цілісності і доступності комп'ютерних систем, мереж і комп'ютерних даних, а також зловживання такими системами, мережами і даними, що тягнуть кримінальну відповідальність.

Список використаних джерел:
1. Біленчук П. Д. Комп'ютерна злочинність: поняття, сутність, характеристика / П. Д. Біленчук, О. О. Шульга // Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення: матеріали всеукр. наук.-практ. конф. 9 груд. 2011 р. – Донецьк: Донец. юрид. ін-т, 2012. – С. 28-31.
2. Бутузов В. М. Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку: Науково-практичний коментар / В. М. Бутузов, С. Л. Остапець, В. П. Шеломенцев; МВС України. Департамент ДСБ з економічною злочинністю. – К., 2005. – 86 с.