

Колос О.В.

кандидат юридичних наук,
доцент кафедри кримінального права та кримінології,
Навчально-науковий інститут права,
Університет державної фіскальної служби України

У Кримінальному кодексі України 2001 року [1] (надалі – *КК, КК України*) вперше виокремлено розділ XVI Особливої частини під назвою «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» На сьогоднішній день до нього увійшли ст.ст. 361, 361-1, 361-2, 362, 363, 363-1 КК України (тобто всього 6 статей), які відносять до так званих «комп'ютерних злочинів» або «кіберзлочинів».

Втім, перелік комп'ютерних злочинів, не вичерпується діями, передбаченими розділом XVI КК України.

Певні злочини, які існували ще задовго до виникнення комп'ютерних, також можуть бути вчинені із застосуванням інформаційних технологій. Використання електронно-обчислювальних машин або спрощує вчинення злочину, або надає йому іншої – нової форми. То які ж злочини можна вважати комп'ютерними?

Проаналізувавши зміст Особливої частини КК України, опираючись на дослідження Гавловського В.Д. та Цимбалюка В.С. [2], у певній мірі, до таких можна віднести наступні склади злочинів, передбачені статтями КК України:

Розділ I	«Злочини проти основ національної безпеки України»	ст.ст. 109, 110, 110-2, 111, 113, 114, 114-1 КК України
Розділ II	«Злочини проти життя та здоров'я особи»	ст.ст. 120, 129, 132, 145 КК України.
Розділ IV	«Злочини проти статевої свободи та статевої недоторканості особи»	ст.156 КК України
Розділ V	«Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина»	ст.ст. 157, 158, 158-2, 159, 159-1, 160, 161, 162, 163, 168, 170, 171, 172, 182, 183 КК України
Розділ VI	«Злочини проти власності»	ст.ст. 185, 186, 189, 190, 191, 192, 194, 194-1, 195, 196, 197, 198 КК України
Розділ VII	«Злочини у сфері господарської діяльності»	ст.ст. 199, 200, 203-1, 203-2, 205, 205-1, 206, 206-2, 209, 209-1, 212, 212-1, 216–233 КК України
Розділ VIII	«Злочини проти довкілля»	ст. 238 КК України
Розділ IX	«Злочини проти громадської безпеки»	ст.ст. 255, 256, 258, 258-2, 258-3, 258-4, 258-5, 259, 262, 266, 267 КК України
Розділ XI	«Злочини проти безпеки руху та експлуатації транспорту»	ст.ст. 276, 277, 279, 281, 282, 290, 292 КК України
Розділ XII	«Злочини проти громадського порядку та моральності»	ст.ст. 293, 294, 295, 298-1, 300, 301, 304 КК України
Розділ XIII	«Злочини у сфері обігу наркотичних засобів, психотропних речовин, їх аналогів або прекурсорів та інші злочини проти здоров'я населення»	ст.ст. 306, 308, 312, 313, 318, 319 КК України
Розділ XIV	«Злочини у сфері охорони державної таємниці, недоторканості державних кордонів, забезпечення призову і мобілізації»	ст.ст. 328, 329, 330 КК України

Розділ XV	«Злочини проти авторитету органів державної влади, органів місцевого самоврядування, об'єднань громадян та злочини проти журналістів»	ст.ст. 343, 344, 345, 345-1, 346, 347, 347-1, 348, 348-1, 350–352, 357–360 КК України
Розділ XVII	«Злочини у сфері службової діяльності та професійної діяльності, пов'язаної з наданням публічних послуг»	ст.ст. 364–370 КК України
Розділ XVIII	«Злочини проти правосуддя»	ст.ст. 376–378, 381, 383, 387, 397–399 КК України
Розділ XIX	«Злочини проти встановленого порядку несення військової служби (військові злочини)»	ст.ст. 405, 409–413, 422 КК України
Розділ XX	«Злочини проти миру, безпеки людства та міжнародного правопорядку»	ст.ст. 436–437, 439, 440, 444 КК України

Проте не важко передбачити, що це лише приблизний перелік тих статей, які за тими чи іншими ознаками можна віднести до списку комп'ютерних злочинів.

З цього приводу слід відзначити, що на думку М. Гуцалюка правопорушення, пов'язані з комп'ютерами, слід розглядати за трьома основним групами.

До першої групи належать правопорушення, де сам комп'ютер чи інформація у ньому є предметом вчинення протиправних дій.

До другої групи слід віднести правопорушення, де комп'ютер виступає як знаряддя вчинення злочину. Особливо розповсюдженими такі правопорушення є у фінансово-банківській сфері.

До третьої групи належать правопорушення, доказом про які є інформація, що міститься в комп'ютерних системах. Для прикладу: організована злочинна група кілерів з Дніпропетровська отримувала "замовлення" на свої жертви через Інтернет. Комп'ютерна інформація може також свідчити про торгівлю наркотиками або, наприклад, відмивання коштів [3].

Втім варто нагадати, що деякі положення Конвенції про кіберзлочинність, укладеної 23 листопада 2001 року та ратифікованої Україною 7 вересня 2005 року (*надалі – Конвенції*), так і не знайшли відображення у вітчизняному кримінальному законодавстві. Автор погоджується з думкою Орлова Ю.Ю., що КК України і досі не передбачила кримінальної відповідальності за:

- придбання шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (п. «а і» ч.1 ст.6 Конвенції);
- виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром їх використання для вчинення будь-якого комп'ютерного злочину (п. «а ii» ч.1 ст.6 Конвенції);
- володіння зберігання зазначеними вище шкідливими комп'ютерними програмними чи технічними засобами, комп'ютерними паролями кодами доступу чи іншими аналогічними даними (п. «b» ч.1 ст.6 Конвенції);
- здобуття дитячої порнографії через комп'ютерну систему (п. «d» ч.1 ст.9 Конвенції);
- володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних (п. «e» ч.1 ст.9 Конвенції).

Запровадження кримінальної відповідальності за більшість з указаних діянь кожна держава-учасниця Конвенції має право визначати самостійно. Тому питання щодо необхідності криміналізації цих діянь залежить від ступеня їх суспільної небезпеки в умовах України та кримінологічних характеристик (рівня, динаміки тощо).

Водночас питання щодо криміналізації діянь, передбачених п. «а ii» ч.1 ст.6 Конвенції, необхідно вирішувати з урахуванням змісту ч.3 ст.6 цього документу, що контекстуально зобов'язує всіх держав-учасниць передбачити кримінальну відповідальність за продаж, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути вчинено комп'ютерний злочин [4].

Література:

1. Кримінальний кодекс України: чинне законодавство України зі змінами та допов. станом на 8 серпня 2017 року. [Офіц. текст]. – К.: Право. – 2017. – 264 с.
2. Гавловський В. Кіберзлочинність як чинник державної інформаційної політики України / В. Гавловський, В. Цимбалюк // Боротьба з організованою злочинністю і корупцією: теорія і практика. – К., 2002. – №5. – с.106–112.
3. М. Гуцалюк. Координація боротьби з комп'ютерними правопорушеннями / Михайло Гуцалюк / Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні. – 2001 р. – Вип. 3. – с. 32.
4. Конвенція про кіберзлочинність [Електронний ресурс]. – Режим доступу до документу: http://zakon2.rada.gov.ua/laws/show/994_575
5. Орлов Ю.Ю. Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України / Науковий вісник Національної академії внутрішніх справ. – 2011 р. – №6. – с. 3–6.

Щодо віртуальної власності як об'єкту кіберпростору

Кузьмініх А.

студент факультету №4

Одеського державного університету внутрішніх справ

Науковий керівник: Даниленко С.К.

старший викладач кафедри цивільно-правових дисциплін

Одеського державного університету внутрішніх справ

З розширенням віртуального простору та доступністю до нього, постає питання про регулювання відносин, що виникають у цій сфері, способів захисту та відповідних прав та обов'язків, а також правонаступництво які пов'язані із віртуальною власністю. З кожним днем правові проблеми, пов'язані з онлайн іграми, соціальними мережами або іншими віртуальними ресурсами, стають все більш актуальними практично і цікавими теоретично. Все більше речей матеріального світу, стають частиною віртуального світу та постає питання, щодо правового регулювання цих речей. Віртуальна власність - це онлайн-майно, що включає в себе доменні імена, веб-сайти і онлайн-сервіси.

Професор школи права Ратгерського університету (штат Нью-Джерсі) Грег Ластовка (Greg Lastowka), говорить, що домен в Інтернеті - це теж „рядок коду”. Однак законодавство США визнає право власності на домен. Домени, банківський рахунок - теж „рядок коду”. І тим не менше є власністю. Г.Ластовка стверджує, що віртуальна власність сильно відрізняється від реальної, а значить, вимагає особливого підходу. І все ж не зараз, в майбутньому через років десять законодавство прийде до необхідності вважати ігрові предмети власністю[1].

Власністю є право особи на майно, яке вона здійснює відповідно до закону за своєю волею, незалежно від волі інших осіб та відповідно власникові належать право володіння, користування, та розпорядження своїм майном [2]. Віртуальність (лат. Virtualis - можливий) - об'єкт або стан, які реально не існують, але можуть виникнути при певних умовах [3]. Відповідно до зазначених трактувань, віртуальна власність обмежена у володінні, користуванні та розпорядженні тільки рамками самої віртуальності, тобто власність яка може виникнути при певних умовах. Наприклад, особа має індивідуальний обліковий запис у онлайн-гри „World of tanks”, де на його рахунку є певні блага, які отримувані за реальні гроші, та можуть бути продані, також за реальні гроші. Але умовою користування даним благом, або власністю є доступ до мережі інтернет. Даний вид власності є одним із предметів кіберзлочинів, та потребує доцільного захисту, як зі сторони провайдера, так зі сторони власника індивідуально облікового запису.

Натомість, проводячи паралель із реальним світом, також існують подібні відносини, де відповідно до договору купівлі-продажу, майно що передається, обмежується у користуванні, а саме може виникнути при певних умовах. Так завод Феррарі, налічує декілька моделей автомобілів, які можуть їздити тільки на спеціальних майданчиках. Власники машин не мають права експлуатувати їх в повсякденному режимі, а також зберігати в особистих гаражах. Всі випущені екземпляри знаходяться на зберіганні в технічному центрі Феррарі, а їздити можна тільки на трасі під час спеціальних тестових днів [4].

Використання як класифікаційної ознаки якісних характеристик об'єктів власності дає змогу виокремити матеріальний та нематеріальний типи власності. У складі нематеріальної власності необхідно виділяти інтелектуальну та віртуальну форми власності. Категорія „віртуальна власність”