

УДК 002.6:341.48

Ганна Володимирівна ФОРОС,

кандидат юридичних наук, доцент,

професор кафедри кібербезпеки та інформаційного забезпечення

Одеського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0001-6377-3287>;

Дмитро Сергійович БІЛОКОНЬ,

аспірант кафедри кібербезпеки та інформаційного забезпечення

Одеського національного університету внутрішніх справ;

ORCID: <https://orcid.org/0000-0002-0959-4381>

СУБ'ЄКТИВНІ ОЗНАКИ КІБЕРЗЛОЧИНІВ

Проблема кваліфікації кіберзлочинів набула значного наукового і практичного значення з розвитком комп'ютерних технологій та широким впровадженням їх в повсякденне життя. Багато вчених у своїх дослідженнях приділяли увагу розгляду цього питання, серед яких: Д. С. Азаров, Д. П. Біленчук, В. Б. Вехов, В. Д. Гавловський, В. М. Гуцалюк, М. В. Рудик, В. В. Кузнецов, А. А. Музика, С. О. Орлов, О. В. Смаглюк та багато інших.

Кожна країна має свою національну законодавчу систему, котра відрізняється від систем інших країн. Багато країн уже мають спеціальні норми в кримінальному законодавстві, які передбачають відповідальність за вчинення кіберзлочинів; інші – тільки в процесі прийняття відповідних законів. У деяких країнах відповідальність за вчинення кіберзлочинів настає за традиційними статтями кримінального законодавства (крадіжка, шахрайство, підробка та ін.). Проблематика полягає в тому, що сучасні технології розвиваються та вдосконалюються з кожним днем, а так само і розвивається, поширюється кіберзлочинність. В світовій правничій термінології вже давно існує та активно використовується поняття «кіберзлочинність». Більше того, 07 вересня 2005 року Україна ратифікувала Конвенцію Ради Європи про кіберзлочинність. Тим не менш, українське законодавство не містить нормативного визначення поняття «кіберзлочинність» чи «кіберзлочин». В XVI розділі Особливої частини КК України «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку», встановлена саме відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем, комп'ютерних мереж і мереж електрозв'язку, але поняття «кіберзлочину» не передбачено.

З точки зору кримінально-правової кваліфікації, необхідно чітко встановити конкретну норму КК України, за якою відбудеться юридична оцінка певного діяння, що становить завдання такої кваліфікації. Це обумовлює актуальність наукової розробки питань кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів),

систем та комп'ютерних мереж і мереж електрозв'язку. При кваліфікації того чи іншого діяння як кіберзлочину, в першу чергу, увагу потрібно приділити оцінці суб'єктивних ознак: суб'єкта та суб'єктивної сторони складу злочину, оскільки їх невідповідність вимогам КК України виключає кримінальну відповідальність.

Оцінка ознак суб'єкта злочину в сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку є надзвичайно важливою тому, що в умовах масової «інтернетизації» суспільства, більшість користувачів є неповнолітніми, а точніше такими що не досягли віку, з якого може наставати кримінальна відповідальність.

В випадках наявності ознак спеціального суб'єкта, їх необхідно встановити та оцінити. Треба звернути увагу, що останнім часом перелік вже відомих психічних захворювань зростає, його поповнюють нові види, пов'язані із використанням комп'ютерних технологій (інформаційні хвороби, комп'ютерні фобії). Тому, задля оцінки осудності цієї особи, слід звернути окрему увагу на поведінку підозрюваного в ході слідства та відображенням її в механізмі злочинної поведінки (вчиненого діяння).

Завершальний етап у констатації складу злочину – це встановлення всіх ознак суб'єктивної сторони. Вона виступає обов'язковим елементом будь-якого складу злочину, а її наявність чи відсутність дає можливість відмежувати злочинне діяння від правомірного. Саме зміст суб'єктивної сторони впливає на ступінь тяжкості вчиненого злочину, ступінь його суспільної небезпеки і тим самим, на призначення покарання винній особі.

Суб'єктивна сторона злочинів, передбачених у розділі XVI КК України, може виражатися як у формі умислу, так і необережності – при порушенні правил експлуатації автоматизованих електронно-обчислювальних систем.

Також необхідно згадати про мотиви та мету вчинення комп'ютерних злочинів. До основних мотивів вчинення кіберзлочинів відносять: отримання особистої або фінансової вигоди, розвага, помста, спроба добути чутливе ставлення до себе від будь-кого, самовираження, випадковість, вандалізм. Але значної шкоди, біля 60 % усіх втрат, приносять помилки людей та інциденти.

Якщо розглянути мету вчинення злочинів комп'ютерними злочинцями, то вона дуже різноманітна. Це може бути знищення, модифікування, копіювання інформації, або вивчення режиму захисту інформації від несанкціонованого доступу та систем контролю, або отримання таємних кодів магнітних карток, незаконне заволодіння комп'ютерним обладнанням та інформацією особливої категорії.

У всіх випадках при розслідуванні конкретного злочинного мотив і мета повинні бути з'ясовані. Це має важливе значення не тільки для визначення судом справедливого покарання за вчинене, але і сприяє повному розкриттю злочину. Дані про найбільш розповсюджені

мотиви та мету вчинення будь-яких злочинів, у тому числі і кіберзлочинів, використовуються при висуванні версій щодо суб'єкта і суб'єктивної сторони злочину, а також при організації цілеспрямованого пошуку злочинця.

В ході оцінки події, яка не містить достатніх ознак складу злочину, хоч в ній і фігурували ЕОМ (комп'ютер), система, комп'ютерна мережа або мережа електрозв'язку, слід мати на увазі, що вона може бути кваліфікована як незакінчений злочин або співучасть у злочині. Зокрема, досить розповсюдженими є діяння, передбачені ст. 6 Конвенції про кіберзлочинність, вони можуть розглядатися як умисний продаж, розповсюдження або надання для використання іншим чином комп'ютерних паролів, кодів доступу або подібних даних з метою подальшого вчинення злочинів, передбачених статтями розділу 16 КК України і являти собою пособництво у вчиненні відповідних злочинів (необхідним є посилання на ч. 5 ст. 27 КК України); володіння шкідливими засобами з метою подальшого вчинення злочинів необхідно, згідно з національним законодавством, вважати готуванням до відповідних злочинів (необхідним є посилання на ч. 1 ст. 14 КК України).

Таким чином, під час кваліфікації та виявлення суб'єктивних ознак кіберзлочинів, доцільно дотримуватися певних правил:

1) незалежно від складу злочину слід оцінити суб'єктивні ознаки з огляду на знижений вік комп'ютерних користувачів та вплив комп'ютерних технологій на психіку людини;

2) при оцінці сукупності злочинів слід звертати увагу на велику ймовірність поглинення діяння, яке містить ознаки комп'ютерного злочину, складом іншого, як правило більш тяжкого злочину;

3) при оцінці діянь в комп'ютерній сфері, які прямо не передбачені КК України, необхідно спробувати застосувати до них правила кваліфікації незакінченого злочину або співучасті у злочині.

Список бібліографічних посилань

1. Кримінальний кодекс України : закон України від 05.04.2001 № 2341-III // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/laws/show/2341-14> (дата звернення: 01.11.2018).

2. Про ратифікацію Конвенції про кіберзлочинність : Закон України від 07 вересня 2005 року № 2824-IV // БД «Законодавство України» / ВР України. URL: <http://zakon.rada.gov.ua/cgi-bin/laws/main.cgi?nreg=2824-15> (дата звернення: 01.11.2018).

3. Протидія кіберзлочинності в Україні : правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. К. : Видавничий дім «Скіф», 2012. 728 с.

Одержано 05.11.2018