

Бабанін С.В.

доцент кафедри кримінального права та кримінології Дніпропетровського державного університету внутрішніх справ, к.ю.н., доцент

КРИМІНАЛЬНО-ПРАВОВИЙ ЗАХИСТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ В УКРАЇНІ

Одним з завдань розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України є забезпечення кримінально-правового захисту інформаційних технологій в Україні. Ефективність такого захисту залежить, зокрема, від якості законодавчої техніки, яка застосовується у процесі розробки диспозицій відповідних норм вказаного розділу КК України (описі об'єктивних та суб'єктивних ознак кримінальних правопорушень у цій сфері).

На наш погляд, конструкція норм розділу XVI Особливої частини КК України далека від досконалості.

Аналіз диспозицій ст.ст. 361-363¹ КК України свідчить про їх неконкретність щодо визначення ознак суспільно небезпечних діянь у сфері інформаційних технологій та їх наслідків, що, у свою чергу, дозволяє надавати достатньо широке тлумачення цих об'єктивних ознак і, відповідно, дезорієнтує практичного працівника при вирішенні питання кваліфікації таких діянь і притягнення особи до відповідальності.

Так, ч. 1 ст. 361 КК передбачає відповідальність за несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, що призвело до витоку, втрати, підробки, блокування інформації, спотворення процесу обробки інформації або до порушення встановленого порядку її маршрутизації [1].

На сьогодні комп'ютери у своїй власності має чи не кожна родина, підприємство, установа, організація. Під ознаки ч. 1 ст. 361 КК підпадає будь-яке діяння, пов'язане з несанкціонованим втручанням в роботу будь-якого комп'ютера, що призвело до відповідного наслідку. Тому, наприклад, формально за ч. 1 ст. 361 КК слід кваліфікувати дії студента, який з ноутбука свого товариша без його відома шляхом вільного доступу «зкачав» будь-яку інформацію (фільм, фотографію, курсову роботу тощо). Проте таке діяння, на нашу думку, не становить достатнього для криміналізації ступеня суспільної небезпеки.

Пропонуємо передбачити у цій статті відповідальність за: 1) комп'ютерне шпигунство, що полягає у незаконному доступі до інформації, а також незаконне одержання інформації, яка має відношення до державної безпеки, міжнародних відносин і питань атомної енергетики України; 2) незаконний доступ до інформації Офісу Президента України, Кабінету Міністрів України, Верховної Ради України, міністерств та відомств України, а також незаконне втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних

мереж чи мереж електрозв'язку цих органів.

Крім того, пропонуємо: 1) надати нормативне визначення поняття «комп'ютерні кримінальні правопорушення», до яких віднести не лише кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку (ст.ст. 361-363¹ КК України), а й ряд кримінальних правопорушень, передбачених іншими розділами Особливої частини КК України (ст. 301 «Ввезення, виготовлення, збут і розповсюдження порнографічних предметів» та ін.); 2) класифікувати поширені види шкоди у сфері інформаційних технологій та передбачити відповідальність за її заподіяння залежно від ступеня тяжкості у кваліфікованих та особливо кваліфікованих складах кримінальних правопорушень розділу XVI «Кримінальні правопорушення у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Особливої частини КК України.

У зв'язку з поширенням у мережі Інтернет такого суспільно небезпечного явища як розміщення підроблених сайтів з метою заволодіння конфіденційною інформацією пропонуємо передбачити у розділі XVI Особливої частини КК України відповідальність за розміщення веб-ресурсів в мережі Інтернет з метою незаконного заволодіння персональними або автентифікаційними даними, реквізитами платіжних карток, банківських рахунків.

Використані джерела:

1. Кримінальний кодекс України: Закон України від 05 квітня 2001 р. / Верховна Рада України. URL: <https://zakon.rada.gov.ua/laws/show/2341-14#Text> (дата звернення: 14.11.2020).

Рижков Е.В., завідувач кафедри економічної та інформаційної безпеки, к.ю.н., доцент
Мирошниченко В.О., професор кафедри к.т.н., доцент

ПАТЕНТНА ДІЯЛЬНІСТЬ ЯК ПРЕДМЕТ ТРАНСФЕРУ ТЕХНОЛОГІЙ (НА ПРИКЛАДІ ПАТЕНТУ НА КОРИСНУ МОДЕЛЬ «ПРИСТРІЙ РАДІОЛОКАЦІЙНОГО РОЗПІЗНАВАННЯ ОБ'ЄКТІВ»)

Патентна діяльність науково-педагогічних колективів у навчальних закладах зі специфічними умовами навчання є невід'ємною складовою їх загальної діяльності.

В кожному закладі є свої винахідницькі напрацювання, які з часом породжують свій профіль, традиції та школи.

За результатами роботи відповідних комісій колективу Дніпропетровського державного університету внутрішніх справ другий рік поспіль вдається досягти