

портал Українського агентства фінансового розвитку [Електронний ресурс]. – Режим доступу: http://ufin.com.ua/analit_mat/poradnyk/094.htm

4. Шахрайство при покупках і продажах в мережі Інтернет. Незалежна асоціація банків України ваш захисник від кіберзлочинності [Електронний ресурс]. – Режим доступу: http://anticyber.com.ua/article_detail.php?id=133

УДК 341.824:338.47 (043.2)

Лебедь Н. В., Гришко Н. С., студентки,
Навчально-науковий Інститут комп'ютерних
інформаційних технологій,
Національний авіаційний університет, м. Київ
Науковий керівник: Миронець О. М., старший викладач

ТЕОРЕТИКО-ПРАВОВІ АСПЕКТИ ПРАВОПОРУШЕННЯ В СФЕРІ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ

З розвитком комп'ютерних технологій, які пов'язані зі збереженням, обробкою, передачею інформації, зростає залежність суспільства від роботи комп'ютерної техніки. Практично вся документація юридичних осіб, операції з валютою, відео та фотографії знаходяться у відкритому доступі в режимі онлайн. Звичайно, з одного боку «комп'ютеризація» комунікації між людьми, засобів виробництва дозволяє робити велику кількість необхідних операцій за менші проміжки часу, що значно полегшує життєдіяльність. Проте з іншого боку у наші дні зважаючи на вказане вище створено сприятливі умови для безперешкодного одержання сторонніми людьми, які маючи певні знання комп'ютерної науки, важливої, а головне секретної інформації. Використання вказаних даних звичайно може здійснюватися зі злочинною метою, порушувати права, свободи та законні інтереси людини і громадянина. На сьогодні в Україні кількість злочинів, які вчинено у сфері використання електронно-обчислювальних машин дедалі збільшується, тому питання захисту громадян від правопорушень у комп'ютерній сфері, безперечно, є актуальним.

Поняття правопорушень у сфері комп'ютерної інформації можна з'ясувати досліджуючи поняття комп'ютерної злочинності, яка є особливим видом злочинів, які посягають на встановлений в суспільстві порядок інформаційних відносин та скоюються з використанням електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж. Об'єктом злочину виступають інформаційні відносини у суспільстві, що охороняються законом, а предметом – електронно-обчислювальні машини (комп'ютери), системи та комп'ютерні мережі, а також комп'ютерна інформація, що обробляється

за їх допомогою. В їх основі можуть бути політичні, хуліганські, корисливі й інші мотиви. Тому існує необхідність розвитку й удосконалення правових засобів регулювання суспільних відносин у сфері інформаційної діяльності. Інформаційні відносини, тобто відносини, що виникають при одержанні, використанні, поширенні та зберіганні інформації, регулюються положеннями Конституції України, розділом XVI Кримінального кодексу України, законами від 2 жовтня 1992 р. № 2657-XII «Про інформацію», від 25 червня 1993 р. № 3322-XII «Про науково-технічну інформацію», від 18 листопада 2003 р. № 1280-IV «Про телекомунікації», від 5 липня 1994 р. № 80/94-ВР «Про захист інформації в інформаційно-телекомунікаційних системах», а також низкою підзаконних актів, зокрема Положенням про технічний захист інформації в Україні (затверджене Указом Президента України від 27 вересня 1999 р. № 1229/99) та ін. У залежності від виду правопорушення особи, винні у вчиненні «комп'ютерних» злочинів, несуть кримінальну, адміністративну, цивільно-правову, дисциплінарну або матеріальну відповідальність [1].

Як показують соціологічні опитування в різних країнах, і насамперед, у високорозвинених, кіберзлочинність посідає одне з перших місць серед тих проблем, які турбують людей. Отже, проблема відсутності єдиного понятійного апарату та норм, щодо кваліфікації комп'ютерних злочинів, зокрема, пов'язаних з незаконним втручанням в роботу комп'ютерних систем актуальна сьогодні, як ніколи. Так, у Резюме Десятого Конгресу Організації Об'єднаних Націй по попередженню злочинності і поводженню з правопорушниками, який відбувся у Відні 10-17 квітня 2000 року, вказано: «Для ефективного попередження кіберзлочинності і боротьби з нею необхідний узгоджений міжнародний підхід на різних рівнях. На внутрішньому рівні для розслідування кіберзлочинів потрібен належний персонал, спеціальний досвід, знання та процедури. На міжнародному рівні для розслідування кіберзлочинів необхідні оперативні дії, що спираються на координацію зусиль національних правоохоронних органів і прийняття відповідних юридичних підстав» [2, с. 333].

Однією з проблем викриття комп'ютерних злочинів є недосконалість внутрішньодержавного законодавства. Високий рівень розкриття комп'ютерних злочинів, зокрема, у США, Франції, Німеччині, обумовлений ефективним законодавчим регулюванням відповідальності за протиправні посягання на роботу комп'ютерних систем та комп'ютерну інформацію [3].

Загальносвітові вимоги боротьби з комп'ютерною злочинністю передбачають необхідність розробки в кожній державі власних норм щодо захисту від посягань на дані, що зберігаються в автоматизованих системах. Кримінальні кодекси, наприклад: Республіки Білорусь, Естонської Республіки, Республіки Таджикистан передбачають

кримінальну відповідальність за великий перелік «комп'ютерних» правопорушень. Даний інститут кримінального права в Україні ще недостатньо розроблений. Однак, разом з поширенням Internet і зростанням загрози від комп'ютерної злочинності суспільним інтересам України, законодавець має визначити коло комп'ютерних злочинів, чітко розробивши норми, за якими буде можливо притягнути до відповідальності винних у їх вчиненні. Також необхідно прийняти єдині заходи, які б надавали можливість узгодження таких формулювань, як з метою їх вдосконалення, так і з метою застосування їх до осіб, що вчинюють комп'ютерні злочини на території СНД [3].

Література

1. Судова практика розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку [Електронний ресурс]. – Режим доступу: <http://www.scourt.gov.ua/clients/vsen.nsfh>

2. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А. Г. Волеводз. – М.: Юрлитинформ, 2002. – 496 с.

3. Розенфельд Н. А. Кримінально-правова характеристика незаконного втручання в роботу електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж: автореф. дис. ... канд. юрид. наук. – К., 2003 [Електронний ресурс]. – Режим доступу: http://adhdportal.com/book_1479_chapter_1_Anotaja.html

УДК 340.130.3(043.2)

Лукашенко Т. О., студентка,
Навчально-науковий Юридичний інститут,
Національний авіаційний університет, м. Київ,
Науковий керівник: Шапенко Л. О., асистент

СИСТЕМА ДЖЕРЕЛ ПРАВА В УКРАЇНІ

Формування сучасної системи джерел права є складним, тривалим та багатофункціональним процесом, що відбувається в умовах глобалізації. Нині національна система джерел права накопичує значну кількість міжнародних договорів, відбувається зміна видів та місця законів у системі, розширюються предметні сфери законодавчого регулювання тощо. При цьому зазнає змін і взаємодія у системі чинних джерел вітчизняного права, особливо нормативно-правових актів та нормативно-правових договорів.

Саме тому так гостро в Україні стоїть питання законотворчості. Воно є актуальним з точки зору оцінки стану законодавчої діяльності на