УДК 341.1

Бєлєнький В. П.,
аспірант кафедри кримінального права, кримінального процесу та криміналістики
економіко-правового факультету
Одеського національного університету імені І. І. Мечникова

КІБЕРЗЛОЧИНИ ЗА ЗАКОНОДАВСТВОМ США

Анотація. США є однією з найбільш комп'ютеризованих країн західного світу. Ця країна стала однією з перших, які включили до своїх законів відповідальність за кіберзлочини. У статті досліджено сутність, форми та ознаки, а також регулювання кіберзлочинів за законодавством США. Аналізуються склади цих злочинів, відповідальність за їх скоєння. Стаття допоможе проаналізувати кримінальне право США у сфері кіберзлочинів та вдосконалити вітчизняне кримінальне право.

Ключові слова: США, кіберзлочинність, кіберзлочин, відповідальність, види, типи, ознаки.

Постановка проблеми. Початок правового регулювання комп'ютерних технологій у США пов'язується з появою в цій країні комп'ютерних мереж. США стали першою країною, у якій почали створюватися комп'ютерні мережі для вирішення певних завдань. Спочатку утворювались локальні комп'ютерні мережі, а згодом для здійснення інформаційного обміну між ними – глобальні комп'ютерні мережі.

Метою статті є розгляд кіберзлочинів згідно із законодавством США.

Виклад основного матеріалу. У 1961 році Агентство передових досліджень Міністерства оборони США (Advanced Research Agency) почало проект щодо створення експериментальної мережі передачі пакетів інформації. У назві мережі було використано абревіатуру міністерства – Arpanet. Експеримент був успішним, Arpanet перетворилась на робочу мережу. Її користувачами поряд із Міністерством оборони США стали університети (Стенфордський, Каліфорнійський, університет штату Юта) [1, с. 227]. Однак у 1983 році Міністерству оборони США довелось виділити окрему мережу (Milnet), яка використовувалась лише цим міністерством. Через деякий час ці мережі знову було об'єднано під знайомою нам назвою Internet. Перший законопроект про захист федеральних комп'ютерних систем з'явився в 1977 році, а федеральний закон США – Акт про захист комп'ютерних систем – було прийнято в 1979 році [2, с. 656]. Цей закон встановлював відповідальність за введення свідомо неправильних даних у комп'ютерну систему, незаконне використання комп'ютерних обладнань, внесення змін у процеси обробки інформації або порушення цих процесів, розкрадання коштів, паперів, майна, послуг, цінної інформації, проведене з використанням комп'ютерних технологій або з використанням комп'ютерної інформації [3, с. 88].

Згодом цей закон неодноразово змінювався й доповнювався. Нині згаданий акт включено у вигляді § 1030 у Титул 18 Зводу законів США [4, с. 632–634].

Необхідно відзначити, що на додаток до цього федерального акта в 1978 році на рівні штату було прийнято Закон Флориди про відповідальність за модифікацію, знищення та несанкціонований доступ до комп'ютерної інформації. А вже після вказаного федерального закону, а саме з 1984 року, низка штатів прийняли свої закони на його основі. Зокрема, у штаті Техас у 1985 році було прийнято Закон про комп'ютерні злочини (Texas Computer Crimes Law), згаданий у розділі, присвяченому термінології. Згідно із цим законом каралося незаконне використання комп'ютерної інформації, незаконне проникнення в комп'ютерну мережу. За техаським законом 1985 року кіберзлочини було віднесено залежно від конкретного виду злочинів із класу «В» (місдімінори) до третього класу (фелонії) [5].

Тому повернемось до § 1030 у Титулі 18 Зводу законів США. Цей закон встановлює відповідальність за діяння, предметом посягання яких є «захищений комп'ютер» (точніше, інформація, що перебуває в ньому). Під ним розуміється комп'ютер, що перебуває у винятковому користуванні уряду чи фінансової організації, або комп'ютер, функціонування якого було порушено під час роботи в інтересах уряду чи фінансової організації, а також комп'ютер, що є частиною системи чи мережі, елементи якої розташовано більше ніж в одному штаті США. Водночас закон встановлює, що кримінальна відповідальність настає в таких випадках: а) несанкціонованого доступу, коли невповноважена особа щодо комп'ютера чи комп'ютерної системи втручається в них ззовні та користується ними; б) перевищення санкціонованого доступу, коли законний користувач комп'ютера чи системи здійснює доступ до комп'ютерних даних, на які його повноваження не поширюються.

Згаданий закон встановлює відповідальність за такі основні склади злочинів:

1) комп'ютерне шпигунство, що полягає в несанкціонованому доступі або перевищенні санкціонованого доступу до інформації, а також отриманні інформації, яка має відношення до державної безпеки, міжнародних відносин і питань атомної енергетики (§ 1030(a)(1));

2) несанкціонований доступ або перевищення санкціонованого доступу до інформації з урядового відомства США з будь-якого захищеного комп'ютера, що має відношення до міжштатної чи міжнародній торгівлі, а також отримання інформації з фінансових записів фінансової установи, емітента, карт або інформації про споживачів, що міститься у файлі управління обліку споживачів (§ 1030(a)(2));

3) вплив на комп'ютер, що перебуває у винятковому користуванні урядового відомства США, або порушення функціонування комп'ютера, використовуваного повністю чи частково Урядом США (§ 1030(a)(3));

4) шахрайство з використанням комп'ютера: доступ, здійснюваний із шахрайськими намірами, та використання комп'ютера з метою отримання будь-чого цінного за допомогою шахрайства, у тому числі незаконне використання машинного часу вартістю більше 5 тис. доларів США протягом року, тобто без оплати використання комп'ютерних мереж і серверів (§ 1030(a)(4));

5) навмисне або необережне ушкодження захищених комп'ютерів (§ 1030(a)(5));

6) шахрайство шляхом торгівлі комп'ютерними паролями чи аналогічною інформацією, що дозволяє отримати несанк-

ціонований доступ, якщо така торгівля впливає на торговельні відносини між штатами та з іншими державами, або на комп'ютер, використовуваний урядом США (§ 1030(a)(6));

7) погрози, вимагання, шантаж та інші протиправні діяння, вчинені з використанням комп'ютерних технологій (§ 1030(a)(7)).

Аналізуючи наведені злочини, необхідно відзначити, що виділення такої кваліфікуючої ознаки, як використання комп'ютера державним органом США, є досить обґрунтованим. Безумовно, інформація, яка може знаходитись у цьому комп'ютері, підвищує суспільну небезпеку злочину та, відповідно, вимагає більш суворого покарання, оскільки комп'ютер виступає лише засобом відтворення інформації й базою даних, а основну цінність становить саме інформація, що зберігається на комп'ютері. Крім того, у певних ситуаціях цей злочин буде двохоб'єктним, оскільки злочинець зазіхатиме не лише на суспільні відносини, що забезпечують інформаційну безпеку, а й на суспільні відносини, що охороняють державну владу. Введення подібної кваліфікуючої ознаки до кіберзлочинів, передбачених у розділі 16 Кримінального кодексу України (далі – КК України), вважаємо доцільним.

Ще одна група кіберзлочинів міститься в § 1029 Титулу 18 Зводу законів США [4, с. 631–632], яким передбачається відповідальність за торгівлю викраденими або підробленими засобами доступу, які можуть бути використані для отримання грошей, товарів чи послуг. Зокрема, подібну відповідальність встановлено за такі дії: виробництво, використання й торгівлю підробленими засобами доступу; використання або отримання засобів для несанкціонованого доступу з метою отримання матеріальної вигоди в розмірі більше 1 тис. доларів США; володіння 15 та більше підробленими чи недозволеними засобами доступу; виробництво, продаж або володіння устаткуванням для виготовлення підроблених засобів доступу; здійснення угод за допомогою засобів доступу, призначених для іншої особи; пропозиція якій-небудь особі засобів доступу або придбання за плату інформації, яка може бути використана для отримання засобів доступу; використання, виробництво, продаж чи володіння телекомунікаційним діагностичним устаткуванням, модифікованим або пристосованим для несанкціонованого отримання телекомунікаційних послуг; використання, виробництво, продаж або володіння скануючими приймачами, устаткуванням чи програмним забезпеченням для модифікації телекомунікаційної апаратури з метою несанкціонованого використання телекомунікаційних послуг; примус якої-небудь особи представити члену кредитної системи або його агенту для оплати запису транзакцій, зроблених за допомогою засобів несанкціонованого доступу.

У цілому варто зазначити, що цей перелік злочинів свідчить про розробленість права про кіберзлочини в США. Що стосується запозичення тих або інших складів комп'ютерних злочинів, то до цього питання необхідно підходити максимально обережно. У розділі 16 КК України можуть бути поміщені лише ті склади, об'єктом яких є суспільні відносини у сфері безпеки комп'ютерної інформації й нормального функціонування електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж та мереж електрозв'язку, які заподіюють їм шкоду чи ставлять під загрозу завдання такої шкоди. Обґрунтованою постає ідея, що необхідно запозичити з кримінального права США до українського права такі злочини, як використання чи отримання засобів для несанкціонованого доступу з метою отримання матеріальної вигоди, або ж дещо трансформувати українське право та додати кваліфікуючі ознаки до вже наявних складів. Наприклад, до кваліфікуючих ознак шахрайства можна додати таку ознаку, як здійснення цього злочину з використанням електронно-обчислювальної машини, системи електронно-обчислювальних машин або їх мережі.

Ще одна група комп'ютерних злочинів являє собою діяння, пов'язані з навмисним ушкодженням майна, обладнання, мережевих вузлів, ліній чи систем зв'язку. Відповідальність за них встановлено приписами § 1361 Титулу 18 Зводу законів США [4, с. 672]. Цей злочин за кримінальним правом США також належить до «федеральних злочинів, пов'язаних із тероризмом». Подібний склад злочину в КК України відсутній. Відповідальність за знищення засобів зв'язку лише з метою підриву економічної безпеки й обороноздатності України встановлено в ст. 113 КК України (диверсія). Однак склад у кримінальному праві США, що передбачає відповідальність за навмисне ушкодження майна, устаткування, мережевих вузлів, ліній або систем зв'язку, є набагато ширшим. Підвищена відповідальність за знищення такого майна, безумовно, є виправданою. В інформаційному суспільстві комунікації та інформація мають підвищене значення й вимагають більш серйозної охорони. Таким чином, під час конструювання цього складу злочину законодавець не повинен вказувати мету здійснення злочину, вони можуть бути як економічними (наприклад, боротьба з конкурентами), так і політичними. Вважаємо за доцільне запозичити цей склад злочину з кримінального права США до українського права та викласти його в такій редакції: *суспільно небезпечні діяння, пов'язані з навмисним ушкодженням майна, обладнання, мережевих вузлів, ліній або систем зв'язку.* Ті цілі, які являють собою підвищену небезпеку, можуть бути виділені як кваліфікуючі ознаки.

Аналізуючи наступний вид кіберзлочинів у США, необхідно звернути увагу на Е.Дж. Сноудена (народився 21 червня 1983 року в Північній Кароліні) [6] – американського технічного фахівця, колишнього співробітника ЦРУ та Агентства національної безпеки (далі – АНБ) США. На початку червня 2013 року Е.Дж. Сноуден передав газетам «The Guardian» і «The Washington Post» секретну інформацію АНБ, що стосується тотального стеження американських спецслужб за інформаційними комунікаціями між громадянами багатьох держав у всьому світі за допомогою існуючих інформаційних мереж і мереж зв'язку, у тому числі відомості про проект «PRISM», а також «X-Keyscore» і «Tempora». Згідно з даними закритої доповіді Пентагону Е.Дж. Сноуден викрав 1,7 млн секретних файлів, більшість документів стосується «життєво важливих операцій американської армії, флоту, морської піхоти та військово-повітряних сил» [7].

У зв'язку із цим у США 14 червня 2013 року Е.Дж. Сноудена заочно звинувачено в шпигунстві й викраденні державної власності [8], оголошено американською владою в міжнародний розшук [9]. Незабаром Е.Дж. Сноуден утік із США спочатку в Гонконг, потім до Росії, де пробув більше місяця в транзитній зоні аеропорту «Шереметьєво». 1 серпня 2013 року він отримав тимчасовий притулок у Російській Федерації, а рік потому – трирічний вид на проживання. Проживає в Росії за межами Москви (за іншим, більш пізнім, повідомленням – у Москві [10]). Його точне місцезнаходження не розголошується з міркувань безпеки.

Викриття Е.Дж. Сноудена викликало запеклі суперечки (як у США, так і в інших країнах) про допустимість масового негласного спостереження, межі державної таємниці та баланс

між захистом персональних даних і забезпеченням національної безпеки в епоху після 11 вересня 2001 року.

Водночас американське кримінальне право приділяє велику увагу недоторканності особистого життя громадян і, відповідно, інформації щодо неї. Згідно з § 2511 Титулу 18 Зводу законів США [4, с. 842–844] карається перехоплення й розголошення повідомлень, переданих телеграфом, усно або електронним способом. Спеціально встановлено кримінальну відповідальність за порушення конфіденційності електронної пошти та мовної кореспонденції на сервері. У § 2701 Титулу 18 Зводу законів США «Незаконний доступ до збережених повідомлень» встановлено караність навмисного отримання або видозміни повідомлень, що зберігаються в пам'яті комп'ютера чи комп'ютерної системи, а також створення перешкод для санкціонованого доступу до таких повідомлень [4, с. 871–872].

Висновки. Наявність у КК України ст. 163 «Порушення таємниці листування, телефонних переговорів, поштових, телеграфних та інших повідомлень» знімає необхідність копіювання цього складу. Законодавець, регулюючи таємницю не лише повідомлень, переданих традиційними засобами зв'язку (телеграфом, поштою), а й «інших повідомлень», надав правозастосовникам можливість карати також злочинців, які перехоплюють комп'ютерні повідомлення. Однак виявлення й покарання подібних злочинців багато в чому є ускладненим особливостями розслідування та збору доказової бази за цими злочинами [11, с. 152].

Література:

1. Evans L.E. Internet Overview / L.E. Evans, Jr. – New York : 63 TEX. B.J., 2000. – 247 p.
2. Курс уголовного права : в 5 т. / под ред. Г.Н. Борзенкова и В.С. Комиссарова. – М. : Зерцало, 2002– . – Т. 4 : Общая часть. – 2002. – 786 с.
3. Волеводз А.Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества / А.Г. Волеводз. – М. : Юрлитинформ, 2002. – 546 с.
4. Federal Criminal Code and Rules : Title 18 Crime and Criminal Procedure – § 1030 Fraud and related activity in connection with computers (amendment received to February 15, 1999). West Group. – St. Paul, 1999. – 954 p.
5. Texas Computer Crimes Law [Електронний ресурс]. – Режим доступу : http://www.isot.com/OLD/supportISOT/htdocs/law.htm.
6. Edward Snowden did enlist for special forces, US army confirms [Електронний ресурс]. – Режим доступу : http://www.theguardian.com/world/2013/jun/10/edward-snowden-army-special-forces.
7. Пентагон подсчитал, что Э. Сноуден похитил 1,7 млн секретных файлов [Електронний ресурс]. – Режим доступу : http://www.rbc.ru/politics/10/01/2014/898589.shtml.
8. U.S. charges Snowden with espionage [Електронний ресурс]. – Режим доступу : https://www.washingtonpost.com/world/national-security/us-charges-snowden-with-espionage/2013/06/21/507497d8-dab1-11e2-a016-92547bf094cc_story.html.
9. Путин В.В. США для России важнее Сноудена / В.В. Путин [Електронний ресурс]. – Режим доступу : http://rbcdaily.ru/politics/562949987968395.

Беленький В. П. Киберпреступления по законодательству США

Аннотация. США является одной из самых компьютеризированных стран западного мира. Эта страна стала одной из первых, которые включили в свои законы ответственность за киберпреступления. В статье исследована сущность, формы и признаки, а также регулирование киберпреступлений по законодательству США. Анализируются составы этих преступлений, ответственность за их совершение. Статья поможет проанализировать уголовное право США в сфере киберпреступлений и усовершенствовать отечественное уголовное право.

Ключевые слова: США, киберпреступность, киберпреступление, ответственность, виды, типы, признаки.

Bielienkiy V. Cybercrimes according to the legislation of USA

Summary. USA if one of the most computerized countries of West world. This country became the one who includes in their legislation the liability for cybercrimes. The essence, features, forms and regulation of cybercrimes according to the legislation of USA are researched in this article. There are analyzed the content of these crimes and liability for them. This article will help to analyze the criminal law of USA in the field of cybercrimes and to develop native criminal law.

Key words: USA, cybercriminality, cybercrime, liability, kinds, types, characteristics.