подарунків від друзів, а не тільки як прояв гостинності. У КК України слід закріпити обумовленість між сторонами надання–одержання неправомірної угоди, обов'язковість у диспозиціях корупційних злочинів корисливого мотиву для одержувача неправомірної вигоди.

Список використаних джерел:

1. Банчук О. Запобігання і протидія корупції в органах місцевого самоврядування. Практичний посібник / О. Банчук; Швейцарсько–український проект «Підтримка децентралізації в Україні – DESPRO». – К. : ТОВ «Софія-А». – 2012. – 88 с.

2. Киричко В. М. Проблема розмежування кримінальної та адміністративної відповідальності за порушення заборон одержання неправомірної вигоди й подарунків, шляхи її вирішення. [Електронний ресурс] / В. М. Киричко // Проблеми законності. – 2017. Вип. 138. – Режим доступу: http://plaw.nlu.edu.ua/article/viewFile /105435/106111.

3. Мезенцева І. Визначення предмета корупційних злочинів [Електронний ресурс] / І. Мезенцева // Вісник Національної академії прокуратури України. – 2014. – № 5. – С. 76–81. – Режим доступу: http://nbuv.gov.ua/UJRN/Vnapu_2014_5_13.

УДК 343.346.8

АНАЛІЗ ЗАРУБІЖНОГО КРИМІНАЛЬНОГО ЗАКОНОДАВСТВА У СФЕРІ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Бараненко Роман Васильович
кандидат технічних наук, доцент,
професор кафедри професійних та спеціальних дисциплін
(Херсонський факультет Одеського державного університету внутрішніх справ, м. Херсон, Україна)
Задорожна Антоніна Юріївна
студентка
(Херсонський національний технічний університет, м. Херсон, Україна)

Поява кіберпростору сприяла також й появі кіберзлочинності. Проте кожне злочинне діяння передбачає за собою відповідальність для особи, що його вчинила. Детально проаналізовано випадки настання кримінальної відповідальності за вчинення комп'ютерних злочинів в Сполучених Штатах Америки. Розглянуто види злочинів з

використанням комп'ютера, за які передбачено відповідальність в кримінальному законодавстві Канади.

Проведено аналіз європейського кримінального законодавства у сфері протидії комп'ютерній злочинності, зокрема скандинавського, голландського, німецького, британського, французького, бельгійського, австрійського, швейцарського та ін. Наведено відповідні норми кримінального законодавства Японії та КНР.

Ключові слова: кіберпростір, кіберзлочини, комп'ютер, комп'ютерна мережа, злом, інтернет, злочинець, кримінальна відповідальність.

Анализ зарубежного уголовного законодательства в сфере противодействия киберпреступности

Бараненко Роман Васильевич
кандидат технических наук, доцент,
профессор кафедры профессиональных и специальных дисциплин
(Херсонский факультет Одесского государственного университета внутренних дел, г. Херсон, Украина)
Задорожная Антонина Юрьевна
студентка
(Херсонский национальный технический университет, г. Херсон, Украина)

Появление киберпространства способствовало также и появлению киберпреступности. Однако каждое преступное деяние предусматривает за собой ответственность для совершившего его лица. Детально проанализированы случаи привлечения к уголовной ответственности за совершение компьютерных преступлений в США. Рассмотрены виды преступлений с использованием компьютера, за которые предусмотрена ответственность в уголовном законодательстве Канады.

Проведен анализ европейского уголовного законодательства в сфере противодействия компьютерной преступности, в частности скандинавского, голландского, немецкого, британского, французского, бельгийского, австрийского, швейцарского и др. Приведены соответствующие нормы уголовного законодательства Японии и КНР.

Ключевые слова: киберпространство, киберпреступления, компьютер, компьютерная сеть, взлом, интернет, преступник, уголовная ответственность.

The Analysis of Foreign Criminal Legislation in the Field of the Counteraction to Cybercrimes

Roman Vasilyovich Baranenko,
Candidate of technical sciences, assistant professor,
professor of department of professional and special disciplines,
(Kherson Faculty of Odessa State University of Internal Affairs, Kherson, Ukraine)

Antonina Yuriyivna Zadorozhna,
student
(Kherson National Technical University, Kherson, Ukraine)

Today anyone can use information resources of the Internet, social networks or of an e-mail.

All this leads to vulnerability of users from various criminals. The emergence of the virtual information environment for the information exchange and communication between people – the cyberspace has also contributed to the emergence of cybercrimes. However, every criminal act provides responsible for the person who committed it.

Cases of criminal responsibility for committing computer crimes in the United States are analyzed in details. The attention is focused on the difficulties of prosecuting persons committing these crimes by accessing US computers abroad.

The types of computer crime for which criminal liability is provided in Canada are considered.

The analysis of European criminal law, including Scandinavian, Dutch, German, British, French, Belgian, Austrian, Swiss and others in the field of counteraction to computer crimes turned out to be interesting.

Criminal liability for such crimes is stipulated in the countries of the south-east Asia, particularly in Japan and China. Relevant norms of criminal law are provided.

Keywords: cyberspace, cybercrimes, computer, computer network, hacking, internet, criminal, criminal responsibility.

Вступ і постановка проблеми. Бурхливий розвиток інформаційних технологій призвів до зростання відносної важливості окремих аспектів суспільного життя. Внаслідок інформаційної революції основною цінністю для суспільства взагалі й окремої людини зокрема поступово стають інформаційні ресурси [1]. Сьогодні важко уявити собі особу, яка не користується інформаційними ресурсами мережі інтернет, соціальними мережами або електронною поштою.

Все це призводить до вразливості користувачів з боку різноманітних злочинців. Поява віртуального інформаційного середовища для обміну інформацією й спілкування людей між собою – кіберпростору сприяла також й появі кіберзлочинності. Проте кожне злочинне діяння передбачає за собою відповідальність для особи, що його вчинила. Тому постає питання аналізу відповідного законодавства, що регулює питання відповідальності за вчинення кіберзлочинів.

Аналіз попередніх досліджень. Дослідженням питань кримінальної відповідальності за вчинення комп'ютерних злочинів в Україні займалися Д.С. Азаров, П.П. Андрушко, П.С. Берзін, П.Д. Біленчук, В.М. Бутузов, В.Б. Вєхов, В.Д. Гавловський, В.Д. Гулкевич, М.В. Гуцалюк, М.В. Карчевський, С.Я. Лихова, М.І. Панов, М.В. Плугатир, Н.А. Савінова, С.О. Харламова, В.Б. Харченко, А.В. Черних.

Метою даної роботи є аналіз зарубіжного кримінального законодавства та вивчення особливостей характеристик об'єктивної сторони комп'ютерних злочинів.

Основний матеріал. Під кіберзлочинами будемо розуміти злочини, вчинені в кіберпросторі за допомогою засобів комп'ютерної техніки та телекомунікаційних мереж. В більшості країн Європи та Америки за їх вчинення передбачено кримінальну відповідальність.

Однією з перших країн світу, яка прийняла заходи по встановленню кримінальної відповідальності за вчинення подібних злочинів, були Сполучені Штати Америки, де комп'ютерна злочинність з'явилася дещо раніше, ніж в інших державах. У 1977 році в США було розроблено законопроект про захист федеральних комп'ютерних систем. Він передбачав кримінальну відповідальність за введення завідомо неправдивих даних до комп'ютерної системи; незаконне використання комп'ютерних пристроїв; внесення змін до процесів обробки інформації або порушення цих процесів; розкрадання грошових коштів, цінних паперів, майна, послуг, цінної інформації, що вчинені з використанням можливостей комп'ютерних технологій або з використанням комп'ютерної інформації. На основі даного законопроекту в жовтні 1984 було прийнято Закон про шахрайство та зловживання з використанням комп'ютерів – основний нормативно-правовий акт, що встановлює кримінальну відповідальність за злочини в сфері комп'ютерної інформації. В подальшому він неодноразово (в 1986, 1988, 1989, 1990, 1994 і 1996 рр.) доповнювався. Нині його включено у вигляді §1030 Титулу 18 Зводу законів США. Даний закон встановлює відповідальність за діяння, предметом посягань яких є «захищений комп'ютер» (та комп'ютерна інформація, що знаходиться в ньому) [2].

Цей кримінальний закон встановлює, що кримінальна відповідальність настає у випадках: 1) несанкціонованого доступу, коли стороння, по відношенню до комп'ютера або комп'ютерної системи, особа вторгається до них ззовні й користується ними; 2) перевищення санкціонованого доступу, коли законний користувач комп'ютера або системи здійснює доступ до комп'ютерних даних, на які його повноваження не поширюються. Закон встановлює відповідальність за сім основних складів злочинів, якими визнаються [2]:

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

– несанкціонований доступ або перевищення санкціонованого доступу до інформації з урядового відомства США, з якого б то не було захищеного комп'ютера, що має відношення до міжштатової або міжнародної торгівлі, а

також отримання інформації з фінансових записів фінансової установи, емітента карт або інформації про споживачів, що міститься в файлі керування обліком споживачів (§1030 (a) (2));

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

– шахрайство з використанням комп'ютера – доступ, що здійснюється з шахрайськими намірами, й використання комп'ютера з метою отримання чого б то не було цінного за допомогою шахрайства, включаючи незаконне використання машинного часу вартістю понад 5 тисяч доларів протягом року, тобто без оплати використання комп'ютерних мереж і серверів (§1030 (a) (4));

– умисне або з необережності пошкодження захищених комп'ютерів (§1030 (a) (5));

– шахрайство шляхом торгівлі комп'ютерними паролями або аналогічною інформацією, що дозволяє отримати несанкціонований доступ до інформації, якщо така торгівля впливає на торговельні відносини між штатами та з іншими державами, або на комп'ютер, який використовується урядом США (§1030 (a) (6));

– загрози, вимагання, шантаж та інші протиправні дії, що здійснюються з використанням комп'ютерних технологій (§1030 (a) (7)).

Деякі аспекти вчинення кіберзлочинів розглядаються в преамбулі VIII «Патріотичного Акту» США. Патріотичний акт – (англ. USA PATRIOT Act; повна назва: Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001) – федеральний закон, прийнятий в США в жовтні 2001 року, який надає владі та поліції широкі повноваження щодо надзору за громадянами [3].

Відповідно до статті 814 Закону про боротьбу з тероризмом, покарання застосовується до осіб, що пошкодили чи отримали несанкціонований доступ до захищеного комп'ютера й таким чином викликали у людини сукупний збиток більше, ніж на $5000; сприяли зриву чийогось медичного обстеження, діагностики або лікування; змушують інших осіб заподіяти шкоду; несуть загрозу громадській безпеці; або завдають шкоди урядовим комп'ютерам, які використовуються в якості інструменту для здійснення правосуддя, національної оборони або національної безпеки [4]. Розділ 814 також забороняє будь-яке вимагання грошей через захищений комп'ютер, а не тільки здирництво проти «фірми, асоціації, освітнього закладу, фінансової установи, державної установи або іншої юридичної особи» [4]. Санкцію було розширено, щоб включати до складу розділу спробу незаконного доступу або використання захищених комп'ютерів. Пошкодження захищених комп'ютерів за допомогою використання вірусів

або іншого механізму програмного забезпечення передбачає позбавлення волі терміном до 10 років, в той час як покарання за несанкціонований доступ і подальше пошкодження захищеного комп'ютера передбачає більше п'яти років позбавлення волі. У разі, якщо злочин вчинено вдруге, санкція передбачає до 20 років позбавлення волі. До Федеральних принципів винесення вироку було внесено поправки, що дозволяють застосовувати санкцію статті до будь-якої особи, яку було визнано винною в комп'ютерному шахрайстві й зловживанні, без урахування будь-яких обов'язкових мінімальних термінів позбавлення волі.

Незважаючи на таку детальну регламентацію питань кримінальної відповідальності за кіберзлочини, правоохоронні органи США відчувають значні труднощі у випадках, коли мова ведеться про притягнення до відповідальності осіб, які вчиняють ці злочини, здійснюючи доступ до комп'ютерів США з-за кордону. На думку експертів цього можна було б уникнути за умови включення до статей кримінального закону кваліфікуючих ознак – вчинення злочинів з використанням можливостей глобальних комп'ютерних мереж і здійснення несанкціонованого доступу з комп'ютерів, що знаходяться за межами США, або через них [2].

В кримінальному законодавстві Канади передбачено відповідальність за крадіжку, підробку кредитних карт або несанкціоноване використання комп'ютера (для подальшого викрадення даних кредитних карт). Санкція передбачає позбавлення волі терміном до десяти років [5].

Для осіб, які за допомогою будь-якого електромагнітного, акустичного, механічного або іншого пристрою самовільно перехоплюють приватні повідомлення, передбачено кримінальну відповідальність з позбавленням волі терміном до п'яти років [5].

У кримінальному кодексі Голландії з 1993 р. встановлено відповідальність за умисне проникнення до комп’ютера чи системи, якщо цим порушується безпека або якщо особа отримує доступ за допомогою технологічних засобів, використовуючи неправдиві сигнали, неправдивий ключ чи неправдиві повноваження. Наступне копіювання даних, які зберігались у комп'ютері чи системі, для їх використання чи передачі іншим особам, є обтяжуючою це діяння обставиною (ч. 1 і 2 ст. 138-а); неправомірне проникнення до комп’ютера, вчинене через телекомунікаційну інфраструктуру чи телекомунікаційний прилад, які використовуються для обслуговування населення, якщо внаслідок цього обчислювальну здатність комп’ютера чи системи використано для одержання незаконних доходів (ч. 3 ст. 138-а); умисне або вчинене через необережність руйнування, пошкодження чи приведення до непридатного стану комп’ютера чи системи для зберігання чи обробки даних або телекомунікаційного приладу; умисне порушення їх роботи; умисне порушення заходів безпеки

щодо них, якщо ці діяння призвели до невиправданих перешкод у зберіганні чи обробці інформації, яка використовується населенням, або до порушення роботи телекомунікаційної інфраструктури чи телекомунікаційного приладу, або якщо цими діяннями створюється загроза власності чи життю іншої особи (статті 161-s 161 septies); комп'ютерне шпигунство (ч. 2 ст. 273); умисна або необережна незаконна зміна, стирання, приведення до непридатного стану чи недоступності інформації, яка зберігається, обробляється чи передається за допомогою комп'ютера чи системи, внесення до них додаткових даних (ч. 1 і 2 ст. 350-a, ч. 1 ст. 350-b); умисні або необережні незаконні дії, спрямовані на те, щоб зробити доступними чи поширити дані й спричинити шкоду шляхом копіювання у комп'ютері чи системі (ч. 3 і 4 ст. 350-a, ч. 2 ст. 350-b); умисне або необережне руйнування, псування, приведення до непридатного стану чи до несправності, знищення комп'ютера чи системи для зберігання й обробки даних, телекомунікаційного приладу, призначених для використання населенням або для національної оборони (ст. 351 і 351-b) [6].

В даний час законодавство Німеччини включає до себе ряд статей, що передбачають відповідальність, в т.ч. і кримінальну, за різні злочини, що здійснюються за допомогою комп'ютерів і комп'ютерних мереж. Наприклад, «Комп'ютерне шахрайство» (ст. 263 a), «Підробка використовуваних даних» (ст. 269), «Обман в офіційних наукових роботах в сукупності з обробкою даних» (ст. 270), «Заміна даних» (ст. 303 a), «Комп'ютерний саботаж» (ст. 303 b), «Інформаційне шпигунство» (ст. 202 a) та ін. [7]

У Сполученому Королівстві в серпні 1990 року вступив в силу «Закон про зловживання комп'ютерами», відповідно до якого кримінальним злочином є умисний протизаконний доступ до комп'ютера або комп'ютерної інформації чи програм, що містяться в ньому (ст. 1); умисний протизаконний доступ до комп'ютера або комп'ютерної інформації чи програм, що містяться в ньому, для їх подальшого використання в протизаконних цілях (ст. 2); неправомірний доступ до комп'ютерної інформації на машинному носії, в комп'ютері, комп'ютерній системі або мережі, з метою, або якщо це призвело до знищення, блокування, модифікації, або копіювання інформації, порушення роботи комп'ютера, комп'ютерної системи або мережі (ст. 3). А в «Законі про тероризм 2000 року» визначення тероризму вперше розширюється і зачіпає область кіберпростору [2].

В Англії несанкціонований доступ до комп'ютерних матеріалів карається позбавленням волі на строк 12 місяців (або до 6 місяців в Шотландії) і/або штрафом, «що не перевищує 5-го рівня за стандартною шкалою» (з 2015 року, без обмежень). Несанкціонований доступ з метою здійснення або сприяння здійсненню нових злочинів карається

позбавленням волі на строк до 12 місяців/максимальний розмір штрафу (або до 6 місяців в Шотландії) в порядку сумарного виробництва та/або 5 років/штрафом за звинуваченням.

Несанкціонована модифікація комп'ютерного матеріалу карається 12 місяцями позбавлення волі/максимальний розмір штрафу (або 6 місяців в Шотландії) в порядку сумарного виробництва та/або 10 років/штраф за звинуваченням [8].

У Великому герцогстві Люксембург норми, що регламентують відповідальність за вчинення комп'ютерних злочинів, містяться в ст. 509-1, 509-2, 509-3, 524 Кримінального кодексу.

Статтею 509-1 КК Люксембурга передбачено відповідальність за неправомірний доступ до системи чи частини системи обробки даних і незаконне перебування в такій системі. Санкція за цей злочин передбачає штраф чи ув'язнення на строк від 2 місяців до року. Якщо вказані дії призвели до зміни чи знищення даних, що містяться в системі, то верхня межа строку ув'язнення збільшується до 2 років [9].

Стаття 509-2 забороняє вчинення дій, що призводять до ускладнення чи зміни функціонування системи автоматичної обробки даних. В якості санкції передбачено штраф чи позбавлення волі на строк від 3 місяців до 3 років [9].

Стаття 509-3 направлена на охорону цілісності й якості даних. Згідно з нею особа, яка умисно и без відповідних повноважень вводить дані до електронної системи їх обробки, видаляє чи змінює дані, що містяться в цій системі, змінює дію системи чи спосіб передачі даних, підлягає кримінальній відповідальності (штраф чи ув'язнення на строк від 3 місяців до 3 років). Згідно з ст. 524 Кримінального кодексу Люксембурга будь-яке втручання до телекомунікацій є злочином, за який особа може бути піддана штрафу чи ув'язненню від 1 місяця до 3 років [9].

В бельгійському кримінальному законодавстві [6] є стаття 210-b, в якій передбачено відповідальність за підлог шляхом введення даних до інформаційної системи, зміни чи знищення даних, які в ній зберігаються, обробляються нею чи передаються, або шляхом зміни будь-яким технологічним способом можливого використання цих даних (§1); використання завідомо неправдивих і отриманих зазначеним способом даних (§2). У статті 504-quater йдеться про досягнення шахрайської майнової вигоди для себе чи для іншої особи шляхом введення до інформаційної системи, зміни чи скасування даних, які в ній зберігаються, обробляються чи нею передаються, або шляхом зміни будь-яким технологічним способом можливого використання цих даних. В розділі IX-bis «Правопорушення проти конфіденційності, недоторканності й доступності інформаційних

систем та даних, які накопичуються, обробляються й передаються цими системами» встановлено відповідальність за такі діяння:

1) завідомо без дозволу вторгнення до інформаційної системи або залишення у ній (§1), у т.ч. з наміром вчинити обманну операцію (обтяжуюча обставина); перевищення своїх повноважень по доступу до інформаційної системи з наміром обманути чи заподіяти шкоду (§2); дії, передбачені §1 або 2, поєднані з:

а) вилученням, незалежно від способу, даних, накопичених, оброблених або переданих інформаційною системою;

б) будь-яким використанням інформаційної системи, що належить третій особі, або користуванням нею для проникнення до інформаційної системи іншої особи;

в) заподіянням певної шкоди, навіть неумисно, інформаційній системі чи даним, які накопичуються, обробляються й передаються нею (§3); вчинені з обманним наміром чи з метою заподіяння шкоди пошук, збирання, надання у розпорядження, розповсюдження чи торгівля даними, які було накопичено, оброблено чи передано інформаційною системою й з використанням яких можуть бути вчинено діяння, визначені у §1-3 (§5);

2) введення до інформаційної системи, зміна чи скасування даних, або зміна будь-яким технологічним способом можливого використання даних в інформаційній системі, вчинені з метою заподіяння шкоди (§1), або які заподіяли шкоду відомостям, що знаходились в інформаційні системі (§2), або які перешкодили правильній роботі інформаційної системи (§3); вчинені з обманним наміром чи з метою заподіяння шкоди вивчення, надання у розпорядження третіх осіб, розповсюдження чи торгівля даними, які були накопичено, оброблено чи передано інформаційною системою й які завідомо можуть бути використано для викривлення інших даних, закладених в інформаційну систему (§4).

В австрійському кримінальному законодавстві [10] встановлено відповідальність за незаконний доступ до комп'ютерної системи (§118-a); порушення телекомунікаційної таємниці (§119); незаконне перехоплення даних, що передаються комп'ютерною системою, з корисливою метою (§119-a). При цьому під даними розуміються дані про особу, будь-які інші дані або програми; незаконне (неправомірне) використання приладів запису й підслуховування (§120, абз. 2-a); пошкодження даних (§126-a); порушення функціонування комп'ютерної системи (§126-b); незаконне (неправомірне) використання комп'ютерних програм або даних доступу (§126-e); шахрайська, вчинена обманним шляхом, обробка даних (§148-a); фальсифікація даних (§225-a).

Чинний Кримінальний Кодекс Швейцарії [11] передбачає відповідальність за такі комп'ютерні злочини, як придбання з корисливих

мотивів даних, зібраних чи оброблених електронним або іншим схожим способом, якщо ці дані особливо захищені від неправомірного доступу (ст. 143); неправомірне проникнення до чужої, особливо охоронюваної системи обробки даних без корисливої мети (ст. 143-bis); неправомірна зміна, знищення чи пошкодження даних, зібраних або переданих електронним або іншим схожим способом (ч. 1 ст. 144-b); шахрайське зловживання з обладнанням для обробки даних – неправильне, неповне чи неправомірне використання даних, інший вплив на процес обробки чи передачі даних з корисливою метою, яка досягається забезпеченням відстрочки настання майнової шкоди (ст. 147); виробництво й випуск в обіг техніки, її складових частин або програми для обробки даних, призначених для незаконного розшифрування радіопрограм чи служб телекомунікації (ст. 150-b).

Посяганням на системи автоматизованої обробки даних присвячено підрозділ 3 розділу II Книги 3 кримінального кодексу Франції. До них відносяться зокрема: обманне отримання чи обманне збереження доступу до вказаної системи, у т.ч. таке, що спричинило знищення чи зміну даних або погіршення функціонування системи (ст. 323-1); перешкоджання роботі чи порушення функціонування системи (ст. 323-2); обманне введення інформаційних даних до системи або обманне знищення чи зміна даних, які в ній містяться (ст. 323-3); участь в організованій групі чи змові, спрямованих на підготовку до злочинних діянь, передбачених статтями 323-1, 323-3 (ст. 323-4).

Окремо виділено посягання, пов'язані з використанням картотек і обробкою даних на ЕОМ: вчинення або віддача вказівки про вчинення автоматизованої обробки поіменних даних без здійснення передбаченої законом формальності (ст. 226-16); вчинення або надання вказівки про вчинення обробки цих даних без вжиття всіх заходів, необхідних для того, щоб забезпечити безпеку даних (ст. 226-17); збір і обробка даних незаконним способом (ст. 226-18); введення або збереження в пам'яті ЕОМ заборонених законом даних (ст. 226-19); збереження визначених даних понад встановлений законом термін (ст. 226-20); використання даних з іншою метою, ніж це було передбачено (ст. 226-21); розголошення даних, здатне призвести до зазначених у законі наслідків (ст. 226-22).

Французьким кримінальним законодавством передбачено також відповідальність за дії, вчинені з комп'ютерною інформацією на шкоду інтересам держави: збір або передача іноземній державі інформації, яка міститься в пам'яті ЕОМ або у картотеці, знищення, розкрадання, вилучення або копіювання даних, що мають характер секретів національної оборони, що утримуються в пам'яті ЕОМ або в картотеках, а також ознайомлення з ними даними сторонніх осіб (статті 411-7, 411-8, 413-9, 413-10, 413-11).

Стаття 186-1 КК Франції встановлює відповідальність за неправомірне перехоплення даних у телекомунікаційних системах. Нарешті, ще одним видом «комп'ютерного» злочинного діяння є сексуальна агресія, вчинена шляхом використання телекомунікаційних мереж і поширення повідомлень, адресованих невизначеному колу осіб (ст. 222-28) [6].

Кримінальним кодексом Італії передбачено відповідальність за доступ до комп'ютерів або систем, захищених заходами безпеки, або доступ проти вираженого або такого, що мається на увазі, бажання власника (ст. 615-t); незаконне заволодіння й поширення кодів, паролів або інших засобів доступу до комп'ютерів чи телекомунікаційних систем, вчинене з метою одержання прибутку для себе чи для третіх осіб, або з метою заподіяння шкоди (ст. 615 quater); розповсюдження шкідливих комп'ютерних програм (ст. 615-quinquieses); перехоплення або переривання комп'ютерних чи телекомунікацій (ст. 617-quater); встановлення апаратури для перехоплення, запобігання або переривання комп'ютерних чи телекомунікацій (ст. 617-quinquieses); фальсифікація змісту комп'ютерних чи телекомунікацій (ст. 617-sexieses).

Розділом 5 Книги 2 передбачено відповідальність також за пошкодження чи знищення громадських інформаційних інфраструктур, баз даних програм, задіяних на підприємствах комунального обслуговування (ч. 2 ст. 420), а розділом 13 – за знищення, пошкодження чи приведення до непридатного стану комп'ютерних систем чи телекомунікацій, вчинені не уповноваженою особою (ст. 635-b) і за комп'ютерне шахрайство (ст. 640-i) [6].

В китайському кримінальному законодавстві [12] передбачено відповідальність для осіб, що порушують державні правила й вторгаються до комп'ютерних систем з інформацією про державні справи, будівництво оборонних споруд, – до трьох років позбавлення волі (ст. 285 ч.1).

Для осіб, що порушують державні правила й вилучають, змінюють, додають інформацію й втручаються до роботи комп'ютерних інформаційних систем, що призводить до ненормальних операцій в системах і тяжких наслідків, передбачено до п'яти років позбавлення волі; коли наслідки особливо тяжкі – від п'яти років позбавлення волі (ст. 285 ч.2).

Для осіб, що порушують державні правила й вилучають, змінюють або додають дані до прикладних програм, встановлених до системи, або обробляють й передають дані за допомогою комп'ютерних систем, що викликає тяжкі наслідки, передбачено покарання до п'яти років позбавлення волі (ст. 285 ч.2).

Для осіб, що навмисно створюють й поширюють комп'ютерні віруси та інші програми, що підривають нормальне функціонування комп'ютерної системи й викликають тяжкі наслідки, також передбачено покарання до п'яти років позбавлення волі (ст. 286).

Передбачено також відповідальність за використання комп'ютера для заволодіння грошима шляхом шахрайства або їх розкрадання, для хабарництва й нецільового використання громадських коштів, для заволодіння шляхом крадіжки державною таємницею й здійснення інших злочинів (ст. 287).

В японському кримінальному законодавстві [13] передбачається покарання за перешкоджання виконанню професійної діяльності шляхом пошкодження ЕОМ або іншим способом (ст. 234-II) за протиправне отримання вигоди шляхом виготовлення електромагнітного запису, що суперечить істині.

Цікаво буде проаналізувати й скандинавське кримінальне законодавство.

У §262 Кримінального кодексу Норвегії встановлено відповідальність за несанкціонований доступ до «захищеної служби» (тобто до телевізійного чи радіосигналу, послуг, які передаються електронним шляхом за запитом користувача служби, коли для отримання даних потрібен відповідний дозвіл), поєднаний з створенням, введенням, розповсюдженням, продажем, здачею, розпорядженням, встановленням, експлуатацією чи зміною декодувального пристрою для одержання прибутку; анонсуванням чи рекламуванням декодувального пристрою з метою одержання прибутку; намаганням поширити декодувальний пристрій [6].

У Кримінальному кодексі Швеції відповідальність за вчинення комп'ютерних злочинів прямо не передбачено. Проте Швеція була першою країною у світі, що прийняла 4 квітня 1973 року «Закон про дані», який ввів нове поняття до традиційного законодавства – «зловживання за допомогою комп'ютера».

Стаття 263 Кримінального кодексу Данії передбачає кримінальну відповідальність за: порушення таємниці зв'язку (у т.ч. електронної пошти); незаконне проникнення до місць зберігання приватної власності (поширюється і на дані, що зберігаються в комп'ютерній системі); перехоплення даних у телекомунікаційних мережах; незаконний доступ до комп'ютерних даних і комп'ютерних програм. Стаття 193 цього кодексу визначає як злочин вторгнення до громадських систем зв'язку, систем обробки даних, критичних інфраструктур (водопостачання, електро- і газопостачання, охорони здоров'я) та порушення їх нормального функціонування [6].

Стаття 38 Особливої частини Кримінального кодексу Фінляндії встановлює відповідальність особи, яка порушує таємницю повідомлень, адресованих іншій особі, одержує або намагається одержати інформацію про зміст повідомлень, що містять текст, зображення, дані, або зміст іншої форми телекомунікаційного зв'язку, або пошкоджує, знищує, приховує

зазначені повідомлення. На практиці може бути застосована до комп'ютерних злочинів і ст. 28, яка передбачає відповідальність за незаконне використання чужого устаткування, машин. Заподіяння шкоди даним, що зберігаються в комп'ютері або системі, може потягнути відповідальність за ст. 35, а неправомірна модифікація інформації – за статтею 33 [6].

Висновки. Проаналізувавши зарубіжне кримінальне законодавство, можна зробити висновок, що воно має схожі підходи до побудови правових норм, що містять признаки складу злочинів, що посягають на суспільні відношення в сфері охорони інформації та функціонування комп'ютерних систем і мереж. Це можна пояснити єдністю підходів в теорії кримінального права, а також загальними принципами, що сформульовані в міжнародно-правових документах, направлених на боротьбу з кіберзлочинами [14].

Список використаних джерел:

1. Ющук О.В. Інформаційна безпека користувачів мережі Інтернет / О.В. Ющук // Наукові записки. Серія «Культура і соціальні комунікації». – 2009. – Випуск 1. – С.224-231.

2. Мазуров В.А. Компьютерные преступления: анализ уголовного законодательства США и Германии /В.А. Мазуров, Д.П. Потапов, В.В. Сорокин. // Известия Алтайского государственного университета. – 2005. – № 2. – С. 59-66.

3. Uniting and strengthening America by providing appropriate tools required to intercept and obstruct terrorism : USA PATRIOT ACT. – 2001 [Електронний ресурс]. – Режим доступу: http://frwebgate.access.gpo.gov.

4. 18 U.S. Code § 1030 – Fraud and related activity in connection with computers [Електронний ресурс]. – Режим доступу: https://www.law.cornell.edu/uscode/text /18/1030.

5. Criminal Code R.S.C., 1985, C-46 An Act respecting the Criminal Law [Електронний ресурс]. – Режим доступу: http://www.canlii.org/en/ca/laws/stat/rsc- 1985-c-c-46/101543/rsc-1985-c-c-46.html.

6. Лихова С.Я. Методичні рекомендації для підготовки студента до практичних занять з дисципліни «Порівняльне кримінальне право» для студентів спеціальності 081 «Право». / С.Я. Лихова. – К. : НАУ, 2016. – 102 с.

7. Дворецкий М.Ю. Преступления в сфере компьютерной информации в России и зарубежных государствах: проблемы квалификации, уголовной ответственности и наказания /М.Ю. Дворецкий, А.Ю. Карамнов. // Вестник Тамбовского государственного университета. – 2011. – Вып. 11. – С.395-399.

8. Police and Justice Act 2006 [Електронний ресурс]. – Режим доступу: http://www.legislation.gov.uk/ukpga/2006/48/part/5/crossheading/computer-misuse.

9. Киберпреступность [Електронний ресурс]. – Режим доступу: https://sites.google.com/site/kiberprestupnost1026/home/ugolovnaa-otvetstvennost-v-sfere-komputernoj-informacii-za-rubezom

10. Уголовный Кодекс Австрии /МГУ им. М.В. Ломоносова; Пер. с нем. и предисл. А.В. Серебренниковой; Науч. ред. Н.Е. Крылова. – М. : Зерцало-М, 2001. – 144 с.

11. Уголовный кодекс Швейцарской Конфедерации. – СПб. : Изд-во Юридический центр Пресс, 2002. – 350 с.

12. Criminal Law of the People's Republic of China [Електронний ресурс]. – Режим доступу: http://www.fmprc.gov.cn/ce/cgvienna/eng/dbtyw/jdwt/ crimelaw/t209043.htm.

13. Уголовный кодекс Японии / Под ред. и с предисл. проф. А.И. Коробеева. Пер. с япон. Владивосток: Изд-во Дальневост. ун-та, 2000. – 84 с.

14. Бараненко Р.В. Анализ уголовного законодательства в сфере противодействия киберпреступности государств-участниц СНГ / Р.В. Бараненко, А.Ю. Задорожная // Материалы международной научно-практической конференции «Вклад молодых исследователей в развитие публичного управления». – Кишинёв: Академия публичного управления Правительства Республики Молдова, 2017. – С.277-281.

УДК 343.140.02

СТАНДАРТИ ДОВЕДЕННЯ В КРИМІНАЛЬНОМУ СУДОЧИНСТВІ КАНАДИ

Степаненко Віктор Вікторович
кандидат юридичних наук,
Начальник тренінгового центру Головного Управління Національної поліції в Херсонській області (м. Херсон, Україна)

У статті робиться висновок, що в правовій системі Канади запроваджено систему стандартів доведення, що стосуються різних стадій та інститутів кримінального процесу. За ступенем переконання зазначені стандарти можна представити у виді ієрархії: «повітря реальності», «достатність доказів», «розумні підстави», «баланс ймовірностей», «поза розумним сумнівом». Стандарт «доказу, що породжує розумний сумнів», на відміну від інших, передбачає не створення переконання, а його руйнування.

Ключові слова: *стандарти доведення, достатність доказів, повітря реальності, розумна підстава, баланс ймовірностей, поза розумним сумнівом*