УДК 343.3

Ю. М. Піцик
начальник відділу роботи з кадрами
прокуратури міста Києва

МІЖНАРОДНИЙ ДОСВІД У СФЕРІ ПРОТИДІЇ ЗЛОЧИНАМ ПРОТИ ВЛАСНОСТІ, ЩО ВЧИНЯЮТЬСЯ У КІБЕРПРОСТОРІ

Постановка проблеми. Кіберзлочини (у тому числі й кіберзлочини проти власності) є злочинами міжнародного рівня, оскільки відбуваються поза державними кордонами. У зв'язку з цим у багатьох країнах світу сформувалися власні уявлення про протидію кіберзагрозам. Звісно ж, що для розробки найбільш ефективних заходів протидії кіберзлочинам проти власності в Україні необхідно звернутися до досвіду міжнародних організацій і зарубіжних країн. Через транскордонний характер таких кіберзлочинів необхідність у міжнародному врегулюванні даної проблеми виникла ще в 70-х, 80-х роках минулого століття.

Аналіз останніх досліджень і публікацій. Питанням нормативно-правового визначення основних термінів у сфері інформаційної безпеки приділялася увага у наукових працях Д. Азарова, С. Бородіна, О. Книженко, О. Користіна, Л. Краснова, М. Карчевського, М. Литвинова, Ю. Ляпунова, С. Максимова, А. Музики, А. Новікова, О. Радутного, М. Погорецького та інших.

Метою статті є дослідження міжнародного досвіду у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі.

Результати дослідження. У той час у XX ст. у багатьох країнах (Італія – 1978 р., Австралія – 1979 р., Великобританія – 1981 р., США – 1980 р., Данія і Канада – 1985 р., Німеччина – 1986 р., Австрія, Японія і Норвегія – 1987 р., Франція і Греція – 1988 р.) вже існували перші норми про встановлення кримінальної та адміністративної відповідальності за вчинення комп'ютерних злочинів. Однак ці норми дуже відрізнялися одна від одної, вони містили різні визначення одного і того ж злочину, трактувалися по-різному і часто суперечили одна одній.

У зв'язку з цим, з метою уніфікації національних законодавств 13 вересня 1989 року на засіданні Комітету міністрів Ради Європи була прийнята Рекомендація № 89 (далі – Рекомендація), що містить перелік комп'ютерних правопорушень. Країнам-учасницям ЄС було рекомендовано на основі прийнятого переліку розробити єдину кримінальну стратегію боротьби з кіберзлочинами.

Зокрема перший перелік містив «мінімальний» список правопорушень, заборонених на території ЄС. До них було віднено: 1) комп'ютерне шахрайство; 2) комп'ютерна підробка; 3) пошкодження комп'ютерної інформації та комп'ютерних програм; 4) комп'ютерний саботаж; 5) несанкціонований доступ до комп'ютерних мереж; 6) несанкціоноване перехоплення даних; 7) несанкціоноване копіювання захищених комп'ютерних програм.

Другий список містив додатковий («необов'язковий») перелік правопорушень. До них було віднесено: 1) зміна інформації або комп'ютерних програм; 2) комп'ютерне шпигунство; 3) протизаконне застосування комп'ютера; 4) несанкціоноване застосування захищених комп'ютерних программ [1].

Ця Рекомендація була однією з перших реакцій міжнародної спільноти на кіберзагрозу, і, що примітно, «мінімальний» або обов'язковий перелік правопорушень, заборонених на території ЄС очолив такий злочин проти власності як кібершахрайство. Через кілька років, на 93-му пленарному засіданні 56-ій сесії Генеральної Асамблеї ООН, була прийнята Резолюція №56 / 261 від 31 січня 2002 року, що закликає до посилення боротьби з комп'ютерною злочинністю. У Резолюції було запропоновано розвивати національні законодавства країн-членів ООН про кримінальну відповідальність за кіберзлочини і розробити комплекс заходів щодо боротьби зі злочинами, пов'язаними з використанням високих технологій та компьютерів.

У цей день проблема кіберзлочинності вийшла за межі окремих країн і стала однією з світових проблем, нарівні з міжнародним тероризмом і торгівлею наркотиками. Особливу роль в питанні протидії міжнародній кіберзлочинності виконувала «Велика Вісімка» (G-8). Так, 26 червня 1996 року у Франції, в місті Ліон (Франція) відбулися чергові збори «G-8», підсумком якого став Регламент № 16, згідно якого держави-члени «G-8» повинні змінити законодавчі норми, задля гарантування криміналізації і караності діянь, які вчиняються з використанням сучасних технологій.

Держави-члени «G-8» домовилися про вдосконалення зв'язку між співробітниками правоохоронних органів різних країн з метою обміну досвідом та сприяння в подальшій діяльності. На виконання даного Регламенту була створена т.зв. «Ліонська група. Через деякий час, за прикладом Німеччини і Франції, в інших країнах-членах «G-8» були створені спеціальні правоохоронні органи, які в цілодобовому режимі здійснюють

комплекс заходів щодо розвитку міжнародного співробітництва в боротьбі з кіберзлочинністю [2].

На той час в Німеччині в складі Поліцейського управління Мюнхена з 1994 року вже існувала спеціальна Група по боротьбі зі злочинами в сфері високих технологій, а у Франції – Служба з протидії зловживанням у сфері високих технологій. У Великобританії в 2001 році було створено Національне підрозділ по боротьбі зі злочинами в сфері високих технологій, а 1 квітня 2006 було створено Національне агентство з боротьби з організованою злочинністю. У зв'язку з реформою 2013 року функції по боротьбі з комп'ютерною злочинністю були передані Національному підрозділу протидії кіберзлочинам [3].

У 2013 році влада Японії також повідомила про створення відділення поліції по боротьбі з кіберзлочинам. Європейський союз також відреагував на проблему кіберзлочинності, створивши цілу мережу правоохоронних органів для боротьби з нею: «Європейський центр кіберзлочинів» (European cybercrime centre), або «ЄС-3», який складається з 10 самостійних груп і команд, які здійснюють аналіз статистичних даних, підготовку спеціальних способів виявлення і затримання кіберзлочинців тощо.

Ще одним міжнародним актом, спрямованим на протидію комп'ютерним злочинам, є Будапештська Конвенція Ради Європи «Про кіберзлочинність» від 23 листопада 2001 року. Конвенція поділяє всі кіберзлочини на 5 груп: 1. злочини проти конфіденційності, цілісності та доступності комп'ютерних даних і систем (незаконний доступ, перехоплення; втручання в дані і в систему); 2. злочини, пов'язані з використанням комп'ютера як засобу вчинення злочинів, тобто як засіб маніпуляції інформацією (комп'ютерне шахрайство та підроблення); 3. злочини, пов'язані з контентом, тобто змістом даних, розміщених в комп'ютерних мережах; 4. злочини, пов'язані з порушенням авторського права і суміжних прав; 5. акти расизму і ксенофобії.

У 2010 році в Бразилії пройшов дванадцятий Конгрес ООН, на якому обговорювалися питання боротьби з комп'ютерними злочинами і розробки державної кібербезпеки. На Конгресі було розглянуто рекомендація щодо необхідності вивчення питання кіберзлочинності і прийняття рішення по розробці Глобальної Конвенції щодо боротьби з нею [4].

Безумовно, на міжнародному рівні проблема протидії кіберзлочинам, у тому числі і кіберзлочинам проти власності, стоїть дуже гостро. У той час як на міжнародному рівні розгортаються дискусії і суперечки, на національному рівні багато держав самостійно протидіють таким злочинам, приймаючи державні стратегії кібербезпеки і удосконалюючи кримінальне законодавство. Значення стратегій кібербезпеки різних країн складно переоцінити – вони є універсальним маркером, за допомогою якого можна простежити, в які сфери суспільного життя тієї чи іншої країни проникла кіберзлочинність. Однак, згідно з даними Європейського агентства з мережевої інформаційної безпеки («ENISA»), не у всіх країнах існує власна стратегія кібербезпеки.

Серед найпоширеніших напрямків державної політики щодо боротьбі з кіберзлочинами в різних країнах стали:

1. захист стратегічних і урядових інформаційних систем від кібер-атак і актів кібер-тероризму (Німеччина, Великобританія, Канада, Литва, Люксембург, Нідерланди, США, Естонія);

2. правове регулювання, а також вдосконалення кримінального та інформаційного законодавства (Німеччина, Канада, Люксембург, США, Естонія, Японії);

3. захист інформації та персональних даних (Словаччина, Франція, Чеська Республіка, Литва);

4. державне і міжнародне співробітництво (Люксембург, США, Японія). Серед інших напрямків можна виділити навчання співробітників правоохоронних органів і інформування громадян про кібер-загрози (Люксембург, Естонія) та просування міжнародних стандартів економічної безпеки (США, Люксембург).

З аналізу стратегій кібербезпеки різних країн видно, що найбільш загальним напрямком державної політики є захист стратегічних і урядових інформаційних систем, таких як інформаційна система на об'єктах атомної енергетики, об'єктах бюджетної та фінансової сфери, державних банках, в нафтопромисловому і військово-промисловому комплексі. Отже, більшість країн, які розробили національні стратегії кібербезпеки, сприймають загрозу від кіберзлочинів, як загрозу національній безпеці.

Основним заходом протидії в більшості випадків є правове регулювання: вдосконалення кримінального, адміністративного та інформаційного законодавства, криміналізація нових діянь, посилення відповідальності за вже існуючі кіберзлочини.

Законодавство різних країн має безліч особливостей і відмінностей, проте існують норми, що зустрічаються в Кримінальних кодексах майже всіх країн, до них можна віднести такі кіберзлочини проти власності: комп'ютерне шахрайство або комп'ютерне розкрадання; викрадення відомостей, що становлять комерційну таємницю шляхом неправомірного доступу до комп'ютерної інформації (кіберкрадіжка); вимагання з використанням засобів комп'ютерної техніки тощо.

Особливість кібершахрайства і його основна відмінність від звичайного шахрайства в законо-

давстві всіх країнах відображені по-різному, але зміст залишається одним – це розкрадання чужого майна шляхом використання засобів комп'ютерної техніки.

Зокрема Кримінальний кодекс Республіки Білорусь [5] в Примітці 1 до Глави 24 «Злочини проти власності» дає визначення розкрадання як «умисне протиправне безоплатне заволодіння чужим майном або правом на майно з корисливою метою шляхом крадіжки, грабежу, розбою, вимагання, шахрайства, зловживання службовими повноваженнями, привласнення, розтрати або використання комп'ютерної техніки». Іншими словами, розкрадання, вчинене з використанням комп'ютерної техніки, є самостійною формою розкрадання в законодавстві Республіки Білорусь.

Так, ця форма розкрадання передбачена статтею 212 КК Республіки Білорусь. Відповідно до частини 1 цієї статті викрадання майна шляхом зміни інформації, що обробляється в комп'ютерній системі, що зберігається на електронних носіях або переданої мережами передачі даних, або шляхом введення в комп'ютерну систему неправдивої інформації карається штрафом, або позбавленням права обіймати певні посади або займатися певною діяльністю, або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років, або позбавленням волі на той самий строк.

Викрадання шляхом використання комп'ютерної техніки також згадується в статтях: викрадання наркотичних засобів, психотропних речовин та їх прекурсорів (ст. 327 КК Республіки Білорусь); викрадання радіоактивних матеріалів (ст. 323 КК Республіки Білорусь); викрадання вогнепальної зброї, боєприпасів або вибухових речовин (ст. 294 КК Республіки Білорусь) тощо.

У статті 216 КК Республіки Білорусь описані можливі способи заподіяння майнової шкоди без ознак розкрадання, до яких крім обману і зловживання довірою віднесена і модифікація комп'ютерної інформації.

Кримінальний кодекс Данії [6] у статті 279 «а» визначає комп'ютерне шахрайство *(atabedrageri)* як «незаконну зміну, доповнення або стирання інформації або програми, яка використовується для електронної обробки даних з метою отримання для себе або для інших осіб незаконної вигоди».

Кримінальний кодекс Італії містить одразу дві статті щодо комп'ютерного шахрайства *(Frode informatica)*. Стаття 640 КК Італії присвячена звичайному комп'ютерному шахрайству, тобто розкрадання, вчиненого шляхом «втручання в роботу комп'ютерних систем», в той час як стаття 640 (1) присвячена пособництву в комп'ютерному шахрайстві шляхом видачі сертифіката електронного подпісу [7].

У статті 287 Кримінального кодексу Китайської Народної Республіки встановлюється відповідальність за використання комп'ютера для заволодіння грошовими коштами шляхом шахрайства чи іншого *розкрадання (liyong jisuanji shishi fanzui de tishi)*. Дана стаття є бланкетною, в залежності від розміру і ступеня шкоди, санкція визначається іншими статтями Кримінального кодексу КНР, при цьому максимальним видом покарання за вчинення даного злочину є смертна кара [8].

Пункт «а» частини 3 статті 138ab КК Нідерландів передбачає відповідальність за «віртуальне шахрайство». Згідно з цим пунктом «неправомірне проникнення в комп'ютер, вчинене через телекомунікаційну інфраструктуру або телекомунікаційний пристрій, що використовується для обслуговування населення («Інтернет») з метою отримання для себе незаконних доходів, карається позбавленням волі на строк до чотирьох років або штрафом четвертої категорії». Цікавим є той факт, що даний злочин розташоване в Розділі V «Злочини проти громадського порядку» [9].

В розділ XXXV «Злочини проти власності» КК Республіки Польщі включена стаття 287, що встановлює відповідальність за «розкрадання шляхом шахрайства, що супроводжується знищенням, зміною, модифікацією комп'ютерної інформації». Закон США «Про шахрайство і зловживання з використанням комп'ютера» №1030 1986 року встановлює поняття «шахрайство з використанням комп'ютера» *(fraud with computers)*, під яким в пункті (A) (4) розуміється «умисне, з метою розкрадання, здійснення неправомірного доступу до захищеного комп'ютера або здійснення такого доступу без дозволу» [10].

Відповідальність за комп'ютерне шахрайство передбачена в статті 263a КК ФРН *(computerbetrug)*. Відповідно до частини 1 цієї статті кожен, «хто діє з метою отримання для себе або третьої особи протиправної майнової вигоди і цим завдає шкоди майну іншої особи за допомогою впливу на результат обробки даних комп'ютера, складаючи неправильні програми, використи-користовуючи неправильны або неповны даны, несанкціоноване застосування даних або впливу на такий процес будь-яким іншим неправомірним способом, підлягає кримінальній відповідальності і покаранню у вигляді позбавлення волі на строк до 5 років або у вигляді штрафа» [11].

У Кримінальному кодексі Естонії [12] стаття 268 «Комп'ютерне шахрайство» *(arvutikelmus)* розташована у Главі 14 «Злочини у сфері комп'ютерної інформації та обробки даних», згідно з якою «отримання чужого майна, майнової або іншої вигоди шляхом введення комп'ютерних програм або інформації, їх модифікації, знищення, блокування або іншого виду втручання в процес обробки інформації, що впливає на результат обробки інформації і обумовлює

заподіяння прямого майнового або іншого шкоди власності другої про особи, карається штрафом, або арештом, або позбавленням волі на строк від одного року до шести років».

У Південній Кореї шахрайство з використанням комп'ютера *(keompyuteodeung sayongsagi)* передбачено статтею 247-2 Кримінального кодексу. Воно може бути вчинено шляхом використання інформації, введення помилкових або неналежним чином оброблених даних в технічні засоби, включаючи комп'ютер [13].

В Японії діє Закон «Про несанкціоноване проникнення в комп'ютерні мережі» 2000 року. Даний закон не виділяє комп'ютерне шахрайство як самостійний вид злочинів, але встановлює відповідальність за несанкціоноване проникнення в комп'ютерні мережі з метою викрадення.

Таким чином можна побачити, що законодавці різних країн пішли різними шляхами в визначенні кібершахрайства: одні визнали його в якості самостійного виду злочинів проти власності, інші виділили в якості нового виду шахрайства, треті при побудові норми використовували в якості способу неправомірний доступ до комп'ютерної інформації.

З огляду на історичний аспект кожної з країн, а також їх юридичні традиції, кожен з варіантів має право на існування, однак для України найбільш прийнятним, на нашу думку, є підхід Республіки Білорусь, кримінальне законодавство якої найбільш близьке до нашого.

Наступним видом кіберзлочинів проти власності є «кібервимагання». Зокрема кібервимагання закріплено в Кримінальному законодавстві Нідерландів. Так, частина 2 статті 317 КК Нідерландів виступає в якості примітки до статті щодо класичних складів вимагання *(afpersing)*. Згідно з цією статтею, «покарання, передбачене в частині 1 статті 317 КК Нідерландів (вимагання), також застосовується до особи, яка висловлює вимоги під загрозою пошкодження або знищення даних, що зберігаються на комп'ютерному пристрої».

Подібний склад закріплений в пункті (A) (7) Закону № 1030 США: «вимагання з використанням комп'ютера» *(extortion with computers)* – «то є запит або вимога грошей або інших цінних предметів, під загрозою заподіяння шкоди захищеному комп'ютерові або під загрозою неправомірного доступу до інформації, що зберігається в ньому». За вчинення даного діяння передбачено покарання у вигляді штрафу та / або позбавлення волі на строк до 10 років. Варто зазначити, що у вітчизняному кримінальному законодавстві на сьогоднішній день відсутня спеціальна норма про таке вимагання.

Окрім кримінально-правового регулювання, в якості заходів протидії кіберзлочинам в зарубіжних країнах застосовуються і інші, часто більш ефективні заходи. Так, проблема анонімності користувачів кіберпростору, що є однією з причин існування кіберзлочинності, в деяких країнах вирішена на адміністративному рівні.

Наприклад, після терористичного акту 11 березня 2004 року в Мілані італійська влада зобов'язали всіх користувачів Інтернет-кафе і громадських точок доступу в мережу «Інтернет» пред'являти паспорт або ідентифікаційну карту. Без пред'явлення таких документів співробітники Інтернет-кафе не мають права надати користувачеві доступ в мережу.

Схожим шляхом пішла влада Китайської Народної Республіки в 2011 році. Кожен користувач китайського сегменту інформаційного простору при реєстрації в соціальних мережах і на інших сайтах зобов'язаний вводити паспортні дані, інакше доступ до таких сайтів для цього користувача буде закритий. Такі заходи були викликані поширенням шахрайства в кіберпросторі КНР. Вони сильно вплинули на зовнішній вигляд кіберпростору Китаю, фактично знищивши свободу спілкування. Однак свій внесок у протидію кіберзлочинності дані нововведення внесли – рівень кіберзлочинності в соціальних мережах Китаю різко знизився.

Безумовно, нормативне регулювання на сьогоднішній день залишається найпоширенішим заходом протидії кіберзлочинів у всіх країнах, в той час як інші заходи (підвищення фінансування правоохоронних органів, навчання їх співробітників і інформування громадян) застосовуються скоріше як додаткові і супутні. В цілому міжнародний і зарубіжний досвід протидії кіберзлочинності можна охарактеризувати як неузгоджений і тому малоефективний. Різні країни по-різному визначають комп'ютерні злочини, в одних державах діяння криміналізоване вже понад 30 років, в той час як в інших воно залишається законним.

На міжнародному рівні приймаються конвенції, які носять скоріше політичний, ніж правовий характер. У той же час на національних рівнях склалися свої напрямки кримінально-правової політики протидії кіберзлочинності та підходи побудови кримінально-правових норм.

В одних країнах приймаються нові, спеціальні норми про той чи інший традиційний злочин проти власності, який став кіберзлочином (Данія, США, ФРН, Естонія), в той час як в інших розширюється саме поняття злочину шляхом додавання нового способу його вчинення (Республіка Білорусь).

Висновок. Грунтуючись на вищенаведеному, можна зробити наступні висновки: 1. найбільш загальним напрямом державної політики різних країн є захист стратегічних і урядових інформаційних систем, таких як інформаційна система на об'єктах атомної енергетики, об'єктах бюджетної

та фінансової сфери, державних банках, в нафтопромисловому і військово-промисловому комплексі.; 2. Основним заходом протидії в більшості країн є правове регулювання: вдосконалення кримінального, адміністративного та інформаційного законодавства, криміналізація нових діянь, посилення відповідальності за вже існуючі кіберзлочини; 3. найпоширенішими складами кіберзлочинів проти власності в кримінальному законодавстві різних країн є: кібершахрайство та кібервимагання; 4. криміналізація нових складів кіберзлочинів не є оптимальним рішенням для кримінального законодавства України. Більш ефективним рішенням, на наш погляд, було б вдосконалення чинного кримінального законодавства за рахунок розширення поняття «шахрайства», «вимагання» і так далі, а також врахування використання засобів комп'ютерної техніки в якості обставини, що обтяжують покарання.

Література

1. Рекомендація Ради Європи № (89) 9 від 13.09.1989 [Електронний ресурс]. – Режим доступу: https://wcd.coe.int/com.instranet.InstraServlet?command= com.instranet.CmdBlobGet&InstranetImage=610660&SecMode=1&DocId=702280&Usage=2.

2. Сухаренко А.Н. Современные криминальные вызовы и угрозы информационной безопасности [Електронний ресурс]. – Режим доступу: http://sartracc.ru/Press/special/contr_terror_1_12.pdf

3. Інформаційний песурс «Информационная безопасность». [Електронний ресурс]. – Режим доступу: URL:http://www.itsec.ru/newstext.php?news_id=91024

4. Киселёв А.К. Киберпреступность – взгляд из Европы. // Библиотека криминалиста. – 2013. – № 5 (10) – С. 311, 312.

5. Кримінальний кодекс Республіки Білорусь. [Електронний ресурс]. – Режим доступу: URL:http://etalonline.by/?type=text&regnum=hk9900275 #load_text_none_1

6. Кримінальний кодекс Данії. [Електронний ресурс]. – Режим доступу:https://www.retsinformation.dk/Forms/R0710.aspx?id=152827#Kap28

7. Кримінальний кодекс Італії [Електронний ресурс]. – Режим доступу: http://www.altalex.com/?idnot=36653.

8. Кримінальний кодекс Китайскої Народної Республіки [Електронний ресурс]. – Режим доступу: http://constitutions.ru/archives/403.

9. Кримінальний кодекс Нідерландів. [Електронний ресурс]. – Режим доступу:http://wetten.overheid.nl/BWBR0001854/TweedeBoek/TitelV/Artikel138ab/geldigheidsdatum.

10. Свод законодательства США Раздел 18, часть 1, глава 47, §1030 Computer Fraud and Abuse Act (CFAA) [Електронний ресурс]. – Режим доступу: http://www.law.cornell.edu/uscode/text/18/1030.

11. Кримінальний кодекс Німеччини [Електронний ресурс]. – Режим доступу: http://lexetius.com/StGB/263a.

12. Кримінальний кодекс Естонії. [Електронний ресурс]. – Режим доступу: http://www.hot.ee/almanach/kriminaalseadustik.html.

13. Кримінальний кодекс Республіки Корея. [Електронний ресурс]. – Режим доступу:http://www.crime.vl.ru/index.php?p=1324&more=1.

Анотація

Піцик Ю. М. **Міжнародний досвід у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі.** – Стаття.

У статті проведено дослідження міжнародного досвіду у сфері протидії злочинам проти власності, що вчиняються у кіберпросторі. З цією метою проаналізовано нормативно-правові акти зарубіжних країн.

Ключові слова: кіберзлочини, кіберзлочини проти власності, злочини у сфері інформаційних відносин, кіберзлочинність, комп'ютерні злочини.

Аннотация

Пицик Ю. М. **Международный опыт в сфере противодействия преступлениям против собственности, совершаемых в киберпространстве.** – Статья.

В статье проведено исследование международного опыта в сфере противодействия преступлениям против собственности, совершаемых в киберпространстве. С этой целью проанализированы нормативно-правовые акты зарубежных стран.

Ключевые слова: киберпреступления, киберпреступления против собственности, преступления в сфере информационных отношений, киберпреступность, компьютерные преступления.

Summary

Pitsyk Yu. M. **International experience in the field of counteraction to property crimes committed in cyberspace.** – Article.

The article deals with the study of international experience in counteraction to property crimes committed in cyberspace. For this purpose, the normative legal acts of foreign countries are analyzed.

Key words: cybercrime, cybercrime against property, crimes in the field of information relations, cybercrime, computer crimes.