Буяджи С. А.,
Президент благодійного фонду
«Ангели Доброти»
(м. Запоріжжя, Україна)

УДК 340.1:343.97

ОСОБЛИВОСТІ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ ІЗ КІБЕРЗЛОЧИННІСТЮ У США

У статті визначено особливості правового регулювання боротьби із кіберзлочинністю у США. Досліджено акти діючого та проектованого в США законодавства щодо протидії кіберзлочинності. Проаналізовано систему органів державної влади США, що задіяні в механізмі протидії кіберзлочинності. Запропоновано шляхи запозичення позитивного досвіду США у досліджуваній сфері в Україні, зокрема пропонуються зміни до діючого інформаційного законодавства та законодавства у воєнній сфері.

Ключові слова: правове регулювання, боротьба із кіберзлочинністю, кібербезпека, законодавство, авторське право.

Буяджи С.А. Особенности правового регулирования борьбы с киберпреступностью в США. — Статья.

В статье определены особенности правового регулирования борьбы с киберпреступностью в США. Исследованы акты действующего и проектируемого в США законодательства о противодействии киберпреступности. Проанализирована система органов государственной власти США, задействованных в механизме противодействия киберпреступности. Предложены пути заимствования положительного опыта США в исследуемой сфере в Украине, в частности предлагаются изменения в действующее информационное законодательство и законодательство в военной сфере.

Ключевые слова: правовое регулирование, борьба с киберпреступностью, кибербезопасность, законодательство, авторское право.

Buyadji S.A. Peculiarities of Legal Regulation of Cybercrime in the USA. — Article.

The article determines the peculiarities of legal regulation of cybercrime in the USA. The acts of the current and projected legislation in the USA are investigated on combating cybercrime. The system of the USA bodies' state authorities is analyzed, that involved in the mechanism of combating cybercrime. The ways of borrowing positive experience of the United States are suggested in the studied field in Ukraine, in particular, the changes to the current information legislation and legislation in the military sphere are proposed.

Keywords: legal regulation, the fight against cybercrime, cyber security, legislation, copyright.

Процеси глобалізації, у т. ч. глобалізації інформаційних технологій, надають необмежені можливості для здійснення впливу на особистість і суспільство. Одним з негативних наслідків розвитку інформаційних технологій є поява і розвиток нової форми злочинності — злочинності в сфері високих технологій, коли комп'ютери або комп'ютерні мережі виступають в якості об'єкта злочинних посягань, а також як засоби або способи вчинення злочинів. Проблема т. зв. кіберзлочинності актуалізувалася в епоху інформаційного суспільства, коли комп'ютери і телекомунікаційні системи охопили всі сфери життєдіяльності людини і держави, а глобальна мережа Інтернет є однією з найбільш швидких областей розвитку телекомунікаційних технологій [1, с. 45].

Розвиток правового регулювання боротьби із кіберзлочинністю в Україні перебуває на активній стадії протягом останніх двох десятиліть. У США ця система працює вже давно та має позитивні результати, хоча кіберзлочинність на цей момент все ж випереджує за рівнем розвитку інструменти протидії їй. Тому, аналізуючи сучасні вітчизняні реалії, можна відзначити незавершеність даного процесу в Україні та потребу у подальших перетвореннях. За таких умов набуває актуальності вивчення позитивного досвіду США, що є цілком доцільним вектором розвитку досліджуваного інституту.

Проблематика аналізу правового забезпечення боротьби із кіберзлочинністю в зарубіжних країнах часто обговорюється фахівцями на сторінках наукових видань, проте це питання досі не належить до кола достатньо досліджених. Переважно поза увагою залишається

вивчення позитивного досвіду більш прогресивних в цьому відношенні держав та можливості імплементації такого досвіду у вітчизняне законодавство та практику його застосування.

Проблематиці боротьби з кіберзлочинністю присвячено праці М. О. Будакова, В. М. Бутузова, М. Вертузаєвої, М. М. Галамби, Р. А. Калюжного, В. В. Коваленко, Я. Ю. Кондратьєва, Б. А. Кормича, Ю. М. Максименка, В. В. Маркова, А. І. Марущака, Г. В. Новицького, Ю. М. Онищенка, О. В. Орлова, А. Л. Осипенко, Т. Л. Сироїд, В. С. Сідак, Р. Ю. Сень, І. М. Сопілко та інших. Проте питання особливостей правового регулювання боротьби із кіберзлочинністю у США та шляхів запозичення позитивного досвіду в практику України потребує більш комплексного та деталізованого підходу, що і зумовлює актуальність обраної теми дослідження.

Сполучені Штати Америки, як держава, що зазнає значного негативного впливу від кіберзлочинців, та є однією із перших в історії, що зайнялась розробкою відповідних нормативно-правових актів є надзвичайно цікавою та вагомою для дослідження. Як доречно відзначає Н. В. Савчук, американська політика у сфері кіберпростору має значний вплив на країни європейського співтовариства [2, с. 25], а отже дослідження її досвіду є важливим питанням у контексті тематики нашого дослідження. Серед норм Національної стратегії внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес представляє розділ «Кіберзахист», в якому наголошується на необхідності захисту від кібератак у кіберпросторі. США, проголошуючи себе батьківщиною Інтернету, взяли на себе відповідальність перед усім мережевим світом за забезпечення безпеки в кіберпросторі. Окрім того, цією державою проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав та інтересів громадян [3, с. 12]. Тому США є однією із перших держав для дослідження позитивного досвіду протидії кіберзлочинності. Крім того, в США постійно здійснюється активна діяльність з протидії цьому виду злочинності та приділяється значна увага безпеці громадян у цілому. США є однім із головних об'єктів кіберзлочинців з усього світу, тож, як вбачається, їх досвід є корисним для розробки правових інструментів, спрямованих на протистояння цьому негативному явищу. При цьому,

незважаючи на зазначене, в США переважає концепція саморегулювання мережі Інтернет, а отже спеціальне законодавство у цій сфері представлене лише кількома нормативно-правовими актами. Поперед усе, це Закон про електронний підпис, прийнятий у 2000 р. [4, с. 87]. Його мета — забезпечення правового режиму електронного підпису в комерційних відносинах. В США прийнято розглядати цей нормативний акт як символ вступу людства у нову еру — еру електронної комерції. Сам же Закон є доволі стислим і закріплює незначну кількість понять та механізмів, у т. ч. компетенцію державних органів, відповідальних за функціонування усієї інфраструктури у даній сфері, взаємодію її елементів та органів державної влади тощо.

Як відзначає Н. В. Савчук, в країні давно переважає думка, що закон варто приймати лише у тому випадку, якщо усунення проблеми без нього є неможливим. Наприклад, 1 червня 1997 р. президент США Б. Клінтон проголосив доповідь «Політика в галузі глобальної інформаційної комерції», в якій було сформульовано основні принципи політики держави у сфері надання Інтернет-послуг. На наш погляд, на особливу увагу заслуговує один з них: «уряд повинен встановлювати зрозумілі, мінімальні та прості правові норми лише там, де це потрібно» [5, с. 149]. Це означає, що активна боротьба з кіберзлочинністю у вигляді регламентації відповідних відносин здійснюється лише у тих сферах, де існують негативні тенденції до вчинення протиправних діянь, а інші є саморегульованими та привертають увагу законодавця лише за умови виникнення загроз. Такий досвід, на наш погляд, не є позитивним, але, як свідчить практика, США є однією з найзахищеніших країн світу. Тому боротьба із кіберзлочинністю повинна мати комплексний характер, а відповідне галузеве законодавство є лише одним із її елементів.

Найбільшу кількість нормативно-правових актів США у досліджуваній сфері прийнято щодо емісії цінних паперів, охорони інтелектуальної власності, захисту від несанкціонованого доступу до інформації, авторського права тощо [6, с. 25]. Загалом, до недавнього часу американські юристи дотримувалися точки зору про те, що для регулювання боротьби із кіберзлочинністю важливішими є міждержавні, а не національні нормативно-правові акти, оскільки запровадження

певних обмежень одним суб'єктом може негативно вплинути на інтереси інших сторін [4, с. 87]. Проте, внаслідок терористичних актів 11 вересня 2001 р. було значно посилено боротьбу із тероризмом, одним із різновидів якого є кібертероризм. В тому ж році урядом США було прийнято Закон «Про об'єднання та зміцнення США», згідно з нормами якого будь-яка дія, яка спричиняє порушення в роботі чи призводить до незаконного проникнення в комп'ютер, класифікується як тероризм. В свою чергу, провайдер зобов'язаний надати всю відому йому інформацію про користувача на першу вимогу Федерального бюро розслідувань [7]. Таким чином, на сьогодні вектор правового регулювання боротьби із кіберзлочинністю в США пов'язується із протидією кібертероризму як найнебезпечнішому прояву кіберзлочинності. Так, 17 листопада 2014 р. було заявлено про ремонт системи електронної пошти Держдепартаменту США після можливої шкоди, завданої ймовірною хакерською атакою [8, с. 71]. Сьогодні США перебувають у стані постійної готовності до захисту своїх громадян від негативного впливу кіберзлочинців. Зважаючи на загальну кількість кібератак, важливими проблемами, які постають перед США сьогодні, є проведення оперативно-розшукових заходів та покарання порушників закону. Елементами таких процесів є збільшення міри відповідальності за вчинення комп'ютерних злочинів та захист прав та інтересів громадян у разі завдання шкоди.

Деструктивна діяльність в кіберпросторі США карається значно жорсткіше, ніж у Європі. Так, у США визначено кримінальну відповідальність за неналежне зберігання та обробку персональної інформації чи її знищення у відмінному від встановленого законом способу. Для порівняння, у країнах ЄС кримінальні справи можуть порушуватися лише у випадку завдання шкоди державній безпеці та основним правам громадян [9, с. 126]. Це свідчить про те, що соціальним аспектом правового регулювання боротьби із кіберзлочинністю в США не знехтувано, оскільки величезне значення все ще має не лише захист державних інтересів, а й кожного окремого громадянина.

Тож, дослідження сучасного стану боротьби із кіберзлочинністю засвідчило, що даний напрям є одним із пріоритетних у державній

політиці США. Позитивними тенденціями є активна боротьба із кібертероризмом та оперативність заходів з вирішення існуючих проблем. До негативних необхідно віднести, передусім, реагування на загрози лише по мірі їх настання, проте в той же час США залишаються однією із найзахищеніших держав світу.

У контексті боротьби з кіберзлочинністю, важливим є аналіз діючих та проектованих нормативно-правових актів, у яких закріплено повноваження органів державної влади та правоохоронних органів США щодо протистояння кіберзлочинам. У 2009 році в Сенаті США зареєстровано законопроект «Акт про кібербезпеку 2009» (*Cybersecurity Act of 2009*) [10], розроблений Національною розвідкою США, яким було запропоновано значно розширити повноваження федеральної влади у сфері забезпечення кібербезпеки та передбачити обов'язкову ідентифікацію користувачів кіберпростору в інтересах національної безпеки. Даний законопроект, у разі прийняття, міг би значно вплинути на суть сучасного Інтернету, адже за його допомогою планувалось встановити нові стандарти комп'ютерної безпеки, зокрема шляхом встановлення вимог, які б зобов'язали користувачів здійснювати обов'язкову ідентифікацію та дати згоду уряду на законних підставах перевіряти вміст електронних листів, переданих файлів, пошукових запитів користувачів кіберпростору тощо [10]. Проте, даний закон ще не прийнято і це, як вбачається, є позитивним у контексті захисту прав людини і громадянина. Адже прийняття такого акту державою, яка сьогодні має вагомий вплив на усі глобальні процеси, безсумнівно, надало б значного ефекту (негативного для звичайних користувачів і позитивного для підсилення механізму втручання держави в особисте життям громадян) та змінило усю світову систему кібербезпеки. Крім того, цей досвід поступово почав би перейматися іншими країнами.

Сьогодні і в Україні спостерігаються спроби державної влади до встановлення контролю за користувачами Всесвітньої мережі та спрямування діяльності громадян у кіберпросторі у вигідному для держави напрямку, але масштаби наслідків теперішньої ситуації в Україні та перспектив для громадян США, за умови прийняття Акту, все ж значно відрізняються.

Продовжуючи аналіз нормативно-правової бази США, присвяченої боротьбі з кіберзлочинністю, відзначимо вагому роль законодавства у сфері захисту інформації. Як відзначає І. М. Сопілко, щодо захисту інформації уряд США керується принципом недопущення перехоплення іноземними державами конфіденційної державної та приватної інформації, а також відкритої інформації, що передається урядовими і комерційними телекомунікаціями, що може завдати шкоди державі або ж її громадянам [8, с. 73]. Для забезпечення такого рівня захисту були здійснені значні організаційні та технічні кроки з метою убезпечення ліній зв'язку та автоматизованих систем, а у нормативній сфері — прийнято Закон «Про забезпечення безпеки ЕОМ» №HR — 145 [11]. Його норми, зокрема, встановили вимоги для державних організацій щодо забезпечення необхідного рівня захисту інформації. Наприклад, у ч. 3 Закону зазначено, що «важливою є інформація, втрата, зміна або доступ до якої може призвести до небажаних наслідків для національних інтересів» [11]. Це свідчить про те, що на початкових етапах основна увага у правовому регулюванні боротьби з кіберзлочинністю все ж приділялася державним інтересам, а приватні були захищені меншою мірою. Проте, останніми роками спостерігаються спроби посилити захист індивідуальних суб'єктів. США, як високотехнологічна держава, забезпечила захист стратегічних об'єктів на високому рівні, тому кіберзлочини, спрямовані проти держави у цілому, відбуваються набагато рідше і потребують серйозної підготовки і умінь кіберзлочинців. Прості громадяни сьогодні частіше постають об'єктами кібератак, тому сучасна нормотворча діяльність у США здебільшого пов'язується саме із захистом прав та інтересів громадян. І. М. Сопілко відзначає внесення спеціальних законопроектів, які передбачають посилення відповідальності за порушення у сфері захисту індивідуальної інформації, у т. ч. шляхом інсталяції програмного забезпечення для збору індивідуальної інформації, ідентифікації користувача, без його відома та згоди [8, с. 73].

Таким чином, правове регулювання боротьби із кіберзлочинністю у США регламентується жорсткіше, ніж у Європі. Якщо у європейських державах основна увага приділяється завданню шкоди

державним інтересам та основним правам громадян, то у США до кримінальних проступків високого рівня небезпечності належить і неналежне зберігання, і обробка персональної інформації та її знищення не за законом.

Окрім того, привертає увагу і система органів, що здійснюють боротьбу із кіберзлочинністю в США:

1) Кібернетичне командування США (*United States Cyber Command, USCYBERCOM*) — підрозділ збройних сил США, основними завданнями якого є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж США;

2) Комп'ютерна команда екстреної готовності США (*United States Computer Emergency Readiness Team, US — CERT*) — частина Національного відділу кіберзахисту Міністерства внутрішньої безпеки США, яка видає інформацію про поточні питання безпеки, вразливі до кібервпливу об'єкти і працює з постачальниками програмного забезпечення для створення спеціальних програмних пристосувань, які усувають прогалини в системах безпеки;

3) відділ комп'ютерної злочинності та інтелектуальної власності (*Computer Crime and Intellectual Property Section, CCIPS*) — відділ у кримінальних справах Міністерства юстиції США з розслідування комп'ютерних злочинів і порушення прав інтелектуальної власності, який спеціалізується у сфері пошуку і захоплення цифрових доказів у комп'ютерах і мережах [12, с. 213—214].

Для порівняння, в Україні на сьогодні діє лише один такий орган — Департамент кіберполіції Національної поліції України, тобто боротьба із кіберзлочинністю здійснюється лише на правоохоронному рівні, що сьогодні є недостатнім. В США таких рівнів три: військовий, правоохоронний та юстиційний, причому кожен з них має особливі повноваження. Тому, відповідно, і боротьба із кіберзлочинністю здійснюється значно ефективніше.

Звернемо увагу на військовий напрям, який є актуальним для держави, що веде неоголошену війну. О. В. Орлов та Ю. М. Онищенко в даному контексті використовують термін «операції кібервійни» [12, с. 214]. Пристосовуючи це визначення до сучасних українських реалій, необхідно відзначити, що сьогодні відбувається значний та

деструктивний вплив на кібермережі вітчизняних органів державної влади та інших стратегічних для країни об'єктів. Більше того, значних масштабів набули інформаційні атаки у Інтернеті, передусім, у соціальних мережах. Тому такий досвід США є корисним у сучасних умовах.

Таким чином, слід виокремити основні характеристики правового регулювання боротьби із кіберзлочинністю у США: 1) США вважають себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) ця держава має значний вплив на прийняття відповідного законодавства у країнах ЄС; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам.

Окремі із проаналізованих напрямів є безперечно позитивними та доцільними для запозичення нашою державою і, зважаючи на це, можна виокремити наступні шляхи такого запозичення:

1) посилення відповідальності за злочини у сфері захисту індивідуальної інформації. Незважаючи на те, що у цілому в США відповідальність за кіберзлочини є суворішою, ніж у європейських державах, сьогодні в США існує можливість встановлення санкцій за порушення у сфері захисту індивідуальної інформації у розмірі штрафу до 1 млн дол. або ув'язнення до 5 років [8, с. 73]. Вважаємо, що такий досвід варто перейняти Україні і доповнити Розділ XVI Кримінального кодексу України [13] статтею наступного змісту:

«Порушення у сфері захисту індивідуальної інформації

1. Порушення у сфері захисту індивідуальної інформації суб'єктів, персональні дані яких обробляються у вигляді незаконних втручань та втрати даних у мережі Інтернет, — карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до п'яти років.

2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, — караються позбавленням волі на строк до шести років».

2) Посилення захисту від перехоплення іноземними державами конфіденційної державної і приватної інформації, а також відкритої

інформації, яка передається урядовими і комерційними телекомунікаціями, що може завдати шкоди державі або ж її громадянам.

Пропонується прийняти Закон «Про основні засади забезпечення кібербезпеки України», а його цілями визначити: 1) зобов'язання державних організацій забезпечити необхідний рівень захисту інформації від кібервпливу; 2) формування у суспільстві розуміння необхідності захисту інформації; 3) заповнення прогалин вітчизняного законодавства про інформацію. Також у нормах цього Закону пропонуємо встановити норму про те, що захист ліній зв'язку і автоматизованих систем є пріоритетним завданням компетентних державних органів. Крім того, необхідно вирішити питання безпеки приватної та іншої інформації шляхом визначення вимог для державних організацій щодо забезпечення необхідного рівня захисту інформації.

3) Розширити мережу органів, що здійснюють боротьбу із кіберзлочинністю. Для виконання такого завдання необхідно: визначитись, які саме органи є необхідними для забезпечення кібербезпеки в Україні; прийняти нормативно-правову основу їх діяльності.

Зважаючи на досвід США, найбільш доцільним напрямом буде створення підрозділу у рамках Збройних Сил України з назвою «Кібернетичне командування України», а для регламентації його діяльності потрібно: по-перше, внести зміни до ст. 3 Закону України від 06.12.1991 р. «Про Збройні Сили України» [14] та доповнити її наступним чином: «Збройні Сили України мають таку загальну структуру:… Кібернетичне командування України — підрозділ Збройних Сил України, основними завданнями якого є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж України»; по-друге, прийняти Положення про Кібернетичне командування України, яким буде визначено завдання та механізми їх реалізації.

До пріоритетних напрямків діяльності такого органу слід віднести протидію кібертероризму в умовах ведення військових дій, а також кіберзахист воєнних та інших стратегічних об'єктів. Тому в запропонованому Положенні необхідно визначити завдання такого органу, його структуру та повноваження, а також механізми їх реалізації. Його додаткові функції можуть полягати у здійсненні впливу

на кібермережі супротивників в умовах ведення війни. Тобто цей орган буде покликаний, в першу чергу, стримувати і попереджувати агресію супротивника та брати участь у заходах, пов'язаних із боротьбою з кібертероризмом.

Таким чином, США, як стратегічний партнер України та одна із найвпливовіших держав світу, постійно привертають увагу вітчизняних вчених-правознавців. Незважаючи на те, що масив національного американського законодавства у даній сфері є незначним, усі правовідносини у сфері використання кібермереж є регламентованими належним чином. Тому США є гарним прикладом для запозичення досвіду правового регулювання боротьби із кіберзлочинністю та організації її здійснення.

ЛІТЕРАТУРА

1. *Номоконов В. А., Тропина Т. Л.* Киберпреступность как новая криминальная угроза // Криминология: вчера, сегодня, завтра. 2012. № 1(24). С. 45—55.
2. *Савчук Н. В.* Світовий досвід державного регулювання ринку інтернет-послуг // Формування ринкових відносин в Україні. 2012. № 4. С. 24—28.
3. *National Security* Strategy. The White House, February 2015. — Washington D.C., 2015. 29 p. URL: http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf
4. *Курицкий А. Ю.* Интернет-экономика: закономерности формирования и функционирования. — СПб.: Издательство С.-Петербургского университета, 2000. 232 с.
5. *Винарик Л. С., Щедрин А. Н., Васильєва Н. Ф.* Информационная экономика: становление, развитие, проблемы / НАН Украины; Институт экономики промышленности. — Донецк, 2002. 312 с.
6. *Савчук Н. В.* Світовий досвід державного регулювання ринку інтернет-послуг // Формування ринкових відносин в Україні. 2012. № 4. С. 24—28.
7. *Uniting* and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism: USA PATRIOT ACT (Act of 2001). Public Law 107-56-OCT. 26, 2001. URL: https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf
8. *Сопілко І. М.* Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України // Юридичний вісник. Повітряне і космічне право. 2014. № 4. С. 70—75.

9. *Кравчук М. М.* Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет // Наукові записки Інституту законодавства Верховної Ради України. 2013. № 3. С. 123—126.
10. *Cybersecurity* Act of 2010. S. 773 (111th). April 1, 2009. URL: https://www.govtrack.us/congress/bills/111/s773/text/is
11. *Computer Security* Act Of 1987. June 11, 1987 №HR — 145. URL: http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt
12. *Орлов О. В.*, Онищенко Ю.М. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам у мережі інтернет // Теорія та практика державного управління. 2014. Вип. 2. С. 212—219.
13. *Кримінальний кодекс* України, 2001 // Відомості Верховної Ради України. 2001. № 25—26. Ст. 131.
14. *Про Збройні Сили* України: Закон України від 06.12.1991 р. // Відомості Верховної Ради України. 1992. № 9. Ст. 108.