

УДК 341.018

Турченко Ольга Григорівна –

к.ю.н., доцент, доцент кафедри конституційного і міжнародного права
Донецького національного університету

Olha H. Turchenko –

candidate of juridical sciences,
assistant professor of the department of constitutional and
international law of
Donetsk National University
(21, 600-richchia Street, Vinnytsia, 21021, Ukraine)

Проценко Анастасія Сергіївна –

студентка 4 курсу юридичного факультету
Донецького національного університету

Anastasia S. Protsenko –

4th year student of Faculty of Law
of Donetsk National University
(21, 600-richchia Street, Vinnytsia, 21021, Ukraine)

Україна та Конвенція Ради Європи про кіберзлочинність: проблеми виконання і шляхи їх вирішення

У статті досліджуються законодавчі проблеми боротьби із кіберзлочинністю в контексті міжнародного співробітництва. Проводиться аналіз міжнародних угод в зазначеній сфері, стороною яких є Україна. Висвітлено проблеми виконання міжнародних зобов'язань Україною у сфері боротьби з кіберзлочинністю. Запропоновано шляхи реформування чинного законодавства для забезпечення інформаційної безпеки і боротьби із кіберзлочинністю.

Ключові слова: кіберзлочинність, інформаційна безпека, законодавче врегулювання, міжнародні зобов'язання, міжнародні угоди.

В статье исследуются законодательные проблемы борьбы с киберпреступностью в контексте международного сотрудничества. Проводится анализ международных соглашений в данной сфере, стороной которых является Украина. Освещены проблемы выполнения международных обязательств Украины в сфере борьбы с киберпреступностью. Предложены пути реформирования действующего законодательства для обеспечения информационной безопасности и борьбы с киберпреступностью.

Ключевые слова: киберпреступность, информационная безопасность, законодательное урегулирование, международные обязательства, международные соглашения.

O.H. Turchenko, A.S. Protsenko Ukraine and Convention on Cybercrime Adopted by the Council of Europe: Problems of Following and Ways of their Solving

Nowadays cybercrimes are not only a certain group of crimes. Computer systems make it possible to commit almost any crime provided by criminal law. International agreements on fighting against cybercrimes are not enough to ensure informational security in the society. It is necessary to amend significantly Ukrainian legislation to perform international obligations in this sphere. These amendments will contribute that Ukrainian legislation complies with the European one which will accelerate European integration.

Analysis of Ukrainian legislation proves that there are significant problems in legal ensuring within the system of cyber safety in Ukraine. They are the following: the absence of definitions in this sphere which should be developed and provided by legislation; the absence of certain features which threaten to the national cyber space; the absence of the unified elements of cybercrimes, etc.

After acceding to the Convention on Cybercrime, Ukraine acquired a number of obligations in this sphere. New types of illegal actions had to be criminalized in our country. New needs to ensure the access to computer systems within international cooperation have appeared. It has been necessary to provide legislative regulation of computer data recorded by business entities within their activities. Such obligations have not been enshrined in Ukrainian legislation yet.

The authors have proposed a new version of some provisions of the Criminal Code of Ukraine related to the gravest crimes involving computer systems, which are provided by international agreements. Necessity to provide application of criminal means to legal entities in the Criminal law according to the Convention on Cybercrime has been proved. It has been proposed to develop and implement the Procedure for recording and keeping computer data and data of telecommunication network by business entities which provide telecommunication services or use computers, computer systems, telecommunication systems in their activities.

Keywords: *cybercrime, informational security, legislative regulation, international obligations, international agreements.*

Постановка проблеми. Взятий Україною курс на європейську інтеграцію потребує докорінних змін в багатьох сферах життєдіяльності держави. Такі зміни перш за все стосуються юридичної сфери, в якій мають бути досконало налагоджені механізми взаємодії права, держави, суспільства. Відповідні механізми перш за все пов'язані із реалізацією права. Однією з форм реалізації права виступає його виконання - форма реалізації зобов'язуючих норм, змістом якої є вчинення дій, що вимагаються юридичними приписами, тобто виконання покладених обов'язків, у тому числі – договірних. [1, с. 222-223].

Сьогодні Україна є стороною багатьох міжнародних угод. Із початком наближення нашої держави до Європейського Союзу (ЄС), таких угод укладається дедалі більше. Наразі увага дослідників більш за все приділяється безсумнівно актуальним угодам, що стосуються безпосередньо процесу євроінтеграції. Проте дані угоди розраховані на вже адаптоване до європейських змін законодавство. Міжнародні угоди Україні, укладені до початку вказаного процесу, не завжди мали своїм наслідком внесення змін до діючого законодавства України із метою приведення його у відповідність таким угодам. Тому аналіз виконання таких угод та пропозиції щодо приведення законодавства у відповідний таким угодам стан є досить актуальними.

Головною ознакою суб'єкта міжнародного права як надійного партнера є гарантія виконання угод, що укладаються таким суб'єктом, або до яких він приєднується. Таким чином, виконання договірних обов'язків, покладених на Україну міжнародними угодами,

характеризує стан правової сфери нашої держави як такий, що готовий або не готовий до вступу у Європейське співтовариство. Відтак, аналіз виконання Україною міжнародних угод має важливе практичне і наукове значення.

Зростаючий інтерес до інформаційної безпеки на сьогоднішній день підтверджується, наприклад, і прийнятим на вищому рівні керівництва НАТО рішенням про посилення уваги до проблеми забезпечення інформаційної безпеки і здатності вести інформаційні війни, обумовленим збільшенням активності потенційних супротивників блоку і прагненням організації відповідати рівню зростаючих загроз кібербезпеки; акцентуванні НАТО на транскордонній природі загроз інформаційній безпеці і проблемах координації дій на наднаціональному рівні; наявністю служб інформації в практично у всіх міжнародних організаціях, в тому числі і військових.

При цьому, аналіз чинного законодавства України свідчить про значні проблеми в правовому забезпеченні системи кібернетичної безпеки України: відсутність розробленого і нормативно-закріпленого понятійного апарату в цій сфері, відсутність чітко визначених ознак основних загроз в національному сегменті кіберпростору, відсутність уніфікованого складу кіберзлочинності і т.д.

Крім того, актуальність може підтверджуватися і загостренням проблеми Інтернет-злочинності, насамперед, організований кіберзлочинності, яка придбала чітко визначений як національний, так і міжнародний, транснаціональний характер [2, с.295].

Аналіз останніх досліджень і публікацій. Дослідженням проблематики реалізації норм права ЄС, міжнародного права та внутрішньодержавного права займалися такі вчені, як В. А. Василенко, В. Г. Буткевич, В. І. Євінтов, К. В. Смирнова, В. Т. Пятницький, О. М. Шпакович. Аналіз стану виконання окремих міжнародних угод останніми роками проводився такими дослідниками, як О. А. Дячуком, І. М. Чуприним та ін. Крім того, неодноразово у зв'язку із процесом Євроінтеграції, аналіз стану перспектив виконання міжнародних угод проводився органами державної влади та окремими посадовими особами таких органів [3, с. 184-193].

Що стосується рівня дослідження проблеми кібербезпеки, то на сьогоднішній день чимало дослідників описують позитивні моменти як формування інформаційного суспільства, так і необхідності розробки інформаційного права як загального регулятора інформаційних правовідносин (наприклад, Гурковський В.І.). Інша група дослідників зосереджує свою увагу на власних пошуках забезпечення інформаційної безпеки, реалізацію окремих положень державної інформаційної політики, але без урахування сучасних тенденцій в кіберпросторі, концентруючись в більшості випадків на питаннях систематизації інформаційного законодавства та розвитку різноманітних інститутів інформаційного права (наприклад, Баскаков В.Ю., Ліпкан В.А., Максименко Ю.Є., Залізник В.А.).

Невирішені раніше проблеми: Основна частина проведених досліджень стосувалась проблем виконання конкретних міжнародних угод. Також досить щільно розроблено теорії взаємодії або колізії внутрішньодержавного та міжнародного права. Більшість сучасних досліджень спрямовано на криміналізацію окремих діянь, і вони не торкаються питань суб'єктів відповідальності та проблем взаємодопомоги у сфері протидії кібернетичній злочинності.

Мета. Метою даного дослідження є аналіз діючих міжнародних угод, стороною яких є Україна, у сфері протидії кібернетичній злочинності, виявлення нагальних проблем невиконання таких угод і розробка пропозицій щодо приведення українського законодавства у відповідність до них.

Виклад основного матеріалу. Україна є стороною багатьох міждержавних багатосторонніх угод у сфері взаємної допомоги у кримінальних справах. Щодо угод у сфері протидії кіберзлочинності, то вони представлені Конвенцією Ради Європи про кіберзлочинність [4] і Протоколом до цієї Конвенції. Конвенцію ратифіковано із застереженнями і заявами Законом № 2824-IV від 07 вересня 2005 року.

По-перше, слід зауважити, що чинним Кримінальним Кодексом України передбачені не всі злочинні діяння, що містить вказана Конвенція. Так, КК України не передбачає кримінальної відповідальності за: придбання шкідливих комп'ютерних програм і пристроїв, створених чи адаптованих для вчинення комп'ютерних злочинів; виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів; володіння зазначеними вище шкідливими комп'ютерними програмами, пристроями, комп'ютерними паролями, кодами доступу чи іншими аналогічними даними; придбання дитячої порнографії через комп'ютерну систему; володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних [5].

На думку Орлова Ю.Ю., питання щодо криміналізації діянь, передбачених п. "а II" ч. 1 ст. 6 Конвенції, необхідно вирішувати з урахуванням змісту ч. 3 ст. 6 цього міжнародного документа, що контекстуально зобов'язує всіх держав-учасників передбачити кримінальну відповідальність за продаж, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути вчинено комп'ютерний злочин. Відповідальність за ці діяння в Україні не встановлено [6, с.8-9].

Щодо Протоколу до Конвенції, то діяння, передбачені цим протоколом як злочинні, в Україні до сьогодні також не криміналізовані. Мова йде про такі злочинні дії, як поширення расистського та ксенофобного матеріалу через комп'ютерні системи, погроза з расистських та

ксерофобних мотивів, образа з расистських та ксерофобних мотивів, заперечення, значна мінімізація, схвалення або виправдання геноциду чи злочинів проти людства [7].

По-друге, у Конвенції та чинному законодавстві України є розбіжності щодо суб'єктів, що можуть бути притягнені до відповідальності за злочини у сфері кіберзлочинності. На відміну від наслідків приєднання до Кримінальної конвенції Ради Європи про боротьбу з корупцією, Європейської конвенції про боротьбу з тероризмом, наслідком приєднання до досліджуваної Конвенції не стало запровадження кримінальної відповідальності, або, принаймні, заходів кримінального характеру, для юридичних осіб. Так, стаття 12 Конвенції передбачає корпоративну відповідальність за кібернетичні злочини, а саме наступне: Кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для забезпечення того, щоб юридична особа могла нести відповідальність за кримінальне правопорушення, встановлене відповідно до цієї Конвенції, яке було вчинене на її користь будь-якою фізичною особою, як індивідуально, так і в якості частини органу такої юридичної особи. Така фізична особа має займати керівну посаду в рамках юридичної особи, в силу:

- a. повноважень представляти цю юридичну особу;
- b. повноважень приймати рішення від імені цієї юридичної особи;
- c. повноважень здійснювати контроль в рамках цієї юридичної особи.

Кожна Сторона вживає заходів для забезпечення того, щоб юридична особа могла понести відповідальність у разі, коли недостатній нагляд чи контроль, який мав здійснюватися вказаною фізичною особою, створив можливість вчинення кримінального правопорушення, встановленого відповідно до цієї Конвенції, на користь такої юридичної особи фізичною особою, яка діяла під її контролем.

Звісно, Конвенцією передбачено, що відповідно до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною. Проте, український законодавець вже пішов шляхом застосування заходів кримінального характеру до юридичних осіб, що передбачено

главою XIV-1 КК України. Включення таких заходів до кримінального законодавства також було спричинено наявністю зобов'язань міжнародного характеру щодо корпоративної відповідальності. Проте корпоративна відповідальність за кібернетичні злочини у кримінальному законодавстві України досі не передбачено, хоча масштаби здійснення таких злочинів саме юридичними особами набагато більше тих, що здійснюються фізичними особами.

По-третє, існують певні законодавчі перепони для виконання вимог Конвенції щодо співробітництва. Йдеться про такі положення, як, наприклад, положення статті 16 про термінове збереження комп'ютерних даних, які зберігаються: кожна Сторона вживає такі законодавчі та інші заходи, які можуть бути необхідними для надання можливості своїм компетентним органам видавати ордери або іншим подібним шляхом спричиняти термінове збереження визначених комп'ютерних даних, включаючи дані про рух інформації, які зберігалися за допомогою комп'ютерної системи, зокрема у випадку, коли існують підстави вважати, що такі комп'ютерні дані особливо вразливі до втрати чи модифікації. Також відповідно до ст. 17 Конвенції, кожна Сторона вживає по відношенню до даних про рух інформації, які мають зберігатися відповідно до статті 16, такі законодавчі та інші заходи, які можуть бути необхідними для:

- a. забезпечення того, щоб таке термінове збереження даних про рух інформації могло проводитися, незважаючи на те, один чи більше постачальників послуг було залучено до передачі такої інформації; та

- b. забезпечити термінове розкриття компетентному органу Сторони або особі, призначеній таким органом, обсягу даних про рух інформації, достатнього для ідентифікації постачальників послуг і маршруту, яким була передана інформація.

Із законодавчої точки зору, зреагувати на такий запит швидко не виявляється можливим. Відповідно до ст. 263 Кримінального процесуального кодексу України, зняття інформації з транспортних телекомунікаційних мереж (мереж, що забезпечують передавання знаків, сигналів, письмового тексту, зображень та звуків або повідомлень будь-якого виду між

підключеними до неї телекомунікаційними мережами доступу) є різновидом втручання у приватне спілкування, яке проводиться без відома осіб, які використовують засоби телекомунікацій для передавання інформації, на підставі ухвали слідчого судді, якщо під час його проведення можна встановити обставини, які мають значення для кримінального провадження. Також відповідно до ст. 264 КПК України, пошук, виявлення і фіксація відомостей, що містяться в електронній інформаційній системі або їх частин, доступ до електронної інформаційної системи або її частини, а також отримання таких відомостей без відома її власника, володільця або утримувача може здійснюватися на підставі ухвали слідчого судді, якщо є відомості про наявність інформації в електронній інформаційній системі або її частині, що має значення для певного досудового розслідування. Таким чином, будь-які дії із збереження комп'ютерних даних апіорі не можуть бути терміновими, адже для їх вчинення потрібна ухвала слідчого судді. Крім того, виходячи з положень КПК України, такі заходи застосовуються у вже відкритому кримінальному провадженні. Таким чином, вимоги ст. 16, 17 Конвенції про кіберзлочинність законодавчо в Україні не забезпечені [8].

Крім того, в зарубіжних країнах існує досвід законодавчого закріплення за суб'єктами господарювання, що здійснюють надання телекомунікаційних послуг, обов'язку протягом певного періоду (або постійно) зберігати певні комп'ютерні дані. В Україні таких законодавчих вимог не передбачено; більш того, не завжди вказані суб'єкти господарювання в змозі забезпечити організаційно та технічно збереження таких даних. Ці обставини також вказують на не забезпечення Україною вимог Конвенції про кіберзлочинність, а саме статті 20 вказаної Конвенції.

Таким чином, вважаємо доцільним:

1. Закріпити у Кримінальному кодексі України положення щодо кримінальної відповідальності за діяння, передбачені у Конвенції Ради Європи про кіберзлочинність, що досі не передбачені КК України.

2. Частину 1 статті 300, ст. 442 КК України викласти у наступній редакції:

Частину 1 статті 300: «Ввезення, виготовлення або розповсюдження творів, що

пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію

1. Ввезення в Україну творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, з метою збуту чи розповсюдження або їх виготовлення, зберігання, перевезення чи інше переміщення з тією самою метою або їх збут чи розповсюдження, а також примушування до участі в їх створенні, у тому числі з використанням комп'ютерних систем –

караються штрафом до ста п'ятдесяти неоподатковуваних мінімумів доходів громадян або арештом на строк до шести місяців, або обмеженням волі на строк до трьох років, з конфіскацією творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, засобів їх виготовлення та розповсюдження».

Стаття 442. Геноцид

«1. Геноцид, тобто діяння, умисно вчинене з метою повного або часткового знищення будь-якої національної, етнічної, расової чи релігійної групи шляхом позбавлення життя членів такої групи чи заподіяння їм тяжких тілесних ушкоджень, створення для групи життєвих умов, розрахованих на повне чи часткове її фізичне знищення, скорочення дітонародження чи запобігання йому в такій групі або шляхом насильницької передачі дітей з однієї групи в іншу, у тому числі з використанням комп'ютерних систем - карається позбавленням волі на строк від десяти до п'ятнадцяти років або довічним позбавленням волі.

2. Публічні заклики до геноциду, а також виготовлення матеріалів із закликами до геноциду з метою їх розповсюдження або розповсюдження таких матеріалів, у тому числі з використанням комп'ютерних систем - караються арештом на строк до шести місяців або позбавленням волі на строк до п'яти років».

3. Закріпити у Главі XIV-1 КК України положення щодо застосування заходів кримінального характеру до юридичних осіб, що вчинили злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку.

4. Розробити і запровадити Порядок фіксації та зберігання суб'єктами господарювання, що надають телекомунікаційні послуги або застосовують у своїй діяльності комп'ютери, комп'ютерні мережі і мережі

електрозв'язку комп'ютерних даних і даних мереж електрозв'язку.

Список використаних джерел:

1. Теорія держави і права. Академічний курс : підручник / О. В. Зайчук [та ін.] ; ред. О. В. Зайчук, Н. М. Оніщенко. – К. : Юрінком Інтер, 2008. – 688 с.
2. Жаров А. І. Формування кібербезпеки органами ДПС України в умовах глобалізації інформаційного суспільства / А. І. Жаров // Проблеми впровадження інформаційних технологій в економіці : матеріали VIII Міжнародної науково-практичної конференції (23 січня – 30 березня 2012 р., м. Ірпінь). – Ірпінь, 2012. – С. 292-297.
3. Трюхан В. В. Інституційне забезпечення виконання угоди Україна – ЄС [Електронний ресурс] / В. В. Трюхан // Вісник Національної академії державного управління. – 2011. – № 3. – С. 184-193. – Режим доступу : <http://visnyk.academy.gov.ua/wp-content/uploads/2013/11/2011-3-27.pdf>.
4. Конвенція Ради Європи про кіберзлочинність : міжнародний документ від 23.11.2001 // Офіційний вісник України. – 2007. – № 65. – Ст. 107.
5. Кримінальний кодекс України : закон від 05.04.2001 № 2341-III // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.
6. Орлов Ю. Ю. Реалізація вимог міжнародної конвенції про кіберзлочинність у законодавстві України / Ю. Ю. Орлов // Науковий вісник академії внутрішніх справ. – 2011. – № 6. – С. 3-9.
7. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : міжнародний документ від 28.01.2003 // Офіційний вісник України. – 2010. – № 56. – Ст. 73.
8. Кримінальний процесуальний кодекс України : закон від 13.04.2012 № 4651-VI // Відомості Верховної Ради України. – 2013. – № 9-10. – Ст. 474.

References

1. The Theory of State and Law. Academic Course : textbook / O. V. Zaichuk [and others] ; under the editorship of O. V. Zaichuk, N. M. Onishchenko. – K. : Yurinkom Inter, 2008. – 688 p.
2. A. I. Zharov, Establishing Cybersecurity by the Bodies of the State Tax Service of Ukraine within Globalization of the Informational Society / A. I. Zharov // Issues Related to Implementation of Informational Technologies in Economy : materials of VIII International Scientific Conference (January 23 – March 30, 2012, Irpin). – Irpin, 2012. – P. 292-297.
3. V. V. Triukhan, Institutional Ensuring of Performance of Ukraine – European Union Agreement [Online resource] / V. V. Triukhan // Visnyk Natsionalnoi akademii derzhanoho upravlinnia (the Bulletin of the National Academy for Public Administration). – 2011. – No. 3. – P. 184-193.
4. Convention on Cybercrime adopted by the Council of Europe : international document dated 23.11.2001 // Ofitsiinyi Visnyk Ukrainy (the Official Bulletin of Ukraine). – 2007. – No. 65. – Art. 107.
5. The Criminal Code of Ukraine : the Law of Ukraine dated 05.04.2001 No. 2341-III // Vidomosti Verkhovnoi Rady Ukrainy (the Official Bulletin of the Verkhovna Rada of Ukraine). – 2001. – No. 25-26. – Art. 131.
6. Yu. Yu. Orlov, Fulfillment of Requirements Provided by the Convention on Cybercrime in the Legislation of Ukraine / Yu. Yu. Orlov // Naukovyi visnyk akademii vnutrishnikh sprav (Scientific Bulletin of the Academy of Internal Affairs). – 2011. – No. 6. – P. 3-9.
7. Additional Protocol to the Convention on Cybercrime concerning the Criminalization of Acts of a Racist and Xenophobic Nature Committed through Computer Systems : international document dated 28.01.2003 // Ofitsiinyi Visnyk Ukrainy (the Official Bulletin of Ukraine). – 2010. – No. 56. – Art. 73.

8. The Code of Criminal Procedure of Ukraine : the Law dated 13.04.2012 No. 4651-VI // Vidomosti Verkhovnoi Rady Ukrainy (the Official Bulletin of the Verkhovna Rada of Ukraine). – 2013. – No. 9-10. – Art. 474.