УДК 342.1-044.332(477):343.3/.7:061.1ЄС

М. В. Маркарян[*],
старший викладач кафедри теорії та історії права
ДВНЗ «Київський національний економічний
університет імені Вадима Гетьмана»

СТАН І ПЕРСПЕКТИВИ АДАПТАЦІЇ ЗАКОНОДАВСТВА УКРАЇНИ ДО ВИМОГ ЄС У СФЕРІ КІБЕРЗЛОЧИННОСТІ

У статті досліджено процес адаптації законодавства України відповідно до поставлених вимог ЄС у сфері кіберзлочинності, що є одним із етапів на шляху до майбутнього потенційного членства України в Європейському Союзі. Також проаналізовано науковий доробок окремих науковців щодо зазначеної проблематики.

Ключові слова: адаптація законодавства, кіберзлочинність, кібератака, кібербезпека, Конвенція про кіберзлочинність, кримінальна відповідальність, національна безпека.

В статье исследуется состояние процесса адаптации законодательства Украины в соответствии с поставленными требованиями в сфере киберпреступности, что является одним из этапов на пути к будущему потенциальному членству Украины в ЕС. Также проанализированы научные труды отдельных ученых в контексте данной проблематики.

Ключевые слова: адаптация законодательства, киберпреступность, кибератака, кибербезопасность, Конвенция о компьютерных преступлениях, уголовная ответственность, национальная безопасность.

The article researches the process of adaptation Ukrainian legislation according to general requirements in the area of cybercrime, which is one of the stages on the way to the future potential Ukraine's membership in the EU. The author also analyzes some scientific contributions of researcher in such issues.

Keywords: adaptation of the legislation, cybercrime, cyber-attack, cybersecurity, Convention on Cybercrime, the criminal responsibility, national security.

* Markaryan M.V., Senior Lecturer of the Theory and History of Law Department in Kyiv National Economic University named after Vadym Hetman

STATUS AND PROSPECTS OF ADAPTATION OF UKRAINIAN LEGISLATION TO THE EU REQUESTS IN THE AREA OF CYBERCRIME

Постановка проблеми. З розвитком інформаційно-комунікаційних технологій кіберзлочинність набирає стрімких обертів, зростаючи у кількісних і якісних показниках. Тому для подальшої євроінтеграції перед Україною було поставлене завдання здійснювати співробітництво з членами ЄС для боротьби з кіберзлочинністю, що є неможливим без попередньої гармонізації правового поля та адаптації внутрішнього законодавства до європейського.

Аналіз останніх досліджень і публікацій. Над проблематикою адаптації українського законодавства до законодавства ЄС працювали науковці С. Я. Лихова, П. Л. Фріз, зокрема питання кіберзлочинності були темою досліджень В. М. Бутузова, А. Г. Волеводзи, М. Ю. Літвінова, Ю. Ю. Орлова, О. В. Орлова, Ю. М. Онищенка, Є. Д. Скулиша та ін.

Мета та завдання дослідження. Враховуючи серйозну загрозу, яку несе у собі кіберзлочинність, проаналізувати стан і процес адаптації законодавства України у сфері кіберзлочинності на виконання вимог Угоди про асоціацію між Україною та ЄС та окремих наукових доробків щодо зазначеної проблематики.

Викладення основного матеріалу. Двосторонні відносини між Україною та Європейським Союзом розпочалися відразу після проголошення незалежності нашої держави 1991 року, коли 2 грудня 1991 року було прийнято Декларацію ЄС щодо України. У декларації відзначався демократичний характер Всеукраїнського референдуму і пропонувалося вести відкритий і конструктивний діалог з ЄС.

Але, без сумніву, найголовнішим і найвагомішим документом між Україною і Європейським Союзом стала Угода про асоціацію між Україною та ЄС (далі – Угода про асоціацію), яка була повністю підписана 27 червня 2014 р.

Відповідно до ст. 22 «Боротьба зі злочинністю та корупцією» Угоди про асоціацію сторони домовилися про співпрацю у боротьбі з кримінальною і незаконною організованою діяльністю та з метою її попередження. Серед основних видів незаконної організованої діяльності виокремлюються 6 таких: a) незаконне переправлення через державний кордон нелегальних мігрантів, торгівля людьми і вогнепальною зброєю та незаконний обіг наркотиків; b) контрабанда товарів; c) економічні злочини, зокрема злочини у сфері оподаткування; d) корупція як у приватному, так і в державному секторі; e) підробка документів; f) кіберзлочинність [1, ст.

22]. Наведений перелік наштовхує на висновки про те, що прогресивний розвиток інформаційно-комунікаційних технологій, сучасний стан мобільності громадян і подекуди спрощений процес перетину державних кордонів під впливом лозунгу «Світ без кордонів» створює нові виклики перед світовою спільнотою, з якими можливо боротися лише спільними спланованими зусиллями. Запорукою успішної боротьби бачиться врегульоване правове поле між країнами. Адже не рідко законодавчі прогалини і колізії, відмінності у процесуальних моментах і нормах матеріального права стають на шляху розкриття злочинів.

Серед перерахованих злочинів кіберзлочинність невпинно набирає обертів і масштабів, вражає кількісним та якісним розвитком. Так, за даними звіту Центру скарг щодо Інтернет-злочинів (Internet Crime Complaint Center (IC3), який є структурним підрозділом Федерального Бюро Розслідувань (FBI), за 2014 рік було одержано 269 422 скарги, установлені збитки оцінено в 800 492 073 дол. США. Прослідковано також дві характерних тенденції нинішніх Інтернет-злочинів, а саме: 1) зростаюча кількість користувачів соціальними мережами дає злочинцям широку базу персональних даних; 2) поступово зростає популярність віртуальної валюти, що також привертає увагу і злочинців, які спекулюють на уразливості цифрових валютних систем [2].

Що стосується Європейського Союзу, то Європейський центр кіберзлочинності при Європолі (Europol's European Cybercrime Centre (EC3) опублікував документ «Оцінка Інтернет-організованої злочинної загрози 2015» (Internet Organised Crime Threat Assessment 2015 (IOCTA), у якому сказано, що кібератаки, особливо ті, які включають шифрування, зросли за масштабами та результативністю і є однією із основних загроз сучасності, з якими стикаються як різні підприємства, так і громадяни ЄС. Крім того, на їхню думку, кіберзлочинність стає все агресивнішою і має конфронтаційний характер. Ще одним цікавим фактом цього документу є те, що характерним для 2014 року є рекордна кількість мережевих атак. Навіть засоби масової інформації часто називають 2014 р. як «Рік порушення даних». Проаналізувавши ситуацію, що склалася за вказаний звітний період, фахівці Європейського центру кіберзлочинності при Європолі констатують, що дані (інформація) стали ключовим об'єктом і товаром для кіберзлочинності [3].

Враховуючи специфіку кіберзлочинності, її транскордонний і віртуальний характер, надшвидкий розвиток, постає гостра потреба в кооперації світової спільноти навколо цієї проблеми, врегулювання правових норм внутрішнього і міжнародного права, оскільки досить часто саме від цього залежить розкриття кіберзлочину і притягнення до відповідальності винних.

З метою підвищення ефективності кримінальних розслідувань і переслідувань, що стосуються кримінальних правопорушень, пов'язаних з комп'ютерними системами і даними, і для надання можливості збирання доказів, що стосуються кримінального злочину в електронній формі [4], 23 листопада 2001 було прийнято Конвенцію про кіберзлочинність. Станом на 01.10.2017 Конвенцію про кіберзлочинність ратифікували 56 держав, ще 6 підписали, але не ратифікували [5].

Ратифікувавши цей міжнародний документ, Україна визнала потребу в спільній кримінальній політиці, спрямованої на захист суспільства від кіберзлочинності, а також взяла на себе зобов'язання привести внутрішнє законодавство у стан несуперечливості з Конвенцією про кіберзлочинність.

Фактично всі перетворення українського законодавства були пов'язані з внесенням змін до двох кодексів – Кримінального кодексу України і Кримінального процесуального кодексу України. У науковій праці Ю.Ю. Орлова «Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України» проводиться ґрунтовне дослідження проведених змін в українському законодавстві. Провівши паралелі між положеннями Конвенції і Кримінального кодексу України, автор дійшов висновку, що за більшість злочинів, зазначених у Конвенції, у нашій країні передбачено кримінальну відповідальність. Так, статтям 2–10 Конвенції про кіберзлочинність відповідає низка відповідних статей Кримінального кодексу України [6].

Проте нам не зрозумілою бачиться позиція Ю.Ю. Орлова щодо відсутності згадування про ст. 12 Конвенції «Корпоративна відповідальність», відповідно до якої сторони зобов'язуються вжити «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…». На відміну від деяких інших

статей, де стороні Конвенції надається певна варіативність у законодавчій поведінці (наприклад, ст. 6, 9, 10, 11), ст. 12 Конвенції залишає за державою-учасницею лише вибір щодо виду відповідальності, яка може бути застосована до юридичної особи. Це можна простежити в п.3 цієї статті «Відповідно до юридичних принципів Сторони, відповідальність юридичної особи може бути кримінальною, цивільною або адміністративною» [4, ст. 6, 9–12; 6]. Україна й досі не виконала це положення, хоча кримінальна відповідальність юридичної особи за деякі злочини передбачена Кримінальний Кодексом України.

Як зазначає професор С. Я. Лихова, з 1 вересня 2014 року в силу вступив Закон України від 23 травня 2013 р. «Про внесення змін до деяких законодавчих актів України у зв'язку з виконанням Плану дій щодо лібералізації Європейським Союзом візового режиму для України щодо відповідальності юридичних осіб», яким також було доповнено Загальну частину Кримінального кодексу України розділом XIV-1 «Заходи кримінально-правового характеру щодо юридичних осіб». Проаналізувавши законодавчі нововведення, автор надає перелік злочинів, за які мають нести кримінальну відповідальність юридичні особи, а саме: «Легалізація (відмивання) доходів, одержаних злочинним шляхом» (ст. 209), «Використання коштів, здобутих від незаконного обігу наркотичних засобів, психотропних речовин, їх аналогів, прекурсорів, отруйних чи сильнодіючих речовин, або отруйних чи сильнодіючих лікарських засобів» (ст. 306), «Підкуп службової особи юридичної особи приватного права незалежно від організаційно-правової форми» (ч. 1 і 2 ст. 368^3), «Підкуп особи, яка надає публічні послуги» (ч. 1 і 2 ст. 368^4), «Пропозиція, обіцянка або надання неправомірної вигоди службовій особі» (ст. 369), «Зловживання впливом» (ст. 369^2). Ознайомившись із статтею «Юридичні особи як суб'єкти кримінальної відповідальності за КК України» можна зробити припущення, що автор не є прихильником таких перетворень вітчизняного законодавства, які, на її думку, «засновані не на наукових підходах, і є дещо хаотичними і безсистемними, що призводить, по суті, до руйнування основних теоретичних конструкцій у науці кримінального права» [7].

Підтримуємо позицію професора С. Я. Лихової, проте слід пам'ятати, що деякі сучасні загрози такі, як тероризм, торгівля людьми, зброєю та наркотиками, кіберзлочинність, корупція потребують серйозних заходів і нових методів боротьби. Адже ці

злочини є прямою загрозою національній безпеці держави і притягнення до відповідальності фізичної особи не завжди може розв'язати цю проблему. На підтвердження цього звернемо увагу на точку зору П. Л. Фріза [8], який зазначає, що в середині 90-х років в Україні розпочалася тенденція щодо перетворення організованої злочинності у різноманітні організаційно-правові форми юридичних осіб (кооперативи, ТОВ та ін.), вони практично використовували їх для легалізації доходів, здобутих злочинним шляхом. Як вважає професор П. Л. Фріз, «у такій ситуації будь-які дії, спрямовані проти фізичних осіб – лідерів організованої злочинності, не спроможні призвести до позитивних наслідків. Без ліквідації самих юридичних осіб будь-яка спроба припинити злочинну діяльність буде марною, оскільки на місце фізичних осіб – лідерів організованої злочинності прийдуть інші, що будуть продовжувати злочинну діяльність».

Вважаємо, що ставити в один ряд кіберзлочинність поруч із такими глобальними проблемами сучасності, як корупція і тероризм, дозволяє той факт, що кіберзлочини «виросли» вже з сфери приватного життя й досить часто спрямовані на державні стратегічні об'єкти. А подекуди кіберзлочини, які проявляються у формі кібератак, є частиною чи навіть засобом тероризму.

В умовах гібридної війни, яка ведеться проти України сусідньою державою, вітчизняні державні діячі зрозуміли загрозу інформаційній безпеці, що може бути завдана за допомогою кібератак. Тому підтвердженням є випадок, що трапився 23 грудня 2015 року, коли хакери здійснили кілька потужних кібератак проти українських постачальників електроенергії Прикарпаття, атакувавши шість різних енергокомпаній одночасно. Було використано шкідливу програму, потужнішу, ніж так званий вірус BlackEnergy, який уже застосовувався раніше. Унаслідок цього проблеми зі світлом спостерігалися на території всієї Івано-Франківської області. В результаті сталося відключення електроенергії у 103 населених пунктах України. Розслідування на території України проводили представники ФБР, Держдепартаменту, міністерства внутрішньої безпеки та міністерства енергетики США. За його результатами було виявлено докази того, що за атакою на українську енергосистему стояла група добре підготовлених хакерів з Росії. А вже наприкінці січня 2016 року хакери знову атакували комп'ютерну систему «Укренерго» і розіслали вірусні повідомлення на електронні адреси підприємств електро-

енергетики. Скоріше за все, це була не остання, а, можливо, і не перша кібератака, яку застосувала проти нашої держави країна-агресор.

Робота щодо вдосконалення інформаційного законодавства активізувалася ще після анексії Криму. Рішенням Ради національної безпеки і оборони України від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» з метою попередження та нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері було вирішено розробити і затвердити низку нормативно-правових актів. Зокрема: Стратегію розвитку інформаційного простору України; проект нової редакції Доктрини інформаційної безпеки України; Стратегію кібернетичної безпеки України; проект Закону України про кібернетичну безпеку України; законопроекти про внесення змін до законів України «Про основи національної безпеки України», «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про Службу безпеки України», «Про Державну службу спеціального зв'язку та захисту інформації України» для приведення національного законодавства у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, вдосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України [9].

На виконання рішення РНБО України від 28 квітня 2014 року Адміністрацією Державної служби спеціального зв'язку та захисту інформації України було підготовлено Проект Закону України «Про основні засади забезпечення кібербезпеки України». Даний законопроект Постановою Верховної Ради України від 20.09.2016 № 1524-VIII було прийнято за основу та направлено до Комітету Верховної Ради України з питань інформатизації та зв'язку на доопрацювання.

У пояснювальній записці до цього законопроекту автори зазначають, що реальні прояви кібератак мало прогнозовані, а їх результатом є, як правило, значні фінансово-економічні збитки або непередбачувані наслідки порушень функціонування інформаційно-телекомунікаційних систем, які безпосередньо впливають на стан національної безпеки і оборони. У зв'язку з цим, існуючі загрози вимагають впровадження комплексних заходів, спрямованих на забезпечення кібербезпеки України [10].

Важливим аспектом у цьому законопроекті є спроба заповнити термінологічний вакуум, а також визначити правові та організаційні засади державної політики у цій сфері, основні принципи та напрями забезпечення кібербезпеки. Загалом законопроектом передбачено запровадження таких термінів: «кіберпростір», «кібербезпека», «кіберзагроза», «кіберзлочин», «кіберзлочинність», «кібертероризм», «кібератака», «кіберінцидент», «кіберзахист», «кібероборона» та інші [11].

Також про важливість забезпечення кібербезпеки нашої держави і необхідність боротьби з кіберзлочинністю йдеться у Стратегії національної безпеки України, де серед актуальних загроз національній безпеці України – загрози кібербезпеці і безпеці інформаційних ресурсів.

Дана Стратегія спрямована на реалізацію до 2020 року визначених нею пріоритетів державної політики національної безпеки, а також реформ, передбачених Угодою про асоціацію між Україною та ЄС і Стратегією сталого розвитку «Україна–2020», схваленою Указом Президента України від 12 січня 2015 року № 5 [12].

У Плані дій для України на 2015–2017 роки європейські партнери оцінили проведену роботу України на шляху інтеграції до Європейської спільноти, зокрема і в сфері кіберзлочинності. За підсумками проведено аналізу ситуації встановлено, що деякі проблеми залишилися невирішеними. Насамперед це ті, що пов'язані зі співпрацею проти кіберзлочинності. Крім того, потребує завершення законодавчих реформ стосовно кіберзлочинності (процесуальне законодавство та пов'язані з цим гарантії), закінчення розробки навчальних стратегій щодо кіберзлочинності у сфері судочинства, зміцнення потенціалу міжнародного співробітництва в умовах співробітництва «міліція–поліція» та надання підтримки реалізації проекту стратегії кібербезпеки. Крім того, Рада Європи зауважила, що буде працювати в напрямі зміцнення потенціалу в галузі кримінального правосуддя у сфері боротьби з кіберзлочинністю на основі Будапештської Конвенції, включаючи підтримку підрозділів з боротьби з високотехнологічною злочинністю та правоохоронців з метою налагодження співпраці з постачальниками Інтернет-послуг, заходів проти дитячої порнографії та ефективного міжнародного співробітництва [13].

Висновки перспективи подальших досліджень. Кіберзлочинність стала викликом XXI століття, боротися з якою можливо лише за допомогою спільних зусиль і не лише на міждержавному

рівні, але і внутрішньодержавному у межах співпраці між державним і приватним секторами. На виконання Угоди про асоціацію між Україною та ЄС наша держава зобов'язалася привести внутрішнє законодавство у відповідність з міжнародно-правовими нормами, у тому числі з нормами європейського права у сфері кіберзлочинності. Але варто звернути увагу на те, що для України це не просто обов'язок, але й нагальна потреба. Адже фактично наша держава запізно розпочала процес формування правової бази з регулювання відносин у кіберпросторі. Усвідомлюючи важливість вказаної сфери, за кордоном цей процес розпочався значно раніше. Тому складається ситуація, коли задля виконання зобов'язань перед ЄС здійснюється безсистемний процес нормотворчості шляхом внесення змін і доповнення до наявного внутрішнього законодавства замість створення та напрацювання базисних нормативно-правових актів у сфері інформаційного права. У цьому світлі процес адаптації українського законодавства створює ще більше правових колізій і прогалин у і так недосконалому вітчизняному законодавчому масиві.

Список використаних джерел

1. Угода про асоціацію між Україною та ЄС[Електронний ресурс] – Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/984_011.

2. 2014 Internet CrimeReport [Електронний ресурс] – Режим доступу до ресурсу: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

3. 2015 Internet Organised Crime Threat Assessment [Електронний ресурс] – Режим доступу до ресурсу: https://www.europol.europa.eu/iocta/2015.

4. Конвенція про кіберзлочинність від 23.11.2001 [Електронний ресурс] – Режим доступу до ресурсу: http://zakon4.rada.gov.ua/laws/show/994_575.

5. Рада Європи [офіційний сайт] – Режим доступу: http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures.

6. *Орлов Ю. Ю.* Реалізація вимог Міжнародної конвенції про кіберзлочинність у законодавстві України // Науковий вісник Національної академії внутрішніх справ. – 2011. – №6. – С. 3–9.

7. *Лихова С. Я.* Юридичні особи як суб'єкти кримінальної відповідальності за КК України // Юридичний вісник. – 2014. – №4 (33). – С. 128–132.

8. *Фріз П. Л.* До питання про кримінальну відповідальність юридичної особи // Юридичний вісник. Повітряне і космічне право. – 2015. – №2. – С. 152–156.

9. Рішення РНБО від 28 квітня 2014 року «Про заходи щодо вдосконалення формування та реалізації державної політики у сфері інформаційної безпеки України» [Електронний ресурс] – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/laws/show/n0004525-14.

10.Пояснювальна записка до проекту Закону України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

11.Проект Закону України «Про основні засади забезпечення кібербезпеки України» [Електронний ресурс] – Режим доступу до ресурсу: http://w1.c1.rada.gov.ua/pls/zweb2/webproc4_1?pf3511=55657.

12.Стратегія національної безпеки України: Затверджена Указом Президента України від 26 травня 2015 року № 287/2015 [Електронний ресурс] – Режим доступу до ресурсу: http://zakon5.rada.gov.ua/laws/show/287/2015.

13.План дій для України 2015–2017, документ ухвалений Комітетом Міністрів Ради Європи 21 січня 2015 р. [CM/Del/Dec(2015)1217] [Електронний ресурс] – Режим доступу до ресурсу: https://rm.coe.int/CoERMPublicCommon SearchServices/DisplayDCTMContent?documentId=09000016802f600d.

References

1. Association Agreement between the European Union and the European Atomic Energy Community and their member states, of the one part, and Ukraine, of the other part. Retrieved from https://zakon4.rada.gov.ua/laws/show/984_011(in Ukr.).

2. 2014 InternetCrimeReport. Retrieved from http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf (in Eng.).

3. 2015 Internet Organised Crime Threat Assessment. Retrieved from https://www.europol.europa.eu/iocta/2015(in Eng.).

4. Convention on Cybercrime from 23.11.2001. Retrieved from htt://zakon4.rada.gov.ua/laws/show/994_575(in Ukr.).

5. Council of Europe [official site]. Retrieved from http://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures (in Eng.).

6. OrlovYu. Yu. Implementation of the requirements of the International Convention on Cybercrime in the Ukrainian legislation / Naukovyi visnyk Natsionalnoi akademii vnutrishnikh sprav, 2011, 6, 3–9.

7. LykhovaS. Ya. Legal entities as subjects of criminal responsibility for the Criminal Code of Ukraine,Yurydychnyi visnyk, 2014, 4 (33), 128–132.

8. Friz P. L. On the issue of criminal liability of a legal entity, Yurydychnyi visnyk, Povitriane i kosmichne pravo, 2015, 2, 152–156.

9. Decision of the National Security and Defense Council dated April 28, 2014 «On measures to improve the formation and implementation of state policy in the field of information security of Ukraine». Retrievedfromhttp://zakon5.rada.gov.ua/laws/show/n0004525-14.

10. Explanatory note to the draft Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine». Retrieved from http://w1.c1.rada.gov.ua/ pls/zweb2/webproc4_1?pf3511=55657(in Ukr.).

11. Draft Law of Ukraine «On the Basic Principles of Cybersecurity of Ukraine». Retrieved from http://w1.c1.rada.gov.ua/pls/zweb2/ webproc4_1?pf3511 =55657.

12. The National Security Strategy of Ukraine, approved by the Decree of the President of Ukraine dated May 26, 2015 No. 287/2015. Retrieved from http://zakon5.rada.gov.ua/laws/show/287/2015(in Ukr.).

13. Action Plan for Ukraine 2015-2017, document adopted by the Committee of Ministers of the Council of Europe on January 21, 2015. Retrieved from https://rm.coe.int/CoERMPublicCommonSearchServices/ DisplayDCTMContent?documentId=09000016802f600d(in Ukr.).