Література:

1. Кримінальний кодекс України від 5 квітня 2001 р. № 2341-III (з наступними змінами) // Відомості Верховної Ради України. – 2001. – № 25-26. – Ст. 131.

2. Кримінальне право України. Загальна частина : підручник / [Ю.В. Александров, В.І. Антипов, О.О. Дудоров та ін.] ; за ред. М.І. Мельника, В.А. Клименка. – [вид. 4-те, переробл. та допов.]. – К. : Атіка, 2008. – 376 с.

3. Про практику призначення судами кримінального покарання : постанова Пленуму Верховного Суду України № 7 від 24 жовтня 2003 р. (зі змінами, внесеними постановою № 17 від 26 грудня 2003 р.) // Вісник Верховного Суду України. – 2005. – № 1. – С. 13.

4. Ухвала колегії суддів Судової палати у кримінальних справах Верховного Суду України від 13 січня 2005 р. // Вісник Верховного Суду України. – 2005. – № 3. – С. 29.

Маркарян М.В., асистент (м. Київ, Україна)

ДО ПИТАННЯ ПРО РЕФОРМУВАННЯ ЗАКОНОДАВСТВА УКРАЇНИ У СФЕРІ КІБЕРЗЛОЧИННОСТІ

Прогресивний розвиток інформаційно-комунікаційних технологій, сучасний стан мобільності громадян та 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.

16 вересня 2014 року Угода про асоціацію була одночасно ратифікована Верховною Радою та Європейським парламентом. З 1 листопада 2014 року набуло чинності часткове застосування деяких частин Угоди про асоціацію, а стаття 4 Угоди про асоціацію, у котрій йдеться про встановлення Поглибленої та Всеосяжної Зони Вільної Торгівлі (ПВЗВТ), частково вступила в силу 1 січня 2016 року.

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 наступних: 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.

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 доларів 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 [1].

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 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 [2].

Ставити в один ряд кіберзлочинність поруч із такими глобальними проблемами сучасності, як корупція та 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.

Як приклад є випадок, що трапився 23 грудня 2015 року, коли хакери здійснили кілька потужних кібератак проти українських постачальників електроенергії Прикарпаття, атакувавши шість різних енергокомпаній одночасно. В результаті сталося відключення електроенергії в 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 електроенергетики.

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 й нейтралізації потенційних і реальних загроз національній безпеці в інформаційній сфері було вирішено розробити і

затвердити низку нормативно-правових актів. Зокрема таких: 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.

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». 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.

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 [3].

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.

У Плані дій для України на 2015–2017 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 в 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 [4].

Література:

1. 2014 Internet CrimeReport [Електронний ресурс] – Режим доступу до ресурсу: http://www.ic3.gov/media/annualreport/2014_IC3Report.pdf.

2. 2015 Internet Organised Crime Threat Assessment [Електронний ресурс] – Режим доступу до ресурсу: https://www.europol.europa.eu/iocta/2015.

3. 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.

4. 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.

Канцір В.С., д.ю.н., проф. (м. Львів, Україна)
Олашин М.М., к.ю.н., доц. (м. Львів, Україна)

ТЕРОРИЗМ ЯК ЗАСІБ ДЕСТАБІЛІЗАЦІЇ ДЕРЖАВНОЇ ВЛАДИ

Щільність терористичних загроз як для населення, органів державної влади та держави у цілому настільки концентрована, що світова спільнота звикає (!) аналізувати «найбільш резонансні з резонансних».

Так, 10 жовтня 2015 року в Туреччині стався найбільший теракт за всю історію держави. Два вибухи з інтервалом в три секунди прогриміли вранці в столиці Анкарі в районі залізничного вокзалу. Теракт, влаштований двома терористами-смертниками, став причиною загибелі 95 осіб, 246 отримали поранення.

31 жовтня лайнер Airbus 321 авіакомпанії «Когалимавіа», який виконував рейс 9268 Шарм эль Шейх – Санкт-Петербург, вилетів з Єгипту і зник з екранів радарів через 23 хвилини. На борту перебували 217 пасажирів і сім членів