Сама ж система інформаційної безпеки має бути спрямована на ефективний захист об'єктів національної безпеки: людини і громадянина – їх конституційних прав і свобод; суспільства – його духовних, морально-етичних, культурних, історичних, інтелектуальних та інших цінностей; держави – її конституційного ладу, суверенітету, територіальної цілісності й недоторканності. Такий підхід може стати прикладом для інших країн Східного партнерства, які потерпають від гібридних загроз.

Список бібліографічних посилань

1. Сич О. ЗМІ не мають бути лояльними до влади – вони повинні бути об'єктивними й поважати засади державності // Урядовий портал. 30.04.2014. URL: http://old.kmu.gov.ua/kmu/control/publish/article?art_id=247261779 (дата звернення: 10.10.2019).

2. Куйбіда В.; Розпутенко І. Державне управління безпековою сферою України // Політична праксеологія: безпека, технології, комунікації : матеріали Міжнар. конф. / за ред. В. Бебика. Київ : ВАПН, 2016. С. 5–14.

3. Губерський Л. В. Інформаційна політика України: європейський контекст : монографія / голов. ред. С. В. Головко. Київ : Либідь, 2007. 360 с.

Одержано 15.10.2019

УДК 343.3/.7:004.056.5](477)

Олександр Олександрович ЗАГУМЕННИЙ,
ад'юнкт Харківського національного університету внутрішніх справ

ІСТОРИЧНІ ПЕРЕДУМОВИ ВИНИКНЕННЯ І РОЗВИТКУ КІБЕРЗЛОЧИННОСТІ

Будь-яке явище чи процес має свої корені в минулому та через відображення в сьогоденні спрямоване до майбутнього, тобто існує в логіці причинно-наслідкових зв'язків історичного розвитку із сучасністю [1, с. 127].

Історія злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку почалась в Америці у 1945 році, коли була створена перша електронно-обчислювальні машина (комп'ютер), яка використовувалась для розшифровування німецьких військових кодів, а згодом й для іншої діяльності.

Термін «кіберзлочинність» з'явився в американській доктрині на початку 60-х роках, коли були виявлені перші випадки злочинів, здійснених із використанням комп'ютерів. Саме тоді з'явилися перші «хакери», ними були студенти Масачусетського технологічного інституту, які маніпулювали з програмами нового університетського комп'ютера [2, с. 294]. Електронно-обчислювальні машини (далі – ЕОМ) набули широкого застосування як серед працівників правоохоронних органів так і серед вчених, хоча спочатку для цього не було ні кримінологічних, ні правових підстав [3, с. 17]. Після цього, у 1966 р. зафіксовано перший випадок використання ЕОМ як інструмента при пограбуванні банку в Міннесоті.

Першою людиною, що застосувала ЕОМ для вчинення податкового злочину на суму 620 тисяч доларів і постала за це перед американським судом у 1969 р., був Альфонсо Конфессоре.

Якщо узагальнити історичні аспекти прояву «комп'ютерних» злочинів, то можна виділити наступні події: кінець 70-х це пограбування «Секьюріті пасифік банк» (10,2 млн доларів); 1979 р. – комп'ютерне розкрадання у Вільнюсі (78584 крб.); 1984 р. – повідомлення про перший в світі «комп'ютерний вірус»; 1985 р. – виведення з ладу за допомогою «вірусу» електронної системи голосування в конгресі США; 1986–1988 рр. – поява першого «комп'ютерного вірусу» в СРСР; 1989 р. – блокування американським студентом 6000 ЕОМ Пентагону; 1990 р. – міжнародний з'їзд комп'ютерних «піратів» у Голландії з демонстрацією можливості необмеженого втручання в системи ЕОМ; 1991 р. – розкрадання коштів Зовнішекономбанку на суму в 125,5 тис. доларів; 1992 р. – умисне порушення роботи АСОВІ реакторів Ігналінськой АЕС; 1993 р. – електронне шахрайство в Центробанку Росії (68 млрд крб); 1995 р. – спроба російського громадянина пограбувати Сіті-банк на суму 2,8 млн доларів [4, с. 133].

Так, у 1970 роках у США з'явились «фрікери», які з метою безоплатного телефонування світом, зламували телефонні мережі операторів зв'язку. Одним з таких перших зломщиків-»фрікерів» був Джон Дрейпер, який звернув увагу на те, що іграшковий свисток, який продавався разом з кукурудзяними пластівцями Cap'n Crunch видає звук на частоті 2600 герц, що співпадає з частотою сигналу доступу до телефонної мережі далекого зв'язку компанії AT&T. Джон Дрейпер сконструював першу «блакитну коробку» Blue Box, яка в поєднанні зі свистком і телефонним апаратом дозволила йому робити безкоштовні телефонні дзвінки. При цьому Дрейпер є автором одного з перших текстових редакторів під назвою «Easy Writer» для Apple II в 1979 році. Одних телефонних мереж фрікерам стає замало і у 1980 роках і вони почали втручатись до комп'ютерних мереж. Ними створюються так звані електронні дошки об'яв – BBS, такі як «Sherwood Forest» та «Catch-22» де хакери і фрікери спілкуються та обмінюються досвідом щодо крадіжок паролів та номерів кредитних карток. З'являються перші хакерські спільноти «Legion of Doom» в США та «Chaos Computer Club» в Німеччині.

Перше створення шкідливого програмного засобу, а саме вірусу відбулось у 1988 році, коли студент Корнельського університету Роберт Морріс розробив програму, яка самостійно розмножувалась та «комп'ютерного черв'яка» проникла до майже 6000 університетських та урядових комп'ютерів по всій Америці, внаслідок чого було спричинено велику матеріальну шкоду [2, с. 294].

Перший злочин, здійснений із використанням комп'ютера в колишньому Союзі Радянських Соціалістичних Республік (СРСР), було зареєстровано у 1979 р. у Вільнюсі, ним стало розкрадання, збитки від якого складали 78 584 крб. Цей факт було внесено до міжнародного реєстру правопорушень подібного роду і він став своєрідним початком розвитку нового виду злочинів у колишньому СРСР [5, с. 126]. Проте заходів по протидії комп'ютерним злочинам ще не існувало. Створення комп'ютерної безпеки було поставлено на трохи пізніший час, після того, як студент Корнельського університету зумів потрапити до комп'ютерних систем американської розвідки, міністерства оборони та відключив в цих системах кілька тисяч комп'ютерів. Тоді і були зроблені перші заходи протидії: при університеті Карнегі Меллон у Пітсбурзі на кошти Пентагону була створена комп'ютерна група швидкого реагування – CERT (Computer Emergency Response Team), призначена для реєстрації великих «зломів» комп'ютерних мереж і надання допомоги в «латанні» дірок, проробленних злочинцями [6; 7, с. 96].

Перші спеціальні закони по боротьбі з комп'ютерною злочинністю було прийнято у 1973 році у Швеції та у 1976 році у США. Закони стосовно комп'ютерних злочинів прийняті у 70–80 роки майже усіма індустріально розвинутими країнами. У Сполучених Штатах Америки, які найбільше страждають від комп'ютерних злочинів у 1984 році прийнято Computer Fraud and Abuse Act. Поступово і в інших країнах світу були затверджені законодавчі акти стосовно даної категорії злочинів. До боротьби з комп'ютерними злочинами, виходячи з їх широких масштабів та багатоманітних втрат, підключились міждержавні і громадські 38 організації. Але процес вдосконалення чинного законодавства не припиняється і сьогодні, що пояснюється стрімким розвитком інформаційних технологій [8].

Початок XXI століття ознаменувався широким запровадженням на світовому рівні комп'ютеризованих (автоматичних) інформаційно-технологічних систем у виробничій, комерційній, банківській та інших сферах, у зв'язку з чим головною і водночас невідкладною для вирішення проблемою стала розробка адекватної системи захисту цих систем від несанкціонованого вторгнення. Проблема загострювалась пропорційно до зростання обсягів інформації, переважно завдяки активному функціонуванню глобальної комп'ютерної мережі Інтернет, адже ці злочини не вимагали ані ретельної підготовки, ані часу для втілення злочинного замислу. Широка географія, віддаленість об'єкта посягання (за тисячі і сотні тисяч кілометрів від місця вчинення злочину), складнощі з виявлення, доведення вини, а так само високий дохід, зробили цей вид злочинної діяльності одним з найбільш привабливих для «фахівців» злочинного світу.

Перші кроки щодо протидії кіберзлочинам в Україні були здійснені у 1994 році, коли до Кримінального кодексу 1960 року було внесено зміни, якими в ст. 198-1 «Порушення роботи автоматизованих систем» було передбачено кримінальну відповідальність за умисне втручання у роботу автоматизованих систем, що призвело до перекручення чи знищення інформації або носіїв інформації, чи розповсюдження програмних і технічних засобів, призначених для незаконного проникнення до автоматизованих систем і здатних спричинити перекручення або знищення інформації чи носіїв такої інформації. У 2001 році було прийнято Кримінальний кодекс України (КК України), відповідно до якого ця діяльність вийшла на якісно новий рівень.

Проведено чимало наукових досліджень з цього приводу, у яких вживалися терміни: «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку»; «комп'ютерні злочини»; «кіберзлочини»; «злочини у сфері ІТ технологій»; «високотехнологічні злочини»; «інтернет-злочини»; «злочини у сфері високих технологій»; «е-злочини»; «злочини у сфері інформаційно-телекомунікаційних систем» та ін. Надані визначення є досить схожими, однак у них є і відмінності, відправною точкою для визначення понять, якими оперує законодавець у сфері протидії кіберзлочинності є Конвенція про кіберзлочинність від 23 листопада 2001 року (Конвенція). Сьогодні вона ратифікована 18 державами та підписана 25 країнами, серед яких є і Україна від 7 вересня 2005 року [9].

У липні 2006 року, було ратифіковано додатковий протокол до Конвенції, що стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи (Додатковий протокол) [10]. Термінологія, яка вживається у Конвенції та додатковому протоколі до неї, не знайшла повного відображення у вітчизняному законодавстві. У тексті Конвенції та Додаткового протоколу до неї також не міститься визначення поняття «кіберзлочин» та суміжних з ним понять, однак наявний перелік діянь, за які на національному рівні пропонується встановити кримінальну відповідальність, та наводиться їх умовна класифікація залежно від об'єкта правовідносин [16, с. 4].

Слід зазначити, що в українському законодавстві визначено лише перелік злочинів, які вчиняються з використанням комп'ютерів, комп'ютерних систем та мереж електрозв'язку, закріплених у Розділі XVI КК України. Хоча у деяких законодавчих актах згадуються деякі поняття, проблематику формулювання яких ми розглядаємо, проте в жодному із нормативних актів так і не надано їх визначення. У «Доктрині інформаційної безпеки України» використовувались категорії «комп'ютерна злочинність» та «комп'ютерний тероризм» [11, ст. 1783].

Стратегія національної безпеки, затверджена Указом Президента України від 8 червня 2012 року № 389/2012, містить терміни «кіберзлочинність», «кіберзагроза», «кібербезпека» [12]. У Законі України «Про основи національної безпеки України» згадуються поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» [13, ст. 351]. Законом України «Про основні засади забезпечення кібербезпеки України» надано визначення поняття – кіберзлочин. Кіберзлочин (комп'ютерний злочин) є суспільно небезпечним винним діянням у кіберпросторі та/або з його використанням, відповідальність за яке передбачена законом України про кримінальну відповідальність та/або яке визнано злочином міжнародними договорами України [14, ст. 1].

Частково питання визначення термінології мав би вирішити Закон України «Про кібернетичну безпеку України», проєкт якого було зареєстровано ще 4 червня 2013 року. Проте він не містив визначення кіберзлочину і так і не був прийнятий. Дещо пізніше Указом Президента України від 1 травня 2014 року № 449/2014 «Про рішення 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» було поставлено завдання розробити проєкти Стратегії кібернетичної безпеки України і Закону України «Про кібернетичну безпеку України», а також привести національне законодавство у відповідність із міжнародними стандартами з питань інформаційної та кібернетичної безпеки, удосконалення системи формування та реалізації державної політики у сфері інформаційної безпеки України. Стратегія кібернетичної безпеки України було затверджено Указом Президента України від 15 березня 2016 року № 96/2016 [15].

Попри наявність чинних нормативно-правових актів, вітчизняне законодавство лише частково задовольняє потреби сьогодення, оскільки не містить визначення понять, які є відправними у сфері формування державної інфраструктури інформаційної безпеки. Розв'язання проблеми потребує вдосконалення нормативно-правових актів, які є підґрунтям єдиної державної політики забезпечення інформаційної (кібернетичної) безпеки та її реалізації [16, с. 7].

Список бібліографічних посилань

1. Колпаков В. К. Деліктний феномен в адміністративному праві України : дис. … д-ра юрид. наук : 12.00.07. Київ, 2005. 590 с.

2. Ричка Д. О. Історичні аспекти кіберзлочинності // Сучасний стан і перспективи розвитку держави і права : матеріали VII Міжнар. наук. конф. студентів, аспірантів та молод. вчених. Дніпропетровськ, 2015. С. 293–295.

3. Волеводз А. Г. Противодействие компьютерным преступлениям: правовые основы международного сотрудничества. М. : Юрлитинформ, 2002. 496 с.

4. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. *Вісник Академії адвокатури України.* 2010. Число 3. С. 129–136.

5. Батурин Ю. М. Проблемы компьютерного права. М. : Юрид. лит., 1991. 268 с.

6. Иксар В. Компьютерные преступления // Comprice.ru : сайт. URL: http://www.comprice.ru/articles/detail.php?ID=42319 (дата звернення: 29.10.2019).

7. Бєлєнький В. П. Сучасна історія злочинів у сфері комп'ютерної безпеки. *Правова держава*. 2011. Вип. № 1 (3). С. 96–101.

8. Гуцалюк М. І. Проблеми організаційно-правового забезпечення захисту інформаційних систем в Internet. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні.* 2000. № 1. С. 24–27. URL: http://pnzzi.kpi.ua/1/01_p24.pdf (дата звернення: 29.10.2019).

9. Про ратифікацію Конвенції про кіберзлочинність : закон України від 07.09.2005 № 2824-IV : ред. від 14.10.2010 // База даних (БД) «Законодавство України» / Верховна Рада (ВР) України. URL: https://zakon.rada.gov.ua/laws/show/2824-15 (дата звернення: 29.10.2019).

10. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи : закон України від 21.07.2006 № 23-V (ратифікація 21.07.2006) // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/994_687 (дата звернення: 29.10.2019).

11. Про Доктрину інформаційної безпеки України : указ Президента України від 08.07.2009 № 514/2009. *Офіційний вісник України*. 2009. № 52. С. 7.

12. Стратегія національної безпеки України : указ Президента України від 26.05.2015 № 287/2015 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/287/2015 (дата звернення: 29.10.2019).

13. Про основи національної безпеки України : закон України від 19.06. 2003 № 964-IV : втратив чинність 08.07.2018 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/964-15 (дата звернення: 29.10.2019).

14. Про основні засади забезпечення кібербезпеки України : закон України від 05.10.2017 № 2163-VIII (у ред. 08.07.2018) // БД «Законодавство України» / ВР України. URL: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 29.10.2019).

15. Стратегія кібербезпеки України : указ Президента України від 15.03.2016 № 96/2016 // БД «Законодавство України» / ВР України. URL: http://zakon.rada.gov.ua/laws/show/96/2016 (дата звернення: 29.10.2019).

16. Амелін О. Ю. Визначення кіберзлочинів у національному законодавстві. Науковий *часопис Національної академії прокуратури України*. 2016. Вип. № 3. С. 1–10.

Одержано 01.11.2019

УДК 343.97

Сергій Іванович ЗАДНІЧЕНКО,
заступник начальника Департаменту документального забезпечення – начальник управління організаційного забезпечення та контролю Національної поліції України

КОНФЛІКТ ІНТЕРЕСІВ ЯК СКЛАДОВА ЧАСТИНА ЗЛОВЖИВАННЯ ВЛАДОЮ АБО СЛУЖБОВИМ СТАНОВИЩЕМ: НАЦІОНАЛЬНЕ ТА МІЖНАРОДНЕ ЗАКОНОДАВСТВО

Щодо конфлікту інтересів, то очевидно, що він має місце завжди, а головне завдання держави полягає у запобіганні конфлікту інтересів та його врегулюванні й відповідні службові особи зобов'язані вживати заходів щодо недопущення реального і потенційного конфлікту інтересів. Згідно зі ст. 1 Закону України «Про запобігання корупції» *реальний конфлікт інтересів* – це суперечність між приватним інтересом особи та її службовими чи