УДК 342.951:355.40

Юлія Олександрівна ЗАГУМЕННА,
кандидат юридичних наук, доцент,
професор кафедри теорії та історії держави і права факультету № 1
Харківського національного університету внутрішніх справ;
https://orcid.org/0000-0003-0617-8363;

Наталія Олегівна РАСТОРГУЄВА,
курсантка 3 курсу факультету № 1
Харківського національного університету внутрішніх справ

ПРОБЛЕМИ ЗАБЕЗПЕЧЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В УМОВАХ ГЛОБАЛІЗАЦІЇ ТА ГІБРИДНОЇ ВІЙНИ ПРОТИ УКРАЇНИ

Ключ до перетворення України знаходиться в ній самій.
Нам важко змінити зовнішні обставини,
проте в нашій волі змінити себе.
(Андрій Шептицький, 1941 рік)

В умовах інформаційної агресії з боку Росії та виникнення нових глобальних викликів у інформаційній сфері, зміщення центру ваги вирішення спірних та конфліктних питань на всіх рівнях в інформаційний простір створили нові виклики і загрози в інформаційній сфері.

В таких умовах, протягом останніх років в Українському суспільстві спостерігається тенденція до все більшого розуміння важливості проблем розвитку інформаційної сфери та необхідності забезпечення інформаційної безпеки в усіх сферах життєдіяльності людини, суспільства і держави. Актуальними постають питання формування цілісної системи забезпечення інформаційного суверенітету, управління ризиками і можливостями новітніх викликів в інформаційній сфері, розбудови власних спроможностей і стратегічних комунікацій тощо. Як зауважив О. Сич, «скоординована інформаційна політика органів влади – це не контроль над інформаційним простором, а забезпечення за допомогою інформації єдності держави та непорушності державницьких засад» [1].

Це насамперед пов'язано з процесами, що відбуваються в глобальному інформаційному просторі і характеризуються такими основними тенденціями та особливостями:

1. Глобалізаційні світові процеси та впровадження сучасних інформаційно-комунікаційних технологій обумовили виникнення нових викликів та загроз національній та міжнародній безпеці в інформаційній сфері, здатних завдати значної шкоди інтересам людини, суспільства і держави.

2. В умовах інформаційної агресії проти України Російська Федерація використовує новітні інформаційні технології впливу на свідомість громадян, спрямованого на зниження обороноздатності, розпалювання національної і релігійної ворожнечі, пропаганду агресивної війни, зміну конституційного ладу насильницьким шляхом, порушення суверенітету і територіальної цілісності нашої країни. Загроза постійних поразок від інформаційних агресій, що мають наслідки нанесення шкоди образу нашої країни, стала в сучасних умовах реальністю. У зв'язку з цим, інформаційний та іміджевий поступ країни потребує постійного підтримання зовнішньополітичними рішеннями та вдосконаленням національної інформаційної політики [3].

3. Стрімкий розвиток інформаційних технологій, переваги сучасного цифрового світу, відкритий та вільний кіберпростір зумовили зростання кількості та потужності кібератак, вмотивованих інтересами окремих держав, груп та осіб. Поширюються випадки незаконного використання персональних даних та здійснення фінансових операцій, крадіжок і шахрайства в мережі Інтернет. Кіберзлочинність стає транснаціональною.

4. Залишається не вирішеним на законодавчому рівні питання системи інформаційної безпеки. Нова Доктрина інформаційної безпеки України, яка готувалася в умовах гібридної агресії Російської Федерації, не орієнтує на вирішення усього комплексу виявлених проблем, не загострює проблеми необхідності їх законодавчого врегулювання.

5. Управління безпекою в інформаційній сфері залишається найбільш неврегульованою сферою і потребує суттєвого вдосконалення взаємодії, координованості та узгодженості дій і рішень усіх гілок влади з питань виконання конституційних повноважень щодо забезпечення інформаційної безпеки України.

У статті В. Куйбіди, І. Розпутенко «Державне управління безпековою сферою України» наголошується на важливості забезпечення державного та національного суверенітету, шляхом сприяння та удосконалення державної інформаційної політики у воєнній сфері, а також зосередити розробки системи ефективної протидії інформаційно-психологічним впливам іноземних держав, які спрямовані на підрив обороноздатності, порушення суверенітету і територіальної цілісності України, дестабілізацію внутрішньої соціально-політичної обстановки, провокування міжетнічних та міжконфесійних конфліктів в Україні [2].

Таким чином, забезпечення інформаційної безпеки людини, суспільства і держави має дійсно стати системою, до якої будуть залучені не тільки силові структури, але й неурядові організації, приватний сектор, бізнес, експертні і наукові кола, незалежні ЗМІ та інші. Тільки комплексний всеохоплюючий підхід дозволить консолідувати суспільство і забезпечити його безпеку.

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].