Пашнєв Дмитро Валентинович,
кандидат юридичних наук, доцент
(Харківський національний університет внутрішніх справ)

УДК 343.3

НЕОБХІДНІСТЬ СПЕЦІАЛЬНОЇ КРИМІНАЛЬНО-ПРАВОВОЇ ОХОРОНИ КРИТИЧНОЇ ІНФОРМАЦІЙНОЇ ІНФРАСТРУКТУРИ

В статті виявлена різна суспільна небезпечність посягань на інформаційну безпеку на різних її рівнях відповідно до об'єкту (держава, суспільство, особа). Обґрунтована необхідність спеціальної кримінальної відповідальності за суспільно небезпечні

посягання на інформаційно-телекомунікаційні системи суспільного та державного значення (об'єкти критичної інформаційної інфраструктури).
Ключові слова: *кримінальна відповідальність, комп'ютерний злочин, критична інформаційна інфраструктура*

Зважаючи на процеси поступової модернізації безпекового сектору в Україні та стремління ствердитися у якості повноправного партнера на європейському та трансатлантичному безпековому просторі, питання захисту критичної інфраструктури стає все більш актуальним.

З-поміж техногенних загроз критичній інфраструктурі держави особлива увага приділяється втручанням в роботу автоматизованих систем управління технологічним процесом на підприємствах та об'єктах інфраструктури. Хоча у світі досі не повідомлялося про факти руйнувань унаслідок кібератак на критичну інфраструктуру, однак було зафіксовано численні (за оцінками експертів, на 45 тис. об'єктах по всьому світу) випадки зараження автоматизованих систем управління технологічним процесом (перепрограмування контролерів) вірусом Stuxnet [1], а серед останніх подій – спроби втручання в роботу автоматизованих систем управління об'єктів газотранспортних систем США [2].

З огляду на такі тенденції, розпочалося становлення нормативно-правової бази у сфері захисту критичної інфраструктури. Напевно, найбільших успіхів у цій сфері досягли США, де було прийнято низку правових заходів в рамках національної програми «Захист критичної інфраструктури», серед яких: Адміністративний наказ Президента США № 13010 «Про роботу з дослідження вразливості захисту критичної інфраструктури від кібернетичних і фізичних загроз» (липень 1996 р.), Директива Президента США № 63 (травень 1998 р.) [3], Національний план із захисту інформаційних систем (січень 2000 р.), адміністративний наказ Президента США № 13231 «Про захист національних критичних інформаційних систем» (жовтень 2001 р.), Політика у сфері кіберпростору (2009 р.) [4].

У цих нормативних актах одержала офіційне визнання повна залежність інфраструктури сучасної країни від інформаційних систем та мереж і уразливість останніх. Аналогічна залежність спостерігається і в Україні, проте, за висновками експертів, чинна вітчизняна нормативно-правова база у сфері

протидії злочинам в кіберпросторі лише частково задовольняє потреби часу та не завжди охоплює всі ключові елементи, які необхідні для ефективної протидії кіберзлочинам всіх рівнів складності [5].

Нещодавні хакерські атаки, в результаті яких були виведені з ладу сайти центральних органів влади [6], яскраво показують уразливість державних інформаційних ресурсів і комп'ютерних систем. Це дозволяє тільки припускати висновки про стан захищеності об'єктів критичної інформаційної інфраструктури держави, і відсутність поки що посягань на них, крім все ж таки ще не великого ступеню залежності критичної інфраструктури від інформаційних систем, може бути пояснена тільки наявністю здорового глузду в осіб, здатних на це.

В такій ситуації, зважаючи на зростання негативних наслідків для держави, які завдаються кібератаками на інформаційну інфраструктуру органів державної влади, та на можливу шкоду, пов'язану з можливими кібератаками на промислові та інші об'єкти критичної інфраструктури, їх підвищену суспільну небезпечність, підвищеної актуальності набуває кримінально-правова охорона критичної інформаційної інфраструктури.

Взагалі, питання кримінальної відповідальності за комп'ютерні злочини торкалися в своїх дослідженнях багато вчених, зокрема: М. І. Панов, П. П. Андрушко, В. М. Бутузов, Д. С. Азаров, В. О. Голубєв, С. В. Дрьомов, Т. В. Міхайліна, М. В. Плугатир, С. О. Орлов, Н. А. Розенфельд, М. В. Рудик. Аналіз цих досліджень показує, що дискусійними залишаються питання про ознаки й сутність інформації як предмета злочину, зміст інших ознак складів «комп'ютерних» злочинів (ст.ст. 361–363[1] КК України), напрями вдосконалення відповідних положень законів про кримінальну відповідальність. Актуалізує означені питання очевидна неефективність засобів кримінальної юстиції в цій сфері, про що свідчить аналіз відповідної судової практики [7, с. 32].

Загальна думка наукової співдружності щодо питання саме кримінально-правової охорони критичної інформаційної інфраструктури простежується у Рекомендаціях однієї із останніх міжнародних конференцій, де зауважується на необхідності «деталізації правових норм щодо відповідальності за несанкціоноване втручання та несанкціоновані дії щодо державних електронних інформаційних ресурсів та інформаційно-телекомунікаційних систем об'єктів критичної інформаційної

інфраструктури держави, диференціації відповідальності за вчинення таких протиправних посягань» [8].

Нещодавно такі рекомендації було втілено у життя. Кримінальний кодекс України доповнено статтями 361^3, 361^4 та 362^1 Законом України від 16.01.2014 р. № 721-VII «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів захисту безпеки громадян» [9], який втратив чинність на підставі Закону України від 28.01.2014 р. № 732-VII «Про визнання такими, що втратили чинність, деяких законів України» [10]. Проте в тексті КК України на офіційному сайті Верховної Ради України ці статті присутні із коментарем «Кодекс доповнено статтею … згідно із Законом № 721-VII від 16.01.2014 – втратив чинність на підставі Закону № 732-VII від 28.01.2014» [11].

Причини такої ситуації напевно пов'язані із складними часами, у які ці зміни були прийняті та відмінені. Єдиний результат, який залишився: завдання кримінально-правової охорони інформаційної складової критичної інфраструктури України не вирішене. Отже метою цієї статті є з'ясування необхідності спеціальної кримінально-правової охорони критичної інформаційної інфраструктури на основі аналізу вітчизняних досліджень та закордонного досвіду.

Питання охорони критичної інформаційної інфраструктури тісно пов'язане із інформаційною безпекою держави. У загальнотеоретичних дослідженнях питань безпеки як категорії права пропонується виділяти такі її види, як безпека особи, безпека суспільства та безпека держави. До безпеки особи відноситься здатність і готовність держави, суспільства захищати індивіда від загроз та небезпек для його життя, здоров'я, майна, цивільних прав, свобод і законних інтересів. Під безпекою суспільства розуміється певна множинність станів соціальної системи, за якої забезпечується її стабільність і розвиток. Нарешті, безпека держави відображає соціальну потребу – потребу суспільства та його громадян у забезпеченні територіальної цілісності та суверенітету держави, основ політичного, економічного та конституційного ладу як найважливішої умови економічного, національного, духовного розвитку суспільства та кожного його члена [12]. Отже, можна говорити про такі види інформаційної безпеки за ознаками джерела інформаційних потреб: інформаційна безпека особи; інформаційна безпека суспільства; інформаційна безпека держави.

В жодному разі не встановлюючи певну ієрархію пріоритетів інтересів вказаних об'єктів безпеки, ми хочемо звернути увагу на очевидний, на наш погляд, факт зворотної залежності безпеки одних об'єктів від стану безпеки інших: порушення безпеки держави у будь-якому разі потягне за собою шкоду для безпеки суспільства та особи, а шкода безпеці суспільства не омине безпеку особи.

Таким чином, з кримінально-правової точки зору посягання на інформаційно-телекомунікаційні системи суспільного та державного значення мають більшу ступінь суспільної небезпеки. Відповідно і міра кримінальної відповідальності має бути суворішою, що і було реалізовано в санкціях норм, які були додані до КК України 16.01.2014 р.

Як вірно вказує Д. С. Азаров, характер суспільної небезпеки комп'ютерних злочинів обумовлюється ще одним фактором: специфікою та важливістю їхнього об'єкта – суспільних відносин у сфері комп'ютерної інформації, які акумулюють у собі значні сегменти інших галузей життєдіяльності людства [13, с. 36].

Виходячи з цього на практиці часто виникають певні проблеми кваліфікації цих злочинів, пов'язані із порушенням при їх вчиненні не тільки свого безпосереднього об'єкта, але й інших об'єктів кримінально-правової охорони. Єдиним шляхом урахування підвищеної суспільної небезпечності таких злочинів є кваліфікація їх за правилами сукупності зі статтями інших розділів КК України [14].

Проте іноді такий підхід реалізувати не вдається через відсутність прямої шкоди іншим суспільним відносинам, крім тих, що входять до родового об'єкту розділу 16 КК України. Шкода завдається лише інформаційним відносинам і відсутність диференціації їх за різними сферами суспільного життя в кримінальному законі дозволяє враховувати ступінь їх суспільної небезпечності для певної сфери лише в рамках існуючої санкції відповідної статті розділу 16 КК України. Але ж, як було вказано вище, рівень важливості інформаційних відносин залежно від рівня об'єкту безпеки (держава, суспільство, особа) суттєво відрізняється.

На підтвердження наших доводів звернемося до кримінального законодавства іноземних країн, де можна зустріти не один приклад норм, спрямованих на охорону інформаційно-телекомунікаційних систем державного та суспільного значення.

Зокрема, серед федеральних законодавчих актів США, норми яких передбачають кримінальну відповідальність за злочини у сфері комп'ютерної інформації, насамперед потрібно назвати 18-й звід законів США, а саме ст. 1030 глави 47, якою передбачена відповідальність за такі діяння: збирання інформації, яка стосується національної безпеки, міжнародних зносин, атомної енергетики, використання цієї інформації на шкоду США або в інтересах інших держав; збирання або отримання інформації від фінансових та урядових установ; втручання в роботу комп'ютера, який використовується урядом; шахрайство, вчинене з використанням доступу до федерального комп'ютера [15, с. 105].

КК Нідерландів у розділі XXVII «Знищення або нанесення шкоди» передбачає відповідальність за руйнування, псування, приведення у непридатність чи несправність, знищення комп'ютера чи системи для зберігання і обробки даних, телекомунікаційного приладу призначених для використання населенням або для національної оборони (статті 351, 351bis) [16].

Кодекс Франції передбачає відповідальність за дії, вчинені з комп'ютерною інформацією на шкоду інтересам держави. Перелік даних складів злочинів також досить великий: збір чи передача міститься у пам'яті ЕОМ або картотеці інформації іноземній державі, знищення, розкрадання, вилучення або копіювання даних, що носять характер секретів національної оборони, що містяться в пам'яті ЕОМ або в картотеках, а також ознайомлення з цими даними сторонніх (ст.ст. 411-7, 411-8, 413-9, 413-10, 413-11). У КК Іспанії відповідальність встановлена за розкриття та видачу таємниці та інформації, пов'язаних з національною обороною, вчинені з використанням інформаційних технологій (ст.ст. 598, 599).

У ст. 269 глави XXXIII «Злочини проти охорони інформації» КК Республіки Польща передбачена відповідальність за знищення, пошкодження, видалення або зміну запису на комп'ютерному носії інформації, що має значення для обороноздатності держави, безпеки зв'язку, функціонування урядової адміністрації, іншого державного органу або адміністрації органу самоврядування, або порушення чи унеможливлення автоматизованого збирання або передачі такої інформації; знищення чи заміну носія інформації або знищення чи пошкодження пристрою, що служить автоматизованому перетворенню, збиранню або передачі такої інформації [17].

Отже, досвід іноземних країн вказує на підвищену увагу до кримінально-правової охорони державних інформаційних ресурсів, що визначається у встановленні відповідальності за посягання на них не у загальних, а у спеціальних нормах. І з огляду на приведені нами вище доводи, такий підхід є виправданим, оскільки посягання на державні інформаційно-телекомунікаційні системи, зважаючи на їх значення для суспільства, повинні тягти за собою спеціальну відповідальність.

Кримінальний кодекс України містить шість статей, які призвані охороняти інформаційно-телекомунікаційні системи від суспільно небезпечних посягань (ст. 361–363[1]). Їх зміст суперечить вказаному підходу, оскільки державні інформаційно-телекомунікаційні системи та інформаційні ресурси є лише окремим видом предмету складів цих злочинів, поряд з іншими, посягання на які мають значно нижчий ступінь суспільної небезпечності. Це не дозволяє виокремити особливості суспільно небезпечних діянь, вчинених з використанням комп'ютерних технологій проти інформаційно-телекомунікаційних систем державного та суспільного значення, індивідуалізувати відповідальність осіб, які їх вчинили.

В такій ситуації порушується одна із загальнокерівних засад кримінального права – принцип справедливості, який передбачає, зокрема, найбільш повне врахування об'єктивних ознак вчиненого особою діяння, а також пом'якшуючих та обтяжуючих покарання обставин при притягненні її до кримінальної відповідальності, при призначенні покарання, вирішенні питань звільнення від покарання та його відбування, погашення та зняття судимості.

Таким чином, приходимо до висновків:

1. Інформаційна безпека на різних рівнях має суттєву різницю у ступені суспільного значення, що за спаданням слід розташувати так: держава-суспільство-особа. Відповідно і посягання на цих рівнях мають різну суспільну небезпечність, що повинне враховуватися у Законі про кримінальну відповідальність, проте існуючі положення КК України не дозволяють дотримуватися таких вимог.

2. Аналіз реалізації таких вимог у законодавстві інших країн показує, що врахування суспільної небезпечності посягань на різні об'єкти інформаційної безпеки відбувається шляхом встановлення спеціальної відповідальності за злочини про-

ти державних інформаційно-телекомунікаційних систем та інформації, яка в них оброблюється.

3. Доповнення Кримінального кодексу України статтями 361^3, 361^4 та 362^1 є цілком актуальним, необхідним і доцільним. Відміна таких змін разом з іншими Законами, які були прийняті 16.01.2014 р., є помилковою. Отже слід розробити вже окремий законопроект, за змістом аналогічний частині відповідного закону, яким були внесені ці зміни, та прийняти його з метою вирішення завдання спеціальної кримінально-правової охорони критичної інформаційної інфраструктури України.

Список використаних джерел:

1. Stuxnet Dossier // Symantec Security Response. – February. – 2011. – 68 p.

2. ICS-CERT Monthly Monitor. – 2012. – April [Електронний ресурс]. – Режим доступу: http://www.us-cert.gov/control_systems/pdf/ICS-CERT_Monthly_Monitor Apr2012.pdf.

3. Critical Infrastructure Protection Federation of American Scientists : PDD-63 [Електронний ресурс]. – Режим доступу: http://www.fas.org/irp/offdocs/pdd/ pdd-63.pdf.

4. Cyber space policy review: Assuring a Trusted and Resilient Information and Communications Infrastructure / The White House. – Washington, 2009 [Електронний ресурс]. – Режим доступу: http://www.whitehouse.gov/assets/documents/Cyberspace_Policy Review_final.pdf.

5. Дубов Д. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування : Аналітична записка [Електронний ресурс] / Дубов Д., Ожеван М. ; Відділ досліджень інформаційного суспільства та інформаційних стратегій Національного інституту стратегічних досліджень. – Режим доступу: http://www.niss.gov.ua/articles/454/.

6. Захист інформаційних мереж є питанням державної безпеки – голова Держспецзв'язку Геннадій Резніков [Електронний ресурс] / Віталій Сич ; УКРІНФОРМ. – 29.08.2012 р. – Режим доступу: http://www.ukrinform.ua/ukr/news/zahist_informatsiynih_mereg_e__pitannyam_dergavnoii_bezpeki___golova_dergspetszvyazku_gennadiy_reznikov_1752176.

7. Кримінально-правова охорона інформаційної безпеки України : монограф. / М. В. Карчевський ; МВС України, Луган. держ. ун-т внутр. справ ім. Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

8. Рекомендації VI Міжнародної конференції «Захист демократичних цінностей і дотримання прав людини у діяльності

спецслужб» (Київ, 24 квітня 2013 року) [Електронний ресурс] / Служба безпеки України. Режим доступу: http://ssu.kmu.gov.ua/sbu/doccatalog/document?id=117284.

9. Закон України від 16.01.2014 р. № 721-VII «Про внесення змін до Закону України «Про судоустрій і статус суддів» та процесуальних законів щодо додаткових заходів захисту безпеки громадян» // Голос України. – 21.01.2014 р. – № 10.

10. Закон України від 28.01.2014 р. № 732-VII «Про визнання такими, що втратили чинність, деяких законів України» // Голос України. – 01.02.2014 р. – № 19.

11. Кримінальний кодекс України від 05.04.2001 р. № 2341-III [Електронний ресурс] / Верховна Рада України : Законодавство. – 28.02.2014 р. – Режим доступу: http://zakon4.rada.gov.ua/laws/show/2341-14.

12. Зинченко Н. И. Обеспечение безопасности личности, общества и государства: концептуально-теоретический аспект / Н. И. Зинченко // Социально-гуманитарное знание. – 2006. – № 6. – С. 175 – 188.

13. Азаров Д. С. Кримінальна відповідальність за злочини у сфері комп'ютерної інформації : дис. ... канд. юрид. наук: 12.00.08 / Д. С. Азаров. – К., 2002. – 246 с.

14. Васильєв А. А. Особливості кваліфікації злочинів у сфері використання ЕОМ (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку / А. А. Васильєв, Д. В. Пашнєв // Вісник Кримінологічної асоціації України : збірник наукових праць [редкол. Л. М. Давиденко, Т. А. Денисова, О. М. Джужа та ін.]. – Х. : Золота миля, 2013. – С. 34–42.

15. Айков Д. Компьютерные преступления. Руководство по борьбе с компьютерными преступлениями: Пер. с англ. / Айков Д., Сейгер К., Фонсторх У. – М. : Мир, 1999. – 351 с.

16. Уголовный кодекс Голландии / [науч. ред. докт. юрид. наук, заслуж. деятель науки РФ, проф. Б. В. Волженкин ; пер. с англ. И. В. Мироновой] – СПб. : Юридический центр Пресс, 2001. – 510 с. – (Законодательство зарубежных стран).

17. Уголовный кодекс Республики Польша / [науч. ред. канд. юрид. наук, доц. А. И. Лукашов, докт. юрид. наук, проф. Н. Ф. Кузнецова ; вступ. статья канд. юрид. наук, доц. А. И. Лукашова, канд. юрид. наук, проф. Э. А. Саркисовой ; пер. с польск. Д. А. Барилович]. – СПб. : Юридический центр Пресс, 2001. – 234 с. – (Законодательство зарубежных стран).

В статье выявлена разная общественная опасность посягательств на информационную безопасность на разных ее уровнях в соответствии с объектом (государство, общество, чело-

век). Обоснована необходимость специальной уголовной ответственности за общественно опасные посягательства на информационно-телекоммуникационные системы общественного и государственного значения (объекты критической информационной инфраструктуры).
Ключевые слова: *уголовная ответственность, компьютерное преступление, критическая информационная инфраструктура*

The different public danger of infringements on information security at its different levels, in accordance to object (state, society, people) is revealed in the article. The necessity of a special criminal liability for social and dangerous infringement on the telecommunication system of public and state importance (the objects of critical information infrastructure) is substantiated.
Key words: *criminal liability, computer crime, critical information infrastructure.*

Стаття надійшла до редакції 03.03.2014