На загальнодержавному рівні слід відзначити ВГО "Асоціація суддів України" (до 2007 р. організація мала назву "Всеукраїнська незалежна суддівська асоціація"), ВГО "Асоціація суддів та працівників судів України", ВГО "Судова асоціація України "Фундація сприяння правосуддю".

Практична діяльність громадських об'єднань суддів, зазвичай, полягає в проведенні заходів, спрямованих на зміцнення незалежності суддів, обговорення законопроектів і поточних проблем чинного законодавства; співробітництво з органами суддівського самоврядування, Вищою кваліфікаційною комісією суддів України, Вищою радою юстиції України, Державною судовою адміністрацією України й критичний аналіз їх роботи; підвищення професійної кваліфікації суддів та організацію обміну досвідом з суддями інших країн; задоволення інформаційних, культурно-просвітницьких та інших потреб працівників суддівського корпусу та захист спільних інтересів своїх членів[1]; участь у роботі громадської ради при Державній судовій адміністрації України та інших органах державної влади; підвищення авторитету судової влади та належне здійснення судової реформи.

Отже, громадські об'єднання адвокатів і суддів є потужним передовим загоном громадянського суспільства, ефективно обстоюючи не тільки вузькопрофесійні інтереси, але й загальний запит української громади щодо послідовного реформування правової системи країни, утвердження справедливого балансу інтересів особи й держави.

Перспективним напрямом подальших наукових досліджень є аналіз організаційно-правових проблем узаємодії національних і міжнародних громадських об'єднань юридичного профілю.

УДК 343.3/.7

М.В. Карчевський

ЧИ ПОТРІБНА КРИМІНАЛЬНА ВІДПОВІДАЛЬНІСТЬ ЗА ПОРУШЕННЯ ПОРЯДКУ АБО ПРАВИЛ ЗАХИСТУ КОМП'ЮТЕРНОЇ ІНФОРМАЦІЇ (СТ. 363 КК УКРАЇНИ)?

Здійснюється спроба встановити причини вкрай незначної судової практики у сфері протидії порушенню правил експлуатації комп'ютерних засобів оброблення інформації та мереж електрозв'язку, а також порушенню порядку чи правил захисту інформації (ст. 363 КК України). Питання щодо доцільності збереження означеної норми розглядається в контексті раціональної парадигми кримінального права.

[1] Рішення Ради суддів України № 36 від 15 вересня 2014 року [Електрон. ресурс]. – Режим доступу: http://. court.gov.ua/userfiles/file/DSA/RSU_site/2014/rsu3612092014.pdf.

Ключові слова: *злочини у сфері використання комп'ютерної техніки, раціональна парадигма кримінального права, порушення порядку чи правил захисту комп'ютерної інформації, порушення правил експлуатації комп'ютерних засобів оброблення інформації.*

Предпринимается попытка установить причины крайне незначительной судебной практики в сфере противодействия нарушению правил эксплуатации компьютерных средств обработки информации и электросвязи, а также нарушению порядка или правил защиты информации (ст. 363 УК Украины). Вопрос о целесообразности сохранения данной нормы рассматривается в контексте рациональной парадигмы уголовного права.

Ключевые слова: *преступления в сфере использования компьютерной техники, рациональная парадигма уголовного права, нарушение порядка или правил защиты компьютерной информации, нарушение правил эксплуатации компьютерных средств обработки информации.*

An attempt is made to establish the causes of extremely insignificant judicial practice in combating to violation of regulations of computer processing of information and telecommunications, as well as violation of the order or the rules of information protection (Art. 363 of the Criminal Code). The continued relevance of this norm is considered in the context of the rational paradigm of criminal law.

Key words: *crime in the use of computer technology, the rational paradigm of criminal law, violation of the order or the rules of computer information protection, violation of the rules of operation of computer information processing facilities.*

Не можна сказати, що питання кримінальної відповідальності за порушення правил експлуатації комп'ютерних засобів оброблення інформації та мереж електрозв'язку, а також порушення порядку чи правил захисту інформації (ст. 363 КК України) отримали достатній рівень наукового аналізу. Певні аспекти досліджували Д.С. Азаров, П.П. Андрушко, С.В. Дрьомов.

Разом з цим очевидною є недостатня ефективність означеної кримінально-правової заборони. Украй незначна практика використання ст. 363 КК не відповідає кримінологічній характеристиці злочинів у сфері використання комп'ютерної техніки. Як неодноразово зазначалося, фахівці з інформаційної безпеки переважну більшість "комп'ютерних" злочинів пов'язують саме з діяльністю спеціальних суб'єктів, осіб, які мають певні повноваження щодо інформації, яка виступає предметом посягання. Наприклад, у доповіді Global Security Report компанії Trustwave, одного з лідерів ринку апаратних та програмних продуктів для захисту інформації, зазначається, що близько 88 відсотків порушень інформаційної безпеки пов'язано з використанням відповідальними особами недостатньо надійних криптографічних засобів або неналежного рівня безпеки у використанні програмного забезпечення сторонніх виробників [12]. Чинне законодавство містить дві норми про відповідальність таких осіб –

статті 362 та 363 КК. Однак з-поміж осіб, засуджених у 2008 році, лише 12,3% були засуджені за ст. 362, а за ст. 363 взагалі не було засуджено жодної особи [7]. Аналіз актуальної судової практики свідчить про збереження означеної тенденції. Отже, практика застосування національного законодавства явно не відповідає експертним оцінкам щодо структури "комп'ютерної" злочинності. При цьому така невідповідність лежить далеко за межами статистичної похибки, ідеться про переважну більшість в оцінках експертів і меншість у статистичних показниках.

Таким чином, *актуальним є встановлення причин названих тенденцій національної судової практики, а також розгляд питання щодо доцільності збереження кримінальної відповідальності порушення правил захисту комп'ютерної інформації.*

Перш за все необхідно окреслити зміст ознак досліджуваного складу злочину. Отже, *об'єкт* складають суспільні відносини, у межах яких забезпечується безпека використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, а також дотримання порядку та правил захисту комп'ютерної інформації.

Склад злочину, передбаченого статтею 363 КК України, матеріальний. Його об'єктивна сторона характеризується такими ознаками:

1) діяння – порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту комп'ютерної інформації;

2) суспільно небезпечні наслідки – значна шкода;

3) причинний зв'язок між діянням і суспільно небезпечними наслідками.

Аналіз диспозиції дозволяє дійти висновку про те, що діяння може виявлятися в трьох альтернативних формах:

– порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку;

– порушення порядку захисту комп'ютерної інформації;

– порушення правил захисту комп'ютерної інформації.

Порушення правил експлуатації ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку – недотримання вимог, що ставляться власником ЕОМ, автоматизованої системи, комп'ютерної мережі або мережі електрозв'язку до їх використання або обслуговування. Таке порушення може полягати, наприклад, у спробі користувача самостійно встановлювати нове програмне або апаратне забезпечення, підключенні комп'ютерної техніки до електромережі без фільтрів, порушенні порядку включення або відключення засобів комп'ютерної техніки тощо.

Порушення порядку захисту комп'ютерної інформації – недотримання визначених нормативними актами вимог щодо створення системи захис-

ту інформації та організації її роботи. Прикладом такого діяння може бути використання комп'ютерної техніки для роботи з таємною інформацією за відсутності сертифікованої належним чином системи захисту.

Порушення правил захисту комп'ютерної інформації – недотримання вимог щодо використання системи захисту інформації певного інформаційного ресурсу. Це може бути, наприклад, неналежне зберігання паролів для доступу до інформації.

Оскільки аналізований склад злочину є матеріальним, він буде вважатися закінченим від моменту настання суспільно небезпечних наслідків – значної шкоди.

Суб'єкт злочину, передбаченого ст. 363 КК, - спеціальний. Це – особа, яка відповідає за експлуатацію ЕОМ (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку. Такий статус особи встановлюється відповідним наказом або розпорядженням власника інформації чи засобу її автоматизованого опрацювання та закріпленими на підставі цього наказу функціональними обов'язками.

Суб'єктивна сторона цього злочину характеризується тим, що діяння може бути вчинено як умисно, так і з необережності, а щодо наслідків завжди має бути необережність. Якщо настання наслідків охоплюється умислом винної особи, то склад злочину, передбачений ст. 363 КК, - відсутній. У таких випадках дії винної особи, за наявності відповідних ознак, необхідно кваліфікувати як умисне пошкодження майна (ст. 194 КК), або як пособництво в несанкціонованому втручанні в роботу ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ч. 5 ст. 27, ст. 361 КК), або як несанкціоновані дії з комп'ютерною інформацією, вчинені особою, яка має до неї доступ (ст. 362 КК)[9, с. 151-157].

Отже, за винятком деяких технічних зауважень[1] ст. 363 КК України представляє собою задовільну кримінально-правову базу для мінімізації соціальних ризиків порушення порядку та правил захисту комп'ютерної інформації. Разом з цим темпи інформатизації та комп'ютеризації українського суспільства, наведені на початку експертні оцінки структури "комп'ютерної" злочинності, дозволяють уважати обґрунтованою гіпотезу про те, що на сьогодні значна частка суспільно небезпечних наслідків у сфері використання комп'ютерної техніки настає через недотримання правил або порядку захисту інформації. Вочевидь, що *однією з вагомих*

[1]Законодавче визначення суб'єкта досліджуваного злочину перебуває у невідповідності з формами об'єктивної сторони. Слід погодитися з зауваженням А.А. Музики та Д.С. Азарова, що "не може вважатися злочином порушення правил (порядку) захисту інформації, учинене особою, яка за забезпечення цього захисту відповідає, а за дотримання правил експлуатації техніки – ні" [8, с. 78].

причин відсутності означених інцидентів у полі кримінальної юстиції, украй незначної практики застосування ст. 363 КК України слід уважати вади нормативної регуляції захисту комп'ютерної інформації.

Базовим нормативним документом у сфері захисту комп'ютерної інформації є Закон України "Про захист інформації в інформаційно-телекомунікаційних системах" від 31 травня 2005 року. У цьому законі сформульовано, можна сказати, головний принцип регулювання питань захисту комп'ютерної інформації національним законодавством: *відповідальність за захист інформації покладається на власника системи (у якій вона обробляється), при цьому в тих випадках, коли в системі обробляється інформація, що є власністю держави, або інформація з обмеженим доступом, вимога щодо захисту якої встановлена законом, вона повинна оброблятися в системі з застосуванням комплексної системи захисту інформації з підтвердженою відповідністю.* Тобто спеціальні вимоги встановлюються лише до захисту державної інформації або інформації, захист якої спеціально передбачено в законі. Решта нормативних актів у сфері інформаційної безпеки конкретизує це положення.

Спеціальних вимог щодо захисту комп'ютерної інформації, яка не є власністю держави, крім положення Закону України "Про захист інформації в автоматизованих системах", про те, що захист інформації покладається на власника системи, *національне законодавство не встановлює.* Тому порушення правил експлуатації ЕОМ, автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку, у яких обробляється недержавна інформація, стосовно якої законодавство не встановлює спеціальних вимог щодо забезпечення її захисту, а також порушення порядку чи правил захисту такої інформації, якщо воно заподіяло істотну шкоду, буде вважатися злочином, передбаченим ст. 363 КК України, лише тоді, коли власником інформації або власником засобу автоматизованого опрацювання інформації у формі наказу, розпорядження або іншого офіційного документа закріплено відповідні правила експлуатації, порядок і правила захисту інформації.

Отже, обраний законодавцем підхід до правового регулювання захисту комп'ютерної інформації, *головним чином, сприяє підвищенню ефективності заходів інформаційної безпеки у державному секторі.* Стимулюючи відповідальних осіб застосовувати засоби захисту інформації, норми чинного законодавства забезпечують урешті-решт значне зниження ймовірності посягання на державний інформаційний ресурс. Однак недержавні інформаційні системи, зокрема системи середнього та малого бізнесу, представляють сьогодні не менш значний інтерес для кіберзлочинців і причина такої привабливості саме в недостатності заходів інформаційної безпеки [2; 3; 4; 5]. Середній та малий бізнес активно використовує системи інтернет-банкінгу, працює над створенням потужних баз клієнтів, накопичує іншу інфор-

мацію, яка може бути використана для вчинення злочинів. У свою чергу, можливості використання ст. 363 КК у цьому сегменті є значно обмеженими через відсутність норм, які б зобов'язували власників інформаційних систем із недержавною інформацією застосовувати певні засоби захисту інформації. Можна сміливо стверджувати, що відсутність спеціального нормативного регулювання у сфері захисту недержавної інформації, – потенційно небезпечна зростанням показників комп'ютерної злочинності.

Цілком зрозуміло, що ефективним захист інформації буде за умови комплексного використання технічних, програмних та організаційних засобів. Очевидним є також і те, що ставити власникам недержавної інформації вимоги, подібні до передбачених щодо власників державної, - недоцільно. Незбалансовані нормативні вимоги інформаційної безпеки в недержавному секторі навряд чи сприятимуть розвиткові відносин інформатизації в країні, штучно обмежуватимуть розвиток перспективного ринку інформаційних послуг. Наприклад, надмірні вимоги до захисту інформації користувачів інтернету з необхідністю призведуть до необґрунтованого завищення цін на послуги інтернет-провайдерів. Тим не менше, проблема законодавчого стимулювання більш широкого використання засобів захисту недержавної інформації є наявною та потребує розв'язання.

Варто зазначити, що проблема правового стимулювання захисту недержаної комп'ютерної інформації може мати й інше розв'язання. *Можливо, збереження ст. 363 КК України є недоцільним?* А питання відповідальності за порушення порядку або правил захисту комп'ютерної інформації можна було б розглядати, наприклад, в адміністративно-правовій площині.

Відповідь можна сформулювати з використанням раціональної парадигми кримінального права. Застосування кримінального права є завжди видатковим. Причому видатки мають не лише матеріальний характер. Вони також виявляються й у криміналізації суспільства, певних демографічних та соціально-культурних наслідках. Тому оптимальний стан кримінального права, якого слід добиватися, визначається відповідністю реальних соціальних потреб та соціальних видатків на його реалізацію до значимості та захищеності охоронюваних благ [8, с. 3]. Такий стан досягається в тому числі й раціональним (економічним) підходом, який передбачає верифікацію кожного рішення з позицій балансу соціальних видатків і результатів.

У нашому випадку маємо норму, ст. 363 КК України, яка шляхом використання порівняно невеликих санкцій мала б забезпечувати попередження більш серйозних соціальних витрат. До останніх слід відносити: витрати потерпілих, зумовлені вчиненням щодо них злочинів у сфері використання комп'ютерної техніки, та витрати держави, зумовлені не-

обхідністю реалізації кримінальної відповідальності за ці злочини. У термінології раціональної парадигми кримінального права це можна сформулювати таким чином: використання кримінальної відповідальності за порушення правил або порядку захисту комп'ютерної інформації є обґрунтованим, оскільки шляхом порівняно невеликих соціальних витрат досягається більш вагомий соціальний результат – значне зменшення соціальних витрат шляхом попередження злочинів у сфері використання комп'ютерної техніки.

Наведений висновок підтверджується результатами спеціальних досліджень. Так, якщо у 2008 році щорічна шкода від кіберзлочинності у світі складала близько 100 млрд. доларів США[10], то за оцінками 2013 року цей показник наблизився до одного трильйона [6]. При цьому, за результатами моніторингового дослідження компанії Trustwave, у 2014 році 71 % жертв самостійно не ідентифіковували вторгнення до їх інформаційних систем (це відбувалося завдяки діяльності банківських установ або правоохоронних органів) у результаті середній період від початку вторгнення до його виявлення складав 87 днів, а від виявлення до нейтралізації – 7 днів. У випадках, коли завдяки використовуваним засобам інформаційної безпеки потерпілі компанії самостійно виявляли факт уторгнення, середній період від початку вторгнення до його виявлення складав 32 дні, а від виявлення до нейтралізації – 1 день[7]. Таким чином, за умови існування ризику значних соціальних витрат через кіберзлочинність, застосування ефективних засобів захисту комп'ютерної інформації здатне у 2-3 рази забезпечити зменшення збитків потерпілих від "комп'ютерних" злочинів та істотно зменшити відповідні витрати держави на забезпечення кримінально-правового регулювання.

Висновки:

1. У контексті підвищеної латентності злочинів у сфері використання комп'ютерної техніки, латентність злочинів, передбачених ст. 363 КК України, додатково зумовлюється вадами чинної нормативної регуляції захисту комп'ютерної інформації. Одним із напрямів удосконалення національного законодавства є створення нормативної бази для розвитку системи захисту недержавної інформації, яка б відповідала можливостям її власників і забезпечувала достатньо надійний захист відповідного сегмента національного інформаційного ресурсу.

2. Доцільним є збереження кримінальної відповідальності за порушення порядку або правил захисту комп'ютерної інформації. Наявність нормативних вимог щодо обов'язкового використання засобів захисту недержавної інформації дозволить більш раціонально використовувати потенціал досліджуваної норми для попередження "комп'ютерних" злочинів.

Використана література:

1. 2014 Trustwave Global Security Report [Electronic resource] // Trustwave Holdings, Inc. – Mode of access : https://www2.trustwave.com/GSR2014.html?utm_source=library&utm_medium=web&utm_campaign=GSR2014.

2. Baldor L. Cyber criminals targeting small businesses [Electronic resource] / Lolita C. Baldor // INVISUS. – Mode of access : http://www.invisus.com/pdf/ID_InfoSafe_Article02msnbc_112509_1%2000.pdf.

3. Big Threats for Small Businesses: Five Reasons Your Small or Midsize Business is a Prime Target for Cybercriminals [Electronic resource] // FireEye, Inc. – Mode of access : https://www2.fireeye.com/smb_five_reasons_wp.html.

4. Glynn F. Why Small Business is a Bigger Target for Cyber Criminals [Electronic resource] / Fergal Glynn // Thought Reach – Small Business Hub. – Mode of access : http://thoughtreach.com/why-small-business-target-for-cyber-criminals/.

5. Kuchler H. Cyber criminals target smaller companies [Electronic resource] / Hannah Kuchler // Financial Times. – 10.02.2014 – Mode of access : http://www.ft.com/cms/s/0/3bb5e5b2-901a-11e3-aee9-00144feab7de.html#axzz3Nx4yULbv.

6. Lewis A., Baker S. The Economic Impact of Cybercrime and Cyber Espionage. Report, July 2013 [Electronic resourse] / James Andrew Lewis, Stewart Baker // Center for Strategic and International Studies (CSIS). – Mode of access: http://csis.org/publication/economic-impact-cybercrime-and-cyber-espionage

7. Гриців М. І. Узагальнення судової практики розгляду справ про злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), автоматизованих систем та комп'ютерних мереж і мереж електрозв'язку / М. І. Гриців, В. В. Антощук [Електронний ресурс] // Офіційний сайт Верховного Суду України. – Режим доступу : http://www.scourt.gov.ua/.

8. Жалинский А. Э. Уголовное право в ожидании перемен: теоретико-инструментальный анализ / Альфред Эрнестович Жалинский. – М. : Проспект, 2008. – 400 с.

9. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : монографія / М. В. Карчевський ; МВС України, Луганський державний університет внутрішніх справ імені Е. О. Дідоренка. – Луганськ : РВВ ЛДУВС ім. Е. О. Дідоренка, 2012. – 528 с.

10. Киберпреступность страшнее финансового кризиса [Электронный ресурс] // Новости сайта Центра исследования компьютерной преступности. – 03.12.2008. – Режим доступа : http://www.crime-research.ru/news/03.12.2008/5056/.

11. Музика А. А. Законодавство про кримінальну відповідальність за "комп'ютерні" злочини: науково-практичний коментар і шляхи вдосконалення / А. А. Музика, Д. С. Азаров. – К. : Вид. Паливода А. В., 2005. – 118 с.

12. На долю общепита пришлось наибольшее количество проникновений в 2010 году [Электронный ресурс] // Хакер.ru. – 21.01.2011. – Режим доступа : https://хакер.ru/2011/01/21/54587/.