МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СУМСЬКИЙ ДЕРЖАВНИЙ УНІВЕРСИТЕТ
НАВЧАЛЬНО-НАУКОВИЙ ІНСТИТУТ ПРАВА

Правові горизонти

Legal horizons

ВИПУСК 11 (24)

Суми – 2018

DOI: http://www.doi.org/10.21272/legalhorizons.2018.i11.p49

ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ ДІЯЛЬНОСТІ СУБ'ЄКТІВ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ

Пахомов Володимир Васильович,
доктор юридичних наук, доцент,
завідувач кафедри кримінально-правових
дисциплін та судочинства,
Навчально-науковий інститут права,
Сумський державний університет

Кравченко Євгеній Володимирович,
Навчально-науковий інститут права,
Сумський державний університет

Дана стаття присвячена дослідженню організаційно-правових засад діяльності суб'єктів протидії кіберзлочинності як одного із небезпечних правопорушень. Особливу увагу приділено способам підготовки, роботи та протидії такому поняттю як кіберзлочин його запобігання та деякі аспекти боротьби з ним.

Сучасне суспільство обумовлює поширення кіберзлочинів у середовищі глобальних інформаційних мереж, які на даний час перетворилися в електронний аналог суспільного життя, так як все більша частина суспільства переходить на більш зручну для себе систему яка знаходиться в мережі кіберпростору, це є як дані одієї особи так і великих багатомільйонних компаній які зберігають свою інформацію в електронних ресурсах. Також хотілося зазначити, що дане питання є досить «розмитим», адже мало, що про нього є у науковій літературі та чинному законодавсті, запобігання цього злочину знаходиться на стадії постійного удосконалення, адже зовсім нещодавно в Кримінальний кодекс України було введено окремий розділ у особливій частині який за останні роки вносяться вагомі поправки для його вдосконалення.

Характеристика поняття кіберзлочинності, як окремого виду злочину в так званому «кібернетичному» або «електронному просторі», суть даного поняття від початку кіберзлочинів та по теперішній час.

Ключові слова: запобігання, протидія, кіберзлочинність, кіберполіція, нормативно-правова база, підрозділ.

Pakhomov V.V., Kravchenko Y.V. Organizational and legal principles of activity of actors of combating cybercrime. This article is devoted to the study of the organizational and legal foundations of the activities of actors to combat cybercrime as one of the most dangerous offenses. Particular attention is paid to the methods of preparation, work and counteraction to such a concept as cybercrime to prevent it and some aspects of the fight against it.

Modern society causes the spread of cybercrime in the global information networks environment, which has now become an electronic analogue of social life, as more and more of society goes to a more convenient system, which is located in the cyberspace network, it is like the data of one person and large multi-million dollar companies that store their information in electronic resources. I would also like to

point out that this issue is rather "blurred", because there is little that is about it in scientific literature and current legislation, prevention of this crime is at a stage of continuous improvement, since most recently the Criminal Code of Ukraine introduced a separate section in a special part which in recent years made significant adjustments for its improvement.

Characteristics of the concept of cybercrime as a separate type of crime in the so-called "cybernetic" or "electronic space", the essence of this concept from the beginning of cybercrime and to date.

Keywords: prevention, counteraction, cybercrime, cyberpolice, normative-legal base, subdivision.

Актуальність дослідження: полягає у відсутності чіткої та злагодженої системи заходів для вчасного виявлення протидії незаконним діянням в сфері кіберпростору, що можуть бути пов'язані з різними діями у галузі кіберзлочинності в Україні. Викладення даного виду злочину поряд з його значною шорокою дією стали безсумнівно істотними перевагами у порівнянні з іншими злочинами, скоєння яких в умовах покращання правоохоронних систем стає все вартіснішим й важчим. Таким чином, проведення дослідження щодо основних схем та засобів злочинів отриманих у сфері кіберзлочинності, на сьогодні є актуальним та необхідним. Так як основними способами протидії кіберзлочинності можуть виступати: вдосконалення норм і прав боротьби з кіберзлочинністю, чітке розмежування компетенції та функцій правоохоронних органів.

Стан дослідження проблеми: цій проблематиці присвячені праці, зокрема, Гавловського Д., Карчерського М., Маркова В., Цимбалюка, Л., Скалозуба Л. та ін. Незважаючи на досить велику кількість публікацій, а також враховуючи останні зміни, що відбулися в законодавстві з даної проблематики, питання удосконалення сучасних напрямів протидії кіберзлочинам в Україні потребують додаткового розгляду.

Основна мета: формування ефективної системи заходів протидії та боротьби з кіберзлочинністю в Україні.

Виклад основного матеріалу. Проблема пошуку шляхів протидії злочинам з уживанням інформаційнокомунікаційних систем уже доволі тривалий час знаходиться у центрі уваги як міжнародної спільноти, так й державних органів України зокрема. Беручи до уваги той факт, що піднесення технологій проходить швидше ніж приймаються нормативно-правові акти, котрими вони регулюються, а об'єми незаконно отриманих коштів кіберзлочинцями зростають, потрібно на сталій основі віднаходити шляхи вирішення нових проблем, пов'язаних з такими галузями, як транскордонний доступ правоохоронних служб до даних, захист даних та обмін інформацією між приватними та державними структурами [1,с.16-18].

За даними проведених досліджень, кіберзлочинність - це п'ятий за розмірами вид економічної злочинності в Україні після незаконного привласнення майна, корупції та хабарництва, недобросовісної конкуренції та маніпуляції з фінансовою звітністю. Тому і не дивно, що в грудні місяці 2011 року був створений Департамент по боротьбі з кіберзлочинністю МВС, саме даний орган є фундаментом протидії з кіберзлочинами і основним способом протидії кіберзлочинності є покращення досвіду працівників даного підрозділу [3,с.56-62].

Організація протидії цьому виду злочинності в Україні складалася тривалий час не досить ефективно, що, в першу чергу, пов'язувалось з відсутністю необхідної законодавчої бази.

Тому можна констатувати той факт, що раніше, зазвичай, не приділялося достатньої уваги цьому виду суспільно небезпечних злочинних діянь. І лише після того, коли, наприклад, матеріальні збитки від незаконних діянь досягли таких розмірів, що стали різко виділятися на загальному рівні збитків від загально кримінальної злочинності, прийшов час, коли на цьому новому злочинному явищі зосереджено увагу, зроблено акцент [6].

З огляду на те, що кібератаки значно почастішали, українська влада вирішила посилити механізми захисту державних комп'ютерних систем. 15 березня 2016 року Президент видав Указ «Про введення в дію рішення Ради національної безпеки та оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України. В складі Ради національної безпеки створено робочий орган - Національний координаційний центр кібербезпеки [7]. Поява цього органу цілком обґрунтована, адже поруч з перевагами інформаційних технологій, їх активно використовують для «здійснення терористичних актів, в тому числі шляхом порушення штатних режимів автоматизованих систем управління технологічним процесами на об'єктах інфраструктури [2,с.324].

В нашій державі нормативно-правову базу правового регулювання в даній сфері складають Конституція України, Кримінальний кодекс України, Конвенція Ради Європи «Про

кіберзлочинність», Закони України «Про основи національної безпеки України», «Про захист інформації в інформаційно-телекомунікаційних системах» тощо, Укази Президента України від 08 липня 2009 року № 514/2009, від 08 червня 2012 року № 389/2012, № 390/2012, інші нормативно-правові акти [10,с.124-128].

Особливу увагу потрібно надати такому питанню як Кримінальний кодекс України, саме йому, адже коли на даний час проблема кіберзлочинності досягла неабияких масштабів, то в кримінальний кодекс був введений розділ XVI який отримав назву "Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку", та вже встиг близько двох разів побувати в редакції із змінами та доповненнями, що свідчить про те як дане питання постійно формується та удосконалюється [8,с.327]. На даний час розділ особливої частини містить шість статей:

Стаття 361. Несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку

Стаття 361- 1 . Створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут

Стаття 361- 2 . Несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації

Стаття 362. Несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї

Стаття 363. Порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється

Стаття 363- 1 . Перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку Відсутність чіткого визначення комп'ютерної злочинності, єдиного розуміння сутності цього явища значно ускладнюють визначення завдань правозастосовних органів у виробленні єдиної стратегії боротьби з нею [5].

Для боротьби із різними типами кіберзлочинів у 2007 році в Україні був створений CERT-UA (Computer Emergency Response Team of Ukraine - команда реагування на комп'ютерні надзвичайні події України) - спеціалізований структурний підрозділ Державного центру захисту інформаційно-телекомунікаційних систем Державної служби спеціального зв'язку та захисту інформації України (Держспецзв'язку). CERT-UA з 2009 року була акредитована у FIRST (Forum for Incident Response and Security Teams - Форум команд реагування на інциденти інформаційної безпеки) та вже протягом 5 років є його повноправним членом [3,с.56-62]. Слід зазначити, що членство у FIRST, в рамках протидії кібернетичним загрозам на міжнародному рівні, надає можливість оперативно взаємодіяти з 284 командами реагування на комп'ютерні інциденти (CERT) з 61 країни світу [11.с.33-34].

Для боротьби із кіберзлочинністю в Україні так і інших країнах світу швидко усвідомили той факт, що з приходом суспільства на електронну систему всіх своїх даних це може стати як позитивних так і негативних даних. Це зовсім не дивно, адже більшість нашої країни передбачають зберігати власні дані в електронному вигляді, так як це є досить зручно. На сам перед це досить зручно розраховуватися однією «карткою» чи тримати всі особисті дані в комп'ютері, але не слід забувати, що для зловмисників це спосіб незаконно користуватися вашими даними, будь-яка операція від несанкціонованого втручання в роботу вашого комп'ютера до інших більш традиційних злочинів, насам перед це є шахрайство, підробка, привласнення чужих данних.

Щодо протидії і запобігання кіберзлочинів, то цю роль відіграє кіберполіція, потік фахівців та експертів здатних застосовувати на високому професійному рівні новітні технології.

До основних завдань кіберполіції відносять:

1. Реалізація державної політики у сфері протидії кіберзлочинності.

2. Протидія кіберзлочинам:

3. Завчасне інформування населення про появу новітніх кіберзлочинів.

4. Впровадження програмних засобів для систематизації та аналізу інформації про кіберінциденти, кіберзагрози та кіберзлочини.

5. Реагування на запити закордонних партнерів, що надходитимуть каналами Національної цілодобової мережі контактних пунктів.

6. Участь у підвищенні кваліфікації працівників поліції щодо застосування комп'ютерних технологій у протидії злочинності.

7. Участь у міжнародних операціях та співпраця в режимі реального часу [12,ст.2535].

Кіберзлочини в науковій літературі класифікуються як правило на два види, це традиційні злочини, що вчиняються за допомогою комп'ютерних технологій та Інтернету(шахрайство з використанням ЕОМ, незаконне збирання відомостей, що становлять комерційну таємницю, шляхом несанкціонованого доступу до комп'ютерної інформації і т.д.), та нові злочини, які утворилися в наслідок нових інформаційних технологій. Повертаючися до вищесказаного хотілося б зазначити, що як правило найчастіше з використанням Інтернету вчиняються такі традиційні злочини: порушення авторського права і суміжних прав(ст. 176); шахрайство (ст. 190); незаконні дії з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, обладнанням для їх виготовлення (ст. 200); незаконне збирання з метою використання або використання відомостей, що становлять комерційну або банківську таємницю (ст. 231) [5].

Кроки у справі по захисту від кіберзагроз Україна робить не тільки створенням управлінням боротьби з кіберзлочинністю а й розробкою законодавчих актів, прикладом можна навести затверджені закони України "Про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки" та "Про захист персональних даних", розглянуто в другому читанні та прийнято в цілому Закон України "Про документи, що посвідчують особу та підтверджують громадянство України", який, однак, був заветований Президентом України через значні невідповідності до Конституції України та певних міжнародних стандартів. Також ініційовано і прийнято низку державних програм, що закріплюють як пріоритетний напрям державної політики упровадження інформаційних технологій 3 у сферу державного управління та побудову інформаційного суспільства. Держава планує збільшити кількість бюджетних місць для ІТ-спеціалістів у ВНЗ, так як спеціалістів і фахівців потрібно готувати вже зараз, щоб вони вже змогти оцінити масштаби даної небезпеки і вносити перспективи щодо усуненню її в майбутньому, освоїти дане питання, тому що ІТ-галузь зростає щорічно на 40 % і забезпечує майже 3 % ВВП, і при цьому держзамовлення у вишах скорочується на 20 % [10.с.124-128].

У ведучих, економічно розвинених країнах рівень втрат від кіберзлочинності вимірюється кількісно тисячами, а економічні збитки складають мільярди доларів США. За оцінками Інтерполу тільки в Європі збиток від дій кіберзлочинців щорічно складає 750 мільярдів євро [11,с.33-34]. Втрати США від кіберзлочинності складають від 20 до $ 140 млрд. доларів, або близько 1% від ВВП країни, а в Латинській Америці фінансові втрати від діяльності кіберзлочинців в 2013 склали 1,1 млрд. доларів. Такі дані опублікувала неурядова організація LACNIC, що займається аналізом Інтернет - активності в регіоні [13,с.173-179].

Тому й не дивно, що таке питання як кіберзлочинність потрібно удосконалювати і вивчати всі його аспекти у повній мірі, адже це одна з головних і першочергових проблем нашого часу, якщо не головна, бо для сучасного громадянина електронні операції стають все більш частіші та повсякденні у своєму використанні. І саме питання кіберзлочинів потрібно проштовхувати вперед для більш якісного виконання, вдосконалення та прийняття рішучих законопроектів, готування провідних спеціалістів для протидії даного виду злочину на даному етапі та запобігання його у майбутньому.

Висновок. Злочини у сфері кіберзлочинності - це перш за все передбачене кримінальним законом винне порушення прав та інтересів стосовно автоматизованих систем обробки даних, що зашкоджує правовій охороні прав та інтересів фізичних і юридичних осіб, суспільства та держави. Таким чином це діяння, суть якого міститься зовсім не у використанні самої електронно-обчислювальної техніки як такого засобу для скоєння злочину. Цей вид злочинності включає суспільнонебезпечні дії, які посягають на безпеку інформації та автоматизовані системи її обробки, та на самих громадян які можуть стати потерпілими. І саме для протидії даного злочину в нашій державі функціонують відповідні вищесказані органи які знешкоджують та запобігають такому виду як кіберзлочин.

Наслідки неправомірного використання особистої інформації можуть бути різним, насам перед це не тільки порушення недоторканності інтелектуальної власності, але й розголошення відомостей про приватне життя громадян, втручання в особистий простір, майнова шкода у вигляді прямих збитків та неотриманих доходів, фінансові операції з використанням особистих даних особи та інші методи шахрайства, пошкоджена репутація компанії, різноманітні види порушень нормальної діяльності підприємства, галузі і т. ін.

Під суб'єктами забезпечення кібернетичної безпеки у проекті Стратегії забезпечення кібернетичної безпеки України було визначено державні органи, органи місцевого самоврядування, установи, організації, підприємства незалежно від форми власності, які здійснюють проектування, впровадження та експлуатацію складових критичних об'єктів

національної інформаційної інфраструктури або забезпечують їх кіберзахист.

Література:

1. Бутузов В. М. Співвідношення понять «комп'ютерна злочинність» і «кіберзлочинність» / В. М. Бутузов // Інформаційна безпека людини, суспільства, держави. – 2014. – № 1(3). – С. 16-18.

2. Бандурка О.М. Інтерпол: Міжнародна організація кримінальної поліції: науково-практичний посібник. – Х.: Основа, 2003. - 324 с.

3. VII регіональної міжвузівської студенської науково-практичної конф., «Проблеми Укр. суспільства: кіберзлочинність» м. Рівне 2017. //56-62. ресурс:http://prog-rdak.16mb.com/wp content/uploads/2017/04/kiberzlochunu.pdf

4. Курс кримінології: Загальна частина: Підручник / О.М. Джужа, П.П. Михайленко, О.Г. Кулик та ін.; За заг. ред. О.М. Джужи. – К.: Юрінком Інтер, 2001. – 352 с.

5. Катеринчук Іван Петрович наукова робота Правоохоронні органи в боротьбі з кіберзлочинністю Одеський державний університет внутрішніх справ «Кібербезпека в Україні: правові та організаційні питання» ресурс: http://oduvs.edu.ua/wpcontent/uploads/2017/01/Katerinchuk_I.P._Pravookhranitelniye_organy_v_borbe_s_kiberprestupnostyu.-5-7.pdf

6. Карий В.В. наукова стаття «правові та організаційні засади розслідування злочинів з використанням телекомікаційних мереж України» ресурс: http://dspace.tneu.edu.ua/bitstream/316497/24254/1/170.PDF.

7. Про рішення Ради національної безпеки та оборони України від 27 січня 2016 року "Про Стратегії кібербезпеки України" Президент України, Рішення від 15.03.2016 № 96/2016 діє з 18.03.2016р.

8. Карчевський М. В. Кримінально-правова охорона інформаційної безпеки України : [моногр.] / Карчевський М. В. – Луганськ : Луган. держ. ун-т внутр. справ, 2012. – 327 с.

9. Кримінальний кодекс України [Електронний ресурс] / Офіційний сайт Верховної Ради України. – Режим доступу: http:// zakon1.rada.gov.ua

10. Шавиркін Б. В. Деякі особливості розслідування кіберзлочинів / Б. В. Шавиркін // Боротьба з інтернет-злочинністю : матеріали міжнар. наук.-практ. конф. (Донецьк, 12–13 черв. 2013 р.). – Донецьк : Донец. юрид. ін-т, 2013. – С. 124-128

11.Пфо, О. М. Основні поняття і класифікація кіберзлочинності / О. М. Пфо // Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016 р. — Кропивницький : КНТУ, 2016. — С. 33-34.

12.Конвенція про кіберзлочинність від 23.11.2001 р. // Офіційний вісник України від 10.09.2007 — 2007 р., — № 65. — стор. 107. — стаття 2535.

13.Міщук Н. Кіберзлочинність як загроза інформаційному суспільству / Н. Мыщук // Вісник Львівського університету. Серія економічна. — 2014. — Випуск 51. — С. 173-179

14. Ліпкан В. А. Інформаційна безпека України в умовах євроінтеграції : навч. посіб. / В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський. – Київ : КНТ, 2006. – 280 с. – (Серія: Нац. і міжнар. безпека).