УДК 343.1
DOI https://doi.org/10.32782/2524-0374/2021-1/59

ОПТИМІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРШАХРАЙСТВОМ: ЗАРУБІЖНИЙ ДОСВІД І ЙОГО ЗНАЧУЩІСТЬ В УКРАЇНСЬКІЙ ПРАКТИЦІ

OPTIMIZATION OF LEGAL REGULATION OF THE FIGHT AGAINST CYBER FRAUD: FOREIGN EXPERIENCE AND ITS SIGNIFICANCE IN UKRAINIAN PRACTICE

Лугіна Н.А., к.ю.н., доцент,
доцент кафедри кримінального права та кримінології
Університет державної фіскальної служби України

Лучук А.М., студентка ІІ курсу
Навчально-науковий інститут права
Університету державної фіскальної служби України

Дана стаття присвячена висвітленню актуальної проблеми сучасності – кібершахрайству, а саме його запобіганню, для якого доцільно використовувати досвід країн, які першими постраждали від даного явища та зуміли налагодити процес правового регулювання даного питання.

Також у статті висвітлено актуальні методи боротьби з кібершахрайством у країні, що як і Україна була у складі СРСР, та також зіткнулася з значною кількістю кримінальних правопорушень, вчинених у віртуальному просторі.

Варто додати, що кібершахрайство є досить новітнім явищем, адже безпосередньо пов'язане з розвитком новітніх інформаційних технологій, вимагає від правопорушників відповідних навичок, але попри те вчиняти такі злодіяння може майже кожна особа, що має вільний доступ до мережі Інтернет. Важливим аспектом цієї статті є характеристика кібершахрайства як дійсно небезпечного виду кримінальних правопорушень, адже саме через нього щодня люди встрачають свої кошти, їх особиста інформація стає незаконно доступною для кола осіб, які можуть її використовувати у своїх цілях.

Звернено увагу й на те, що законодавча система України не закріплює жодного виду кримінальних правопорушень з приставкою «кібер», тим самим не надаючи їм особливої небезпечності. Доволі розповсюдженним є явище «недооцінювання» таких кримінальних правопорушень, адже через те, що люди не можуть побачити своїх збитків, помилково вважають, що їх немає. Проте, саме неоціювання таких кримінальних правопорушень є чи не найпершою причиною їх розвитку.

Кібершахрайство вже давно набуло транснаціонального характеру, через що стало ще більш небезпечним явищем, адже кібершахраям необов'язково бути знайомими особисто, жити в одному місті, тощо. Безмежний простір мережі дає можливість зв'язуватися між собою з різних куточків світу, а також завдавати збитків людині чи компанії, яка також може бути розташована у будь-якому місті чи країні.

Ключові слова: кібершахрайство, запобігання кібершахрайству, зарубіжний досвід у боротьбі з кібершахрайством, вдосконалення законодавчої бази для боротьби з кібершахрайством.

This article is devoted to highlighting the current problem of modernity – cyber fraud, namely its prevention, for which it is advisable to use the experience of countries that first suffered from this phenomenon and managed to establish a process of legal regulation of this issue.

The article also highlights current methods of combating cyber fraud in a country that, like Ukraine, was part of the USSR, and also faced a significant number of criminal offenses committed in cyberspace.

It should be added that cyber fraud is a fairly new phenomenon, as it is directly related to the development of new information technologies, requires offenders to have the appropriate skills, but nevertheless such crimes can be committed by almost anyone with free access to the Internet. An important aspect of this article is the characterization of cyber fraud as a really dangerous type of criminal offense, because it is because of it that people lose their money every day, their personal information becomes illegally available to people who can use it for their own purposes.

Attention is also drawn to the fact that the legislative system of Ukraine does not enshrine any type of criminal offense with the prefix "cyber", thus not giving them much danger. The phenomenon of "underestimation" of such criminal offenses is quite common, because due to the fact that people cannot see their losses, they mistakenly believe that they do not exist. However, the very non-assessment of such criminal offenses is perhaps the first reason for their development.

Cyber fraud has long been transnational in nature, making it even more dangerous, as cyber-fraudsters do not have to know each other personally, live in the same city, and so on. The boundless space of the network makes it possible to communicate with each other from different parts of the world, as well as to cause harm to a person or company, which can also be located in any city or country.

Key words: cyber fraud, prevention of cyber fraud, foreign experience in combating cyber fraud, improvement of the legal framework for combating cyber fraud.

На сучасному етапі розвитку суспільства дедалі більше відчувається значущість інноваційних процесів, що відбуваються в нашому суспільстві у зв'язку з глобальною інформатизацією, але разом із позитивними досягненнями, інформатизація супроводжується й іншими явищами негативного характеру, до яких відносять кібершахрайство. Це, очевидно, вимагає негайного створення системи протидії даному різновиду злочинності на державному рівні. Для сучасного суспільства актуальність цієї проблеми є беззаперечною. Оцінки експертів вказують на те, що щорічно збитки від діяльності кібершахраїв складають близько від 300 до 800 млрд євро [1, с. 144–149].

Державні підходи та механізми повинні сприяти поліпшенню національної безпеки та міжнародному правопорядку, а також скороченню кримінальних правопорушень у кіберпросторі.

В Україні процес боротьби з кібершахрайством ускладнений тим, що самого терміну «кібершахрайство» в законодавстві не визначено, навіть не звертаючи уваги на те, що поняття є не новим як для правоохоронних органів України, так і для зарубіжних держав. На сьогодні інформаційні технології застосовуються практично в усіх сферах суспільного життя, та навіть в економіці держави, що дає змогу висувати проблему боротьби з кібершахрайством у число основних.

Окрім того, що може наноситись безпосередня шкода від неавторизованого доступу до інформації, або її розповсюдження чи модифікації, то кібершахрайство може бути джерелом загрози національній безпеці, економіці та інтересам людини. Проблемою є й те, що загроза таких діянь є не до кінця усвідомленою, причиною цьому є те, що відсутня наукова розробленість фундаментальних понять, що пов'язані з нею.

Інтернет є місцем, у якому вчинити кримінальні правопорушення дуже легко, адже існує анонімність та необмеженість мережі, яку можна використовувати у своїх протиправних діях.

Жодні терміни із частиною «кібер» ще досі не отримали сформованого визначення ані на науковому, ані на нормативно-правовому рівнях, через що залишаються предметом дискусій.

На даному етапі поняття «боротьба з кібершахрайством» є новим для вітчизняної навіки, навіть попри те, що протиправні діяння із застосуванням Всесвітньої павутини мають високий рівень суспільної небезпеки.

Отже, відсутність належного законодавчого закріплення поняття «боротьба з кібезлочинністю» є однією із причин наявності проблем у його повному розумінні та науковому тлумаченні.

Щодо боротьби із кібершахрайством в Україні, за загальним правилом вона здійснюється Департаментом кіберполіції, законодавством та іншими суб'єктами, що зацікавлені у подоланні даного явища. У свою чергу держава здійснює свою діяльність у законодавчому та організаційному напрямах, а Департамент кіберполіції у профілактичному.

Основним аспектом встановлення даного терміну є рівень небезпеки, який характеризує вчинене діяння. Але саме поняття «кібершахрайство» не дає зрозуміти масштаб небезпечності дії та середовища її вчинення. Доцільно розглядати кібершахрайство як специфічний вид протиправної діяльності, що здійснюється у комп'ютерних мережах.

Важливо звернути увагу й на те, що не можна ототожнювати кібершахрайство та інформаційні кримінальні правопорушення. Оскільки в нашій державі кібершахрайство існує у вигляді потенційної загрози, то важливим є впровадження попереджувальних заходів. Це все є поштовхом для створення ефективної системи запобігання та виявлення такої діяльності, що буде базою для успішною боротьби з кібершахрайством в Україні [2, с. 338–342].

Загалом протидія кібершахрайству має включати в себе загальнодержавні заходи економічного, виховного, політичного характеру, а також комплекс вузько спрямованих заходів, направлених на безпосереднє подолання протиправних діянь. Оскільки злодіяння у кіберпросторі мають міжнародний характер, то й боротьба з ними вимагає гармонізації національних законодавств.

Така гармонізація повинна відповідати регіональним вимогам та можливостям. Глобальна програма кібербезпеки базується на п'ятьох принципах:

1) правові заходи;
2) технічні й процедурні заходи;
3) організаційні структури;
4) створення потенціалу;
5) міжнародна співпраця;

Для дієвої протидії з кібершахрайством усі ці принципи повинні бути врахованими. Найважливішим принципом є перший, який передбачає запровадження певних правових заходів. Дані заходи вимагають прийняття основних положень кримінального законодавства, що передбачатимуть кримінальну відповідальність за такі дії, як кібершахрайство, неавторизований доступ до інформації, її пошкодження, порушення авторських прав тощо. Інструменти, необхідні для розслідування протиправних діянь у кіберпросторі, можуть істотно відрізнятися від тих, які використовуються при розслідуванні «традиційних» кримінальних правопорушень.

У зв'язку з міжнародним масштабом кібершахрайства необхідно вдосконалювати основи національного законодавства, зокрема й для того, щоб мати можливість співпрацювати з правоохоронними органами за кордоном. Для того, щоб боротьба з кібершахрайством була ефективною, на належному рівні має бути розвинена організаційна структура, адже не маючи належної системи відповідних органів, яка чітко розподіляє повноваження, навряд чи можна чекати на комплексне вирішення юридичних, технічних та соціальних аспектів цієї проблеми.

Для того, аби мати змогу ефективно розслідувати кримінальні правопорушення пов'язані з віртуальним простором, необхідною є не тільки гармонізація законодавства, а й розробка відповідних механізмів співпраці. Тому, надзвичайним аспектом є рівень довіри, який має бути не тільки між державами, ай між громадянином та державою.

Одним з головних і найперших елементів в попередженні кібершахрайства є обізнаність користувачів платформи Інтернет у її функціонуванні та дотримання усіх вимог безпеки: встановлення паролів, використання спеціальних символів тощо.

Оскільки ми вже згадували про те, що кібершахрайство є транснаціональним явищем, то йому характерний максимальний рівень латентності. Головними факторами латентності кібершахраїв є:

1) таємниця процесу вчинення протиправних діянь, що поєднується з різними сферами та наслідками їх вчинення, а також «комп'ютерна необізнаність» переважної більшості жертв кібершахраїв, їх нехтування своєю безпекою;

2) байдужа поведінка жертв та/або свідків кримінального правопорушення – не звернення жертви та осіб, яким відомо про кримінальне правопорушення, до правоохоронних органів;

3) недоліки в діяльності правоохоронних органів щодо реагування на звернення та повідомлення про кібершайхства [3, с. 193–199].

Запобігання кібершахрайству на загально-соціальному рівні передбачає перелік дієвих соціально-економічних, організаційно-управлінських, ідеологічних, культурно-виховних та інших заходів, спрямованих на вирішення важливих соціальних проблем та суперечок в країні.

Сама реалізація загально-соціальних заходів запобіганню кібершахрайству дає змогу мінімізувати випадки вчинення кримінальних правопорушень цього виду, а також запобігати формуванню особистості правопорушника.

Для належної розробки відповідних заходів протидії кібершахрайству, необхідним аспектом є організація діяльності правоохоронних органів, а також вищих органів держави, що відповідає вимогам, які мають існувати у правовій, незалежній, демократичній державі. Потрібно усувати фактори, що несуть позитивний вплив на існування та розвиток злочинності.

У свою чергу, спеціально-кримінологічне запобігання безпосередньо стосується роботи Національної поліції України та спрямовуються переважно на соціальні групи, що привертають увагу учасників запобіжної діяльності. Основними заходами запобігання кібершахрайству, які повинна реалізовувати Національна поліція (в особі департаменту кіберполіції), слід виділяти такі:

1) розроблення та затвердження Стратегії МВС щодо протидії кібершахрайству, яка у свою чергу повинна містити концепцію кримінально-запобіжної діяльності, а також заходи анти кримінального впливу та моніторингові механізми його забезпечення;

2) збільшення кількості планових та позапланових перевірок названими органами поліції підприємств, установ, організацій, робота яких має зв'язок з використанням комп'ютерних технологій або надання інформаційних послуг;

3) посилення відповідальності уповноважених осіб, які за своїми посадовими або функціональними обов'язками відповідають за безпечне функціонування комп'ютерів та комп'ютерних мереж;

4) встановлення жорсткого нагляду за обігом технічних засобів, які є забороненими у вільному використанні, наприклад, технічні засоби для негласного знаття інформації з каналів зв'язку, перехоплення інформації, добору паролів, тощо;

5) впровадження позитивного досвіду діяльності правоохоронних органів інших країн у даній сфері (перш за все для аналізу технічного забезпечення та технології, які

використовуються для запобігання вчиненню таких кримінальних правопорушень);

б) участь працівників кіберполіції ц міжнародних семінарах, круглих столах, проведення яких присвячено вказаній проблемі, а також ініціювання відповідними органами нашої держави проведення таких заходів на території України.

Важливим елементом діяльності щодо протидії вчиненню кібершахрайств є виявлення осіб, що вчиняють дані протиправні діяння, або ж схильні до вчинення таких злодіянь. Ключовим показником того, що особа схильна до таких діянь є системний перезапис даних без наявної необхідності, їх заміна або видалення, поява фальшивих записів, а також випадки, коли працівник безпричинно починає працювати понад нормою. Окремим заходом запобігання вчиненню кібершахрайств є виявлення діяльності кібертерористів, осіб, що використовують комп'ютери для вчинення терористичних актів [4, с. 295–307].

Увесь масштаб Інтернету вказує на те, що певні аспекти кібершахрайства не обмежуються територією певної країни, тому законодавство на міжнародному рівні має регулювати дане питання, відповідати загальновизнаним стандартам, аби його діяльність була ефективною.

Більше того, процес становлення злагодженої системи правового регулювання боротьби з кібершахрайством неможливий без урахування досягнень до недоліків, що були надбані іноземними державами при формуванні даного інституту.

У зв'язку з активним розвитком кібершахрайства, запобігання йому має бути актуальним завданням для держави. Проте, у багатьох зарубіжних країнах дана система вже давно налагоджена та приносить свої позитивні результати. Тому, проаналізувавши сучасні вітчизняні реалії, ми можемо відзначити незавершеність даного процесу в Україні та необхідність подальших трансформацій.

Розпочнемо з досвіду Сполучених Штатів Америки, як держави, яка потерпіла чимало атак від кібершахраїв і є чи не найпершою в історії, що розробляла відповідні норми для регулювання злодіянь даного типу. Головними нормами Національної стратегії національної безпеки США, прийнятої у 2015 році, є ті, що встановлюють необхідність захисту від кібератак у кіберпросторі. Сполучені Штати Америки, які проголосили себе батьківщиною Інтернету, взяли на себе відповідальність забезпечення кібербезпеки у всьому Інтернет-світі. Крім того, було проголошено курс щодо оптимізації законодавчої бази та підвищення її стандартів захисту прав та інтересів громадян [5, с. 45–46].

Таким чином Сполучені Штати Америки є однією з провідних країн-дослідників у галузі досвіду. Оскільки у цій країні триває активна діяльність з протидії таким негативним явищам, таким як кримінальні правопорушення у віртуальному просторі, зокрема кібершахрайству, то багато уваги приділено безпеці громадян. США можна назвати головною мішенню кібершахраїв, тому досвід саме цієї країни надзвичайно корисний для розробки правових інструментів протидії даному явищу. Незважаючи на все вищезазначене, в США переважає методика саморегуляції Інтернету, як результат законодавство в цій галузі представлено лице кількома нормативно-правовими актами.

Зокрема, це Закон про електронний підпис, що прийнятий у 2000 р. Основною його метою є забезпечення правового регулювання використання електронного підпису в комерційних відносинах. Найбільша кількість нормативно-правових актів діє у сфері випуску цінних паперів, захисту інтелектуальної власності, а також від неавторизованого доступу до інформації, авторських прав, тощо. До прикладу, у США кримінальна відповідальність за неналежне зберігання, обробку, знищення особистої інформації, у формі, що непередбачена законодавством. Для порівняння, у країнах Європейського Союзу кримінальні справи порушуються лише у випадку шкоди безпеці держави або основним правам громадян, що вказує на те, що соціальний аспект правового регулювання боротьби з кібершахрайством має велике значення [6, с. 126-128].

Цікаво також звернути увагу на досвід регулювання такої проблеми у країні, яка як і наша входила до колишнього СРСР, у якій було створено спеціальний орган для боротьби з кримінальними правопорушення у віртуальному просторі Міністерства внутрішніх справ Республіки Білорусь. 27 лютого 2001 р. у структурі кримінальної поліції МВС з'явилося управління оперативно-організаційної діяльності, у складі якого до листопада 2002 р. діяло відділення по розкриттю кримінальних правопорушень у сфері новітніх інформаційних технологій.

Даний орган має статус самостійного оперативно-розшукового підрозділу Міністерства, яке здійснює координацію підрозділів головного управління кримінальної поліції МВС і органів внутрішніх справ при виявленні ними злочинів проти інформаційної безпеки Для здійснення взаємодії з іншими правоохоронними органами і організаціями застосовується умовне найменування Управління «К» МВС Республіки Білорусь [7, с. 164–166].

Загалом законодавча боротьба з кримінальними правопорушеннями у сфері високих технологій представлена невеликою кількістю норм та законів: Глава Кримінального кодексу Республіки Білорусь, Закон про електрозв'язок, закон про інформацію, інформатизацію і захист інформації, Конвенція про кіберзлочини, Додатковий протокол до Конвенції про кіберзлочини, Указ «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», Указ «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність». Загалом варто відзначити схожість законодавчої основи Республіки Білорусь та України, проте особливим є Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність» [8, с. 78–82].

Проаналізувавши правове регулювання боротьби з кібершахрайством, можна стверджувати про спроби встановлення контролю за Всесвітньою мережею, проте важливим аспектом є те, що наявні заборони не містять порушення прав та свобод людини і громадянина. У досліджуваних країнах існує взаємозв'язок між державою та суспільством, який позитивно впливає на розуміння суспільством проблем і необхідністю встановлення меж для їх вирішення.

Доцільно відзначити й роль міжнародного законодавства та міждержавних угод, що мають значний вплив на відносини громадян у різних державах. Це ще раз вказує на те, що їх роль у вітчизняному праві необхідно оптимізувати до вищого рівня.

ЛІТЕРАТУРА

1. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. *Публічне право.* 2015. № 3 (19). С. 144–149.

2. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. *Теоретичні та прикладні питання економіки.* МОНУ. КНУ імені Тараса Шевченка; Ін-т конкурентного суспільства. Київ, 2009. Вип. 19. С. 338–342.

3. Сервецький І.В. Деякі проблеми захисту персональних даних в Україні *Боротьба з організованою злочинністю і корупцією (теорія і практика).* К. МНДЦ, 2014. № 9. С. 193–199.

4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування. Аналітична записка. URL: http://www.niss.gov.ua/articles/454 (дата звернення 18.01.2021).
5. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 45–46.
6. Солодка О.М. Боротьба з комп'ютерною злочинністю як пріоритетний напрям забезпечення інформаційної безпеки України. *Актуальні проблеми управління інформаційною безпекою держави: зб. Матеріалів наук.-практ. конф*., 17 берез. 2010 р., м. Київ. Київ : Нац. акад. СБУ України, 2010. С. 126–128.
7. Якубівська Ю.Є. Кібератаки у сфері інформаційної безпеки: тенденції на євразійському просторі. *Вітчизняна система охорони і захисту інтелектуальної власності в умовах приєднання до Європейського Союзу: Збірник тез доповідей Всеукраїнської науково-практичної конференції*, м. Тернопіль, 24–25 квітня 2015 р., ТНЕУ. Тернопіль, 2015. С. 164–166.
8. Тихомиров О.О. Протидія кіберзлочинності як складова державного забезпечення інформаційної безпеки. *Актуальні проблеми управління інформаційною безпекою держави : зб. Мат. НПК*, (Київ, 22 берез. 2011 р.). Ч. 2. Київ : Вид-во НА СБ України, 2011. С. 78–82.