УДК 343.1
DOI https://doi.org/10.37687/2413-6433.2022-1-2.11

Лугіна Н. А.,
кандидат юридичних наук, доцент,
доцент кафедри кримінальної юстиції
Державного податкового університету
ORCID: 0000-0001-6005-2943

ПЕРСПЕКТИВИ ТА ТЕНДЕНЦІЇ РОЗВИТКУ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ В УКРАЇНІ

PROSPECTS AND TRENDS OF THE DEVELOPMENT OF LEGAL REGULATION OF FIGHTING CYBERCRIME IN UKRAINE

Сьогодні важко сперечатися щодо питання важливості мережі Інтернет у нашому житті. Інтернет відкриває перспективи для саморозвитку, отримання нових знань, пошуку роботи тощо. Цей ресурс ми використовуємо щодня, навіть свій вільний час можемо проводити на його просторах. Але, пропри це, Інтернет має й іншу сторону, ту, в якій щодня, щогодини вчиняються кримінальні правопорушення, адже платформа забезпечує користувачів повною анонімністю та не обмежує їх у своїх діях. До прикладу, у 2018 році в Україні працівники Департаменту кіберполіції Національної поліції України були залучені до більше ніж одинадцяти тисяч кримінальних проваджень, пов'язаних з кримінальними правопорушеннями у сфері новітніх інформаційних технологій. Протягом року було встановлено, що найбільша кількість протиправних діячів знаходиться в Києві, а також на території Одеської, Миколаївської та Львівської областей. Автором констатовано, що 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. Зроблено висновок, що важливим елементом діяльності щодо запобігання 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 наднормово. Окремим заходом запобігання вчиненню кібершахрайств є виявлення діяльності кібертерористів, осіб, що використовують комп'ютери для вчинення терористичних актів.

Ключові слова: *кіберзлочинність, кібершахрайство, кіберполіція, запобігання, правове регулювання.*

Today it is difficult to argue about the importance of the Internet in our lives. The Internet opens up prospects for self-development, gaining new knowledge, finding a job, etc. We use this resource every day, we can even spend our free time on its spaces. But, despite this, the Internet has another side, the one in which criminal offenses are committed every day, every hour, because the platform provides users with complete anonymity and does not limit them in their actions. For example, in 2018 in Ukraine, employees of the Cyber Police Department of the National Police of Ukraine were involved in more than eleven thousand criminal proceedings related to criminal offenses in the field of the latest information technologies. During the year, it was established that the largest number of illegal actors is located in Kyiv, as well as in the Odesa, Mykolaiv, and Lviv regions. The author stated that the process of combating cyber fraud in Ukraine is complicated by the fact that the term "cyber fraud" itself is not defined in the legislation, not even paying attention to the fact that the concept is not new both for law enforcement agencies of Ukraine and for foreign countries. Today, information technologies are used in almost all spheres of social life, and even in the state's economy, which makes it possible to put the problem of combating cyber fraud among the main ones. In addition to the direct harm that can be caused by unauthorized access to information, or its distribution or modification, cyber fraud can be a source of threat to national security, the economy, and human interests. The problem is that the threat of such actions is not fully realized, the reason for this is that the fundamental concepts related to it are not scientifically developed. It was concluded that an important element of activities related to the prevention of cyber fraud is the identification of persons who commit these illegal acts, or are prone to commit such crimes. A key indicator that a person is prone to such actions is the system overwriting data without any real need, their replacement or deletion, the appearance of false records, as well as cases when an employee starts working overtime for no reason. A separate measure to prevent the commission of cyber fraud is the detection of the activities of cyber terrorists, persons who use computers to commit terrorist acts.

Key words: *cybercrime, cyber fraud, cyber police, prevention, legal regulation.*

На сучасному етапі розвитку суспільства все 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 запобігання 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. 45–46]. 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 науки, навіть попри те, що протиправні діяння із застосуванням Всесвітньої павутини мають високий рівень суспільної небезпеки.

Отже, відсутність належного законодавчого закріплення поняття «боротьба з кібепшахрайством» 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, шляхом законодавчого врегулювання 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.

Загалом запобігання кібершахрайству має включати в себе загальнодержавні заходи економічного, виховного, політичного характеру, а також комплекс вузько спрямованих заходів, спрямованих 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: правові заходи; технічні й процедурні заходи; організаційні структури; створення потенціалу; міжнародна співпраця;

Для дієвого запобігання кібершахрайству 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 даної проблеми.

Для того, аби мати змогу ефективно розслідувати кримінальні правопорушення пов'я-

зані 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, а й між громадянином та державою [2, с. 126–128].

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:

– 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;

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

– недоліки в діяльності правоохоронних органів щодо реагування на звернення та повідомлення про кібершайхства.

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 даного виду, а також запобігати формуванню особистості правопорушника.

Для належної розробки відповідних заходів запобігання кібершахрайству, необхідним аспектом є організація діяльності правоохоронних органів, а також вищих органів держави, що відповідає вимогам, які мають існувати у правовій, незалежній, демократичній державі. До того ж, 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 в основному 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:

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

– 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;

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

– 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;

– 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);

– участь працівників кіберполіції у 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 запобігання 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 наднормово. Окремим заходом запобігання вчиненню кібершахрайств є виявлення діяльності кібертерористів, осіб, що використовують комп'ютери для вчинення терористичних актів.

Список використаних джерел:

1. Петрик В. Сутність інформаційної безпеки держави, суспільства та особи. *Юридичний журнал*. 2009. № 5. С. 45–46.

2. 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. К. : Нац. акад. СБУ України, 2010. С. 126–128.