АДМІНІСТРАТИВНЕ ПРАВО І АДМІНІСТРАТИВНИЙ ПРОЦЕС, ІНФОРМАЦІЙНЕ ПРАВО

АРТЕМЕНКО О. В.,
кандидат юридичних наук, доцент кафедри адміністративного та фінансового права
(Національний університет біоресурсів і природокористування України)

БІДОНЬКО Р. В.,
студент V курсу юридичного факультету
(Національний університет біоресурсів і природокористування України)

УДК 342

КІБЕРПОЛІЦІЯ УКРАЇНИ. ОРГАНІЗАЦІЯ ДІЯЛЬНОСТІ ТА ПЕРСПЕКТИВИ РОЗВИТКУ

У роботі розглядається діяльність основного органу захисту прав громадян та держави в інформаційній сфері та сфері ІТ-технологій України – кіберполіції. Проаналізовані нормативно-правові засади діяльності кіберполіції в Україні та подальші перспективи його функціонування. Вивчені статистичні дані вчинених кіберзлочинів.

Ключові слова: *кіберполіція, інформаційні технології, кіберзлочини, нормативно-правовий акт.*

В работе рассматривается деятельность главного органа защиты прав граждан и государства в информационной сфере и сфер ІТ-технологий Украины – киберполиции. Сделан анализ нормативно-правовых основ деятельности киберполиции в Украине и дальнейшие перспективы его фунцинирования. Изучены статистические данные киберпреступлений.

Ключевые слова: *кибрполиция, информационные технологи, киберпреступления, нормативно-правовой акт.*

This paper describes the activities of the main body that protect the rights of citizens and the state in the sphere of information technologies and the field of IT technologies in Ukraine – cyberpolice. There are analyzed legal principles of cyberpolice in Ukraine and future prospects of its operation, are studied statistics of committed cybercrimes.

Key words: *cyberpolice, information technologies, cybercrimes, legal act.*

Вступ. З розвитком науково-технічного прогресу з кожним роком виникають все нові групи відносин, а з ними – і групи прав. Ми маємо на увазі, що сьогодні важко знайти людину, яка б не користувалася комп'ютером чи телефоном. Ці гаджети є колосальним джерелом інформації. Як показує практика, де є права, – там є і порушення (злочини), або посягання на права людей у сфері інформаційних технологій. На противагу злочинам в інформаційній сфері держава, як виконавець волі народу, створює підрозділи з боротьби зі злочинністю – підрозділи кіберполіції в складі Національної поліції України.

Науково-теоретичною основою наукової статті стали праці таких вчених, як І.В. Арістова, Ю.М. Батурин, К.І. Бєляков, А.В. Сорокіна, Н.В. Карпова та інші.

Постановка завдання. Необхідно проаналізувати нормативно-правові акти, наукові праці українських вчених щодо вдосконалення діяльності кіберполіції України та акцентувати увагу на тому, що даний підрозділ поліції має важливе значення для України. У зв'язку з тим, що науково-технічний процес не стоїть на місці з'являтимуться нові види злочинів, а тому треба вдосконалювати захист прав від злочинних посягань в інформаційній сфері.

Результати дослідження. Кіберполі́ція – структурний підрозділ Національної поліції України, що спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізмів підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних та комп'ютерних інтернет-мереж і систем.

Даний орган регламентується наказом Кабінету Міністрів України № 831 від 13 жовтня 2015 року «Про утворення територіального органу Національної поліції», а також відповідно до наказів МВС від 15.10.2015 № 1250 «Про проведення позачергового атестування осіб начальницького складу підрозділів боротьби з кіберзлочинністю» та № 1251 від 15.10.2015 «Про проведення конкурсу на заміщення вакантних посад старших інспекторів, інспекторів і спеціальних агентів інформаційних технологій міжрегіонального територіального органу Департаменту кіберполіції Національної поліції». Також є Положення про Департамент кіберполіції НП України, затверджене наказом Національної поліції від 10.11.2015 № 85, згідно з яким створено Департамент кіберполіції, який є юридичною особою публічного права; Закон України «Про ратифікацію Конвенції про кіберзлочинність» [1–6].

До складу Департаменту входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Поліське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах). А також з метою забезпечення міжнародної діяльності кіберполіції в штатній структурі Департаменту кіберполіції створено сектор Національного контактного пункту з реагування на кіберзлочини [5].

На сьогодні відбувається перетворення колишньої моделі підрозділів боротьби з комп'ютерними злочинами в новий орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєвого реагування на кіберзагрози, а також, у відповідності до кращих європейських та світових стандартів проводитиме міжнародну співпрацю з знешкодження транснаціональних злочинних угрупувань у даній сфері.

Ми вважаємо, що кіберполіція має досить ефективну та конкретну нормативно-правову базу, що забезпечує функціонування та регламентує його діяльність, що свідчить про перспективну діяльність в інформаційній сфері права.

Незважаючи на прийняття національного законодавства з боротьби з кіберзлочинністю в ряді країн, у тому числі й в Україні, її «уніфікований» склад до цих пір чітко не визначений, оскільки як можливості технічних засобів, програмного забезпечення, засобів телекомунікації, так і кримінальні хитрування самих кіберзлочинців безперервно зростають із розвитком науково-технічного прогресу і відсталістю правових норм протидії. [8, с. 30]

Боротьба з комп'ютерними злочинами, на нашу думку, безглузда без знань та розуміння правових проблем регулювання інформаційних мереж. Тому для ефективного реагування на злочини в комп'ютерній сфері та вироблення можливих механізмів боротьби необхідно досліджувати взаємозв'язок між технічними характеристиками мережі, нормативно-правовими і соціальними труднощами.

Розслідування злочинів в інформаційних мережах зазвичай вимагає швидкого аналізу та збереження комп'ютерних даних, які дуже вразливі за своєю природою і можуть бути швидко знищені. У цій ситуації традиційними є механізми правової взаємодопомоги і принцип суверенітету, одним з проявів якого є те, що тільки правоохоронні органи держави можуть проводити слідчі дії на його території, вимагають безліч формальних погоджень, роблячи розслідування транснаціональних кіберзлочинів проблематичним. Окрім співробітництва правоохоронних органів, яке вимагає тимчасових витрат і дотримання безлічі формальностей, встає також питання про дотримання фундаментального принципу, коли необхідна подвійна криміналізація діяння: як у країні, з території якої діяв правопорушник, так і в державі, де знаходиться потерпілий. Різниця в криміналізації діянь, відмінності у визначенні тяжкості вчиненого діяння, особливо у сфері релігійних злочинів і злочинів проти громадського порядку, в області нелегального контенту, в екстремістських злочинах значно ускладнюють процес співробітництва правоохоронних органів, іноді роблячи його неможливим [7].

У ході розроблення концепції з реформування підрозділів боротьби з кіберзлочинністю використано найкращий європейський та світовий досвід, а також пропозиції міжнародних організацій.

Проте необхідно зазначити, що досвід із боротьби з даним специфічним видом злочинності в Україні порівняно з іншими державами досить низький, що впливає на рівень захисту прав у даній сфері. Тому низький рівень захисту в даній Інформаційній сфері права легко обгрунтувати:

1) низький рівень фінансування, що яскраво впливає на технічну базу для боротьби з кіберзлочинами;

2) нема створеного вузькоспеціалізуючого інституту з підготовки кваліфікованих кадрів;

3) штатний колектив кіберполіції налічує 400 осіб, котрі повинні здійснювати моніторинг ситуації в Україні з мільйонним населення та співпрацювати з міжнародними органами для розкриття транснаціональних злочинних угрупувань, що фізично дуже важко;

4) практичний досвід. Досвід та вміння, отримані в практичній діяльності, важливіші за статистику.

Через незаконну діяльність на території України «піратів» різного формату Україну досить тривалий час вважали державою, яка не хоче та не вживає відповідних заходів реагування з даним негативним явищем. Однак протягом останнього року, згідно з даними міжнародних експертів, саме через активну діяльність працівників кіберполіції переважна більшість так званих сайтів «онлайн-піратів» припинила свою злочинну діяльність.

Черговою перемогою на даному «полі бою» є результат діяльності працівників Київського управління кіберполіції та Київської міської прокуратури № 3, внаслідок роботи яких було припинено функціонування піратського сайту «baltazar.org.ua», через діяльність якого правовласникам було завдано матеріальних збитків на загальну суму понад 1 мільйон гривень.

Організатором вказаного ресурсу виявився 44-річний мешканець столиці, який створив, адміністрував та наповнював вказаний сайт піратським контентом. На момент проведення операції з припинення діяльності сайту останній щодня відвідувало близько 3 тис. громадян.

У ході проведення обшуків правоохоронцями було виявлено та вилучено серверне обладнання, комп'ютерну техніку, за допомогою якої здійснювалось адміністрування та підтримання діяльності веб-ресурсу «baltazar.org.ua».

Наразі вилучена техніка направлена для проведення подальшої експертизи, за результатами проведення якої організатору злочинного промислу буде оголошено повідомлення про підозру за вчинення злочину, передбаченого статтею 176 Кримінального Кодексу України [8].

Можемо підсумувати, що чим краще обладнання в держслужбовців, тим ефективніша діяльність підрозділу. Але з огляду на рівень злочинності необхідно підвищити рівень держслужбовців та спеціалістів.

Висновки. Отже, перший крок на шляху боротьби з комп'ютерною злочинністю (кіберзлочинністю) зроблено. Створення підрозділу кіберполіції –початок розвитку правоохоронної системи в ІТ-сфері, що зближує Україну (як прогресуючу державу) з Європейським союзом. Якщо в Україні буде приділятись належна увага до даного питання та підтримка і рефінансування зі сторони парламенту, тоді можна частково прогнозувати успішний розвиток охорони прав в інформаційному суспільстві країни.

На нашу думку, для ефективного функціонування та розвитку правоохоронних органів в даній сфері, зокрема підрозділу кіберполіції, необхідно виділити його в окремий орган, який буде незалежним та складатиметься з професіоналів у даній ІТ-сфері.

Необхідний ефективний контроль злочинів у кібепросторі, який вимагає набагато більш інтенсивного міжнародного співробітництва, ніж існуючі заходи з боротьби з будь-якими іншими формами міжнародної злочинності. Саме тому, окрім гармонізації кримінально-правових норм, потрібна гармонізація процесуальних інструментів і вироблення нових механізмів міжнародного співробітництва. Важливу роль у боротьбі з кіберзлочинністю грають міжнародні угоди у відповідній області, такі як Конвенція Ради Європи про кіберзлочинність, рішення Ради Європейського Союзу, Модельний Закон Співдружності Націй про комп'ютерні злочини 2002 р., Модельний Закон країн Карибського Басейну про кіберзлочинність (проект HIPCAR), спільний проект Європейського союзу і Міжнародного Союзу Електрозв'язку для держав Тихоокеанського регіону (проект ICB4PAC), проект ООН з розробки законодавства в галузі кіберзлочинності для країн Африки (проект ESCWA) та ін.

Розробка спеціальної Стратегії кібербезпеки представляє дуже актуальне завдання для України у сфері протидії загрозам у віртуальному просторі. Частиною цієї стратегії має стати стратегія боротьби з кіберзлочинністю. Подібний досвід вже має цілий ряд держав. Інформаційна безпека вже розглядається державами як одне з пріоритетних завдань у сфері національної безпеки та міжнародної політики. При цьому концепція інформаційної безпеки включає як захист користувачів мереж, так і захист держави і критичних інфраструктур.

Ми вважаємо, що підрозділ кіберполіції є основним та єдиним органом із боротьби з кіберзлочинністю та злочинами в інформаційній сфері, що підкреслює велике значення його діяльності. Перш за все, даний орган повинен захищати інтереси громадян держави та їх персональних чи конфіденційних даних. Також повинен бути швидким, ефективним та обороняти інформаційні кордони України.

Тому розвиток та вдосконалення діяльності кіберполіції України будуть тільки позитивно відображатись на захисті прав та інтересів громадян і держави в цілому.

Список використаних джерел:

1. Закон України «Про національну поліцію» від 2 липня 2015 року № 580-VIII.

2. Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 року № 2824-IV.

3. Постанова Кабінету Міністрів України від 13 жовтня 2015 року № 831 «Про утворення територіального органу Національної поліції».
4. Постанова Кабінету Міністрів України від 28 жовтня 2015 року № 877 «Про затвердження Положення про Національну поліцію».
5. Наказ Національної поліції України від 07.11.2015 № 10 «Про затвердження Штату Департаменту кіберполіції Національної поліції України».
6. Наказ Національної поліції України від 10.11.2015 № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України».
7. Незалежна асоціація банків України. Завдання кіберполіції / Незалежна асоціація банків України. – 2016 [Електронний ресурс]. – Режим доступу до ресурсу : http://anticyber.com.ua/article_detail.php?id=140.
8. Департамент кіберполіції національної поліції України [Електронний ресурс] – Режим доступу до ресурсу : https://ru-ru.facebook.com/cyberpoliceua/.

БЕЛЕЙ Є. Н.,
аспірант кафедри адміністративного права
(Київський національний університет імені Тараса Шевченка)

УДК 342.92

ДЕЯКІ ПИТАННЯ ПУБЛІЧНОГО ПРАВОНАСТУПНИЦТВА ОРГАНІВ ДЕРЖАВНОЇ ВЛАДИ

Стаття присвячена дослідженню проблемних питань публічного правонаступництва органів державної влади, зокрема проблемам співвідношення правового інституту публічного правонаступництва в адміністративному праві зі схожими правовими інститутами в інших галузях права та значення цього інституту для захисту прав та свобод людини.
Ключові слова: *публічне правонаступництво, процесуальне правонаступництво, адміністративне право, адміністративний процес.*

Статья посвящена исследованию проблемных вопросов публичного правопреемства органов государственной власти, в том числе проблемам соотношения правового института публичного правопреемства в административном праве со смежными правовыми институтами в других отраслях права и значения этого института для защиты прав и свобод человека.
Ключевые слова: *публичное правопреемство, процессуальное правопреемство, административное право, административный процесс.*

The article is dedicated to the analysis of the issues of the public succession by state authorities, including the issue of the correlation between the public succession as an institution of law with the similar institutions of law within different branches of law as well as the issue of the significance of this institution of law for the protection of human rights and freedoms
Key words: *public succession, procedural succession, administrative law, administrative procedure.*

Вступ. Публічне правонаступництво є порівняно новим інститутом у науці адміністративного права, наукове дослідження якого розпочате недавно. Проте саме явище публічного правонаступництва існувало давно – протягом історії зі здійсненням реформ у державному апараті на зміну старим органам приходили нові органи, перебираючи на себе повноваження старих.

Особливого значення в Україні публічне правонаступництво набуло протягом останнього десятиліття зі становленням системи адміністративної юстиції, отриманням фізичними та юридичними