УДК 343
DOI https://doi.org/10.32782/app.v75.2025.43

Л. А. Луговець
orcid.org/0009-0002-9138-6115
аспірантка кафедри кримінального права та процесу
Державного податкового університету

ПРАВООХОРОННІ ОРГАНИ ЯК СУБ'ЄКТ ЗАПОБІГАННЯ КІБЕРЗЛОЧИННОСТІ

Вступ. Суспільна значимість і розвиток будь-якого направлення у науці залежать від того, наскільки актуально та правильно буде визначено, здійснено опис предмета дослідження будь якої галузі. Предмет даної статті «Правоохоронні органи як суб'єкт запобігання кіберзлочинності» характеризує актуальність дослідження, дає можливість більш чітко сформулювати розуміння й завдання перспективних досліджень у даному спрямуванні.

Аналіз останніх досліджень і публікацій. Вагомий внесок у дослідження проблем запобігання кіберзлочинності та значення правоохоронних органів як суб'єкта запобігання кіберзлочинності зробили О. М. Бандурко, О. М. Бодунова, В. В. Василевич, В. В. Голіна, Б. М. Головкін, А. П. Закалюк, О. М. Литвинов, В. В. Марков, М. І. Сащенко, В. І. Трапезніков, В. В. Топчій, та інші. Проте окремі питання діяльності правоохоронних органів у запобіганні кіберзлочинності є такими, що постійно потребують наукового аналізу та вивчення для подальшого удосконалення їх діяльності у цій сфері.

Мета дослідження. Проаналізувати окремі питання діяльності правоохоронних органів у запобіганні кіберзлочинності на сучасному етапі розвитку нашого суспільства, оскільки такий вид злочинності є найбільш динамічний вид кримінального правопорушення, яка має швидку тенденцію у поширенні, що зумовлена постійним розвитком комп'ютерних технологій.

Актуальність. Сучасні дослідження кіберзлочинності вказують на необхідність вдосконалення механізмів запобігання кіберзлочинності в Україні саме правоохоронними органами та активно сприяти реалізації нововведень передусім у державних структурах. Доречним буде першою чергою передбачити на законодавчому рівні можливості проведення перевірок правоохоронними органами тих суб'єктів, що надають цифрові послуги, наділити підрозділи поліції новими функціями щодо запобігання кіберзлочинності виданням відповідного нормативного акту. Сприяти у розвитку тісного співробітництва з правоохоронними органами ЄС, спільній діяльності громадськості та наукових центрів з правоохоронними органами на основі стандартів ЄС.

Виклад основного матеріалу. Історичний розвиток людства повсякчас доводить свою багатогранність та, водночас, внутрішню неузгодженість. Незмінним її супутником виявляється злочинність, що адаптивним феноменом пронизує все нові і нові сфери й форми соціальної динаміки. Не є виключенням в цьому сенсі й кіберпростір, як віртуальний ресурсний комунікаційний простір, інтеграція можливостей якого до життєдіяльності суспільства безперечно тягне за собою й впровадження до останнього специфічних видів кримінальних правопорушень. З'являються нові прояви злочинності – комп'ютерної, які отримують поширення при використанні нових методів, наприклад, технології Bluetooth, бездротових систем зв'язку Wi-Fi та WiMAX, піринговых мереж (P2P), спаму та інших. Крадіжки грошей з банківських карток, створення сайтів з дитячою порнографією, комп'ютерні віруси, пропаганда насильства та расової, релігійної, етнічної ненависті, інструкції з виготовлення саморобних вибухових пристроїв, кібератаки на комп'ютерні мережі державних установ – це лише мала частина злочинів, що вчиняються сьогодні в інтернеті та яким намагаються запобігти правоохоронні органи різних країн (Боротьба з кіберзлочинністю– завдання міжнародного рівня, 2009 р.)

Події останніх років повномасштабного вторгнення в Україну країни агресора, засвідчили, наскільки важливим, а інколи критичним є належне забезпечення охорони інформаційної безпеки нашої держави.

Варто зазначити, що ще наприкінці червня 2014 року у складі Національної гвардії України було створено Управління інформаційної безпеки. З того часу було посилено заходи розбудови системи запобігання кіберзлочинності на вищому державному рівні. Так, Указом Президента України від 24 вересня 2014 року № 744/2014 «Про рішення Ради національної безпеки і оборони України від 28 серпня 2014 року «Про невідкладні заходи щодо захисту України та зміцнення її обороноздатності» було передбачено створення національного центру кіберзахисту і протидії кіберзагрозам. А вже 14 жовтня 2014 року наказом Адміністрації Держспецзв'язку створено оперативну групу (координаційний центр) із питань реагування на комп'ютерні інциденти. Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності. До складу оперативної групи входитимуть представники Державної служби спеціального зв'язку та захисту інформації України, Служби безпеки України, Міністерства внутрішніх справ України, Служби зовнішньої розвідки України, Міністерства оборони України та Генерального штабу Збройних Сил України, Генеральної прокуратури України, Національної комісії, що здійснює державне регулювання у сфері зв'язку та інформатизації, представники двох десятків провідних операторів і провайдерів телекомунікацій, а також громадських організацій ІнАУ, «ТЕЛАС» та Київського відділення ISACA. Незважаючи на значну кількість державних та недержавних суб'єктів, що спрямовують свої зусилля на подолання кіберзлочинності, левову частку цієї діяльності забезпечують підрозділи боротьби з кіберзлочинністю Міністерства внутрішніх справ України. Тільки протягом 2013 року було зареєстровано 4123 таких злочинів, при цьому їх розкривання становить близько 50 %. Головними завданнями, що постають перед органами, які беруть участь у протидії кіберзлочинності, сьогодні можна визначити: – внесення змін і доповнень до чинного законодавства. Нормативно-правова база серед іншого потребує змін у частині захисту національного інформаційного простору від протиправного контенту, надання додаткових повноважень правоохоронним органам з оперативного припинення окремих видів кіберзлочинів тощо; – якісну підготовку та підвищення кваліфікації кадрів. На сьогодні ці завдання виконує Харківський національний університет внутрішніх справ на підставі наказу Міністерства внутрішніх справ України «Про організацію підготовки кадрів у Харківському національному університеті внутрішніх справ» від 20.11.2012 № 1062. У серпні 2014 року університет було включено до Стратегії Ради Європи «Підготовка правоохоронних органів» у частині навчання фахівців із протидії кіберзлочинності в Україні; – розробку актуального спеціалізованого програмного та апаратного забезпечення для провадження оперативно-розшукової діяльності в кіберпросторі (визначення місцезнаходження особи за її мережними ідентифікаторами, перехоплення вмісту повідомлень або службової інформації цільового об'єкта, дослідження даних, у тому числі порівняння ідентифікованих та ідентифікуючих об'єктів, документування інтелектуальних слідів учинення злочину, активна дія на цільовий об'єкт); Актуальні питання діяльності правоохоронних органів у сфері протидії кіберзлочинності: удосконалення системи інформаційно-аналітичного забезпечення (створення Єдиної інформаційно-аналітичної системи правоохоронних органів із підсистемами за напрямами, у тому числі з окремим блоком для підрозділів боротьби з кіберзлочинністю); – покращення рівня відповідної внутрішньої та зовнішньої взаємодії (найбільш актуальним питанням є удосконалення механізму міжнародної взаємодії, адже більшість кіберзлочинів мають транснаціональний характер, а тому виникає багато проблем юрисдикційного характеру).

Поширеність та суспільна небезпечність кіберзлочинів в останні роки набула загрозливих масштабів, що диктує необхідність формування адекватної відповіді з боку держави на інноваційні безпекові виклики. Перш за все, варто зауважити на тому, що досвід протидії кіберзлочинності засвідчує неспроможність жодної окремої країни та жодного відомства автономно вирішити зазначену проблему. Успіх можуть гарантувати лише спільні дії, як державних, так і комерційних структур, в тому числі й у міжнародному контактному форматі. Задля ефективної протидії будь-яким проявам кіберзлочинності та більш швидкого і повного розкриття злочинів у цій сфері правоохоронні органи повинні взаємодіяти із суб'єктами ринку телекомунікаційних послуг, зокрема операторами та провайдерами. Зазначена взаємодія повинна ґрунтуватися на зобов'язані відповідних працівників цих організацій в залежності

від функціональних обов'язків або їх власників повідомляти про будь-які випадки незаконного використання мережі, а також всіма доступними в межах закону засобами сприяти виявленню, припиненню, розслідуванню та іншим заходам протидії кіберзлочинам.

Панує думка, що налагодження таких зв'язків можливе через законодавче врегулювання відповідальності зазначених осіб за відмову від співробітництва (ненадання інформації, непредставлення доступу до мережі тощо) обов'язково із позбавленням права зайняття такою діяльністю, а для самих організацій – припинення діяльності. Необхідним напрямком діяльності правоохоронних органів є удосконалення заходів взаємодії з підприємствами, установами, організаціями, діяльністю яких є розробка комп'ютерної техніки та програмного забезпечення. Така взаємодія має декілька цілей: по-перше, відстежувати осіб, які мають певні знання у цій сфері (особливо тих, які звільнилися та офіційно не працевлаштувалися або стали займатися індивідуальною підприємницькою діяльністю), тобто можуть бути потенційними суб'єктами аналізованих злочинів; по-друге, покращення форм та методів діяльності на підставі отримання інформації відносно розвитку комп'ютерних технологій; по-третє, удосконалення програмного забезпечення власних систем через перейняття досвіду. Також зауважимо, що доцільним заходом протидії кіберзлочинності є підтримання та розширення співробітництва відповідних правоохоронних органів з міжнародними організаціями, що спрямовують свою діяльність у зазначеній сфері. В цьому сенсі позитивним слід визнати досвід «відпрацювання» у 2011 р. Службою безпеки України разом з НАТО загальних механізмів боротьби з кіберзлочинністю, результатом чого стало розроблення експертних консультацій відносно кібернетичного захисту (СБУ відпрацьовує з НАТО механізми боротьби з кіберзлочинністю, 2011 р.).

Дотичним до цього аспектом взаємодії суб'єктів протидії кіберзлочинності є приєднання відповідних підрозділів правоохоронних органів до міжнародних програм, що створюються та організовуються різними державами на підставі договорів та угод. Так, наприклад, відповідно до Конвенції «Про кіберзлочинність», держави-учасники (в тому числі й Україна) повинні здійснити організаційні заходи щодо розробки необхідних умов (зокрема, організація контактних пунктів) на національному рівні, та приєднатися до мережі щоденного цілодобового доступу (міжнародне позначення «24/7 Network» або «доступ 24 години 7 діб на тиждень»), що спрямована на співпрацю та надання допомоги при розкритті та розслідуванні (Бабакін В. М, 2011 р., с. 29).

Вбачається, що напрям удосконалення системи суб'єктів запобігання кіберзлочинності щодо взаємодій слід й надалі розвивати та посилювати.

В Україні органом, на який покладаються повноваження щодо створення та функціонування цілодобової контактної мережі для надання невідкладної допомоги при розслідуванні злочинів, пов'язаних з комп'ютерними системами та даними, переслідуванні осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі, є Міністерство внутрішніх справ України. Але, на сучасному етапі, не зважаючи на обов'язковість, зазначені умови не були виконані у необхідному обсязі. Укладення вказаних угод та приєднання до подібних програм є необхідним кроком для здійснення та розроблення заходів розкриття та протидії аналізованим злочинам. Крім того, необхідним кроком міжнародної взаємодії, в зазначеній сфері, є не лише організація та прийняття участі у вказаних мережах, а й укладання угод, з відповідними підрозділами правоохоронних органів інших країн, з метою обміну інформацією відносно вчинених кіберзлочинів (способів, методів, застосованих технічних або інших засобів тощо) та заходів, які застосовуються щодо їх запобігання та розкриття. Нині, наприклад, чинним є Меморандум «Про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом» (Меморандум про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом, 2009 р.).

Напрацювання ефективних зв'язків є необхідною умовою оперативного та всебічного обміну інформацієюз даного питання. Необхідною умовою запобігання злочинності та особли-

во кіберзлочинності, є також взаємодія правоохоронних органів єдиною системою з вітчизняними та міжнародними представниками громадськості у різних її об'єднаннях, окремими підприємствами, що створюються на добровільних началах і мають за мету захист інформації.

Прикладом такої системної співпраці може бути, створена ще на початку 1990-х років організація FIRST – об'єднання груп реагування на інциденти, яка об'єднує їх біля 80, до складу яких входять працівники державних, комерційних, промислових, у тому числі навчальних установ з 19 провідних країн. Такі об'єднання дозволяють, поперше, слідкувати за розвитком сучасних технологій та програмного забезпечення; обмінюватися досвідом у сфері запобігання злочинності; аналізувати діяльність підприємств, установ та організацій, що забезпечують або надають інформаційні кіберпослуги.

Висновки. Вбачається, що одним з головних завдань має стати удосконалення та уніфікація у чинних нормативно-правових актах України системи суб'єктів запобігання злочинності у цілому, чіткого визначення вживаних термінів у сфері кіберзлочинності; постійне оновлення спеціальними охоронними механізмами, призначеними для здійснення моніторингу кіберпростору та явищ, що відбуваються на його теренах; постійне підвищення кваліфікації кадрового потенціалу правоохоронних органів держави щодо запобігання кіберзлочинності.

Література

Боротьба з кіберзлочинністю – завдання міжнародного рівня / SecurityLab – 01 червня 2009 р. Режим доступу: http://www.securitylab/news/380617.php.

СБУ відпрацьовує з НАТО механізми боротьби з кіберзлочинністю. Режим доступу: http://za.zubr.in.ua/2011/10/18/13536/.

Бабакін В. М. Особливості міжнародного співробітництва при розслідуванні кіберзлочинів. Форум права. 2011. № 4. С. 27–30. Режим доступу: http://nbuv.gov.ua/j-pdf/FP_index.htm_2011_4_6.pdf.

Меморандум про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом : від 09.09.2009. Режим доступу: http://zakon.rada.gov.ua/ laws/show/528_031.

References

Borotba z kiberzlochynnistiu – zavdannia mizhnarodnoho rivnia [Cybercrime struggle – international tasks] / SecuritylAB – June 01, 2009. Access mode: http: //www.securitylAb/news/380617.php.

SBU vidpratsovuie z NATO mekhanizmy borotby z kiberzlochynnistiu [The SBU works with NATO mechanisms for combating cybercrime]. Access mode: http: //za.zubr.in.ua/ 2011/10/18/13536/.

Babakin V.M. (2011) Osoblyvosti mizhnarodnoho spivrobitnytstva pry rozsliduvanni kiberzlochyniv [Features of international cooperation in the investigation of cybercrime]. Law Forum. № 4. P. 27–30. Access mode: http: //nbuv.gOv.ua/j-pdf/fp_index.htm_2011_4_6.pdf.

Memorandum pro spivrobitnytstvo mizh Heneralnoiu prokuraturoiu Ukrainy ta Natsionalnoiu prokuraturoiu Korolivstva Niderlandy u borotbi z kiberzlochynnistiu, orhanizovanoiu zlochynnistiu ta vidmyvanniam dokhodiv, oderzhanykh zlochynnym shliakhom : vid 09.09.2009 [Memorandum of cooperation between the Prosecutor General's Office of Ukraine and the National Prosecutor's Office of the Kingdom of the Netherlands in the fight against cybercrime, organized crime and laundering of income obtained by crime: dated 09.09.2009]. Access mode: http: //zakon.rada.gOv.ua/ laws/shhow/528_031

Анотація

Луговець Л. А. **Правоохоронні органи як суб'єкт запобігання кіберзлочинності.** – Стаття.

Останні десятиліття, не зважаючи на війну, спостерігається активний розвиток ІТ технологій. Комп'ютерне забезпечення та техніка вже давно відіграють велику роль у суспільстві на всіх рівнях, особливо у діяльності держави. Зазначається, що поширення комп'ютеризації призвело до виникнення нових суспільних відносин – кібервідносин. Кіберпростір в свою чергу має, крім позитиву, низку негативних, кримінально-правових характеристик та завдають шкідливих наслідків: порушення авторських прав, розповсюдження шкідливих програм, втручання в роботу інформаційних носіїв/спамів, незаконне використання інформації, інші види кримінальних правопорушень, які були названі у фаховій літературі кіберзлочинами. Акцентується увага на тому, що кіберзлочиність є великою проблемою сучасності і основним суб'єктом запобігання їй є правоохоронні органи. Досліджуються питання кіберзлочинності, яка набула суттєвого розповсюдження, викликало суттєву необхідність удосконалення системи правоохоронних та правозахисних органів не тільки України так і інших багатьох держав.

У статті досліджуються питання запобігання правоохоронними органами систематичному зростанню кількості інформаційних злочинів та динаміці їх поширення. Також, систематичне розповсюдження програм-вірусів, фактів несанкціонованого доступу до інформаційних ресурсів кіберпростору, протиправне викрадення важливої інформації з баз даних, що не перебуває у загальному доступі, спричиняє дедалі більше негативних наслідків та несе небезпеку для суспільства якій мають запобігати правоохоронні органи.

Зазначається, що однією із загроз національній безпеці в інформаційній просторі згідно зі ст. 7 Закону України «Про основи національної безпеки України» дано визначення комп'ютерній злочинності і комп'ютерному тероризму. Конституція України закріплює, що забезпечення інформаційної безпеки названо справою усього українського народу. За останній період воєнного стану у державі правоохоронні органи значно удосконалили заходи запобігання кіберзлочинності. Було створено окреме Управління боротьби з кіберзлочинністю у структурі Міністерства внутрішніх справ України, Департамент контррозвідувального захисту інтересів держави у сфері інформаційної безпеки Служби безпеки України, структури із захисту інформації у складі міністерств та інших органів виконавчої влади.

Ключові слова: правоохоронні органи, кіберзлочинність, кримінальне правопорушення, національна безпека, кіберпростір, правоохоронні органи, кіберполіція, інформаційна сфера, протидія, суб'єкти запобігання.

Summary

Luhovets L. A. **Law enforcement bodies as a subject of cybercrime prevention. –** Article.

In recent decades, despite the war, there has been an active development of IT technologies. Computer software and equipment have long played a major role in society at all levels, especially in the activities of the state. It is noted that the spread of computerization has led to the emergence of new social relations – cyber relations. Cyberspace, in turn, has, in addition to positive, a number of negative, criminal-legal characteristics and causes harmful consequences: copyright infringement, distribution of malicious programs, interference with the work of information carriers/spam, illegal use of information, other types of criminal offenses, which have been called cybercrimes in the professional literature. The emphasis is on the fact that cybercrime is a major problem of our time and the main subject of its prevention is law enforcement agencies. The issues of cybercrime, which has become significantly widespread, have caused a significant need to improve the system of law enforcement and human rights protection bodies not only in Ukraine but also in many other countries.

The article examines the issues of preventing law enforcement agencies from a systematic increase in the number of information crimes and the dynamics of their spread. Also, the systematic spread of virus programs, facts of unauthorized access to information resources in cyberspace, illegal theft of important information from databases that are not publicly available, causes more and more negative consequences and poses a danger to society that must be prevented by law enforcement agencies.

It is noted that one of the threats to national security in the information sphere in accordance with Article 7 of the Law of Ukraine "On the Fundamentals of National Security of Ukraine" is computer crime and computer terrorism. The Constitution of Ukraine stipulates that ensuring information security is called the business of the entire Ukrainian people. During the recent period of martial law in the country, law enforcement agencies have significantly improved measures to prevent cybercrime. A separate Department for Combating Cybercrime was created within the structure of the Ministry of Internal Affairs of Ukraine, the Department for Counterintelligence Protection of State Interests in the Field of Information Security of the Security Service of Ukraine, and information protection structures within ministries and other executive bodies.

Key words: Law enforcement agencies, cybercrime, criminal offense, national security, cyberspace, law enforcement agencies, cyberpolice, information sphere, counteraction, prevention.