УДК 34:351.74:004.738.5

# ОРГАНІЗАЦІЙНО-ПРАВОВІ ЗАСАДИ СТВОРЕННЯКІБЕРПОЛІЦІЇ В УКРАЇНІ

**Ю.В. ЯНЧУК**, ***здобувач*[1],**
***Національний університет***
***біоресурсів і природокористування України***

***Анотація.*** *Стаття присвячена висвітленню питання забезпечення захисту суспільства від кіберзлочинності та правовим засадам створення і функціонування підрозділу Національної поліції, який займається запобіганням та протидією кіберзлочинам.*

***Ключові слова:*** *кіберзлочини, кіберполіція, кібербезпека, кіберзахист, Конвенція про кіберзлочинність*

На сьогодні усі сфери суспільного життя пронизані цифровими інформаційно-комунікативними технологіями, що є ознакою його подальшої інформатизації. Проте даний процес, проходячи стрімко, створює можливості та сприятливі умови для здійснення нових видів правопорушень в інформаційній сфері за допомогою апаратного, програмного забезпечення та локальних мереж.

За офіційними даними, обсяг інформації в світовому інформаційному просторі подвоюється кожні десять років, призводячи до його перевантаження. Основною ознакою існування інформаційного суспільства є вільний доступ усіх його членів до глобальної комп'ютерної мережі Інтернет. Для прикладу, український сегмент мережі Інтернет зріс з 5 млн осіб у 2005 р. до 16 млн у 2015 році. Дані цифри пояснюють і стрімке збільшення різновидів та кількості скоєння неправомірних дій щодо суб'єктів інформаційних відносин, тобто тих осіб, які створюють, поширюють та споживають інформацію в глобальній мережі. Отже, все більших обертів набуває комп'ютерна злочинність (кіберзлочинність).

Кіберзлочином є кримінальна дія, відповідальність за яку передбачено кримінальним законодавством, що здійснена (здійснюється) у кіберпросторі та несе у собі суспільну небезпеку [1].

Для України кіберзлочинність є надзвичайно актуальною проблемою, адже за даними «Лабораторії Касперського» наша країна лідирує у списку країн, де кіберзлочини є надзвичайно поширені й становлять загрозу для суспільства та держави в цілому.

**Метою** даної статті є аналіз доцільності й важливості створення кіберполіції та аналіз організаційно-правових аспектів забезпечення кібербезпеки України.

[1]Науковий керівник – доктор юридичних наук, професор В.І. Курило

Через більш ніж десять років після появи мережі Інтернет у світі почала активно розроблятися правова база, спрямована на припинення злочинів у сфері комп'ютерної інформації. Відповідні зміни до кримінального законодавства було внесено Канадою у 1985 р., Німеччиною у 1986 р., Японією у 1987 р., Англією у 1990 р., Ірландією, Португалією та Туреччиною у 1991 р., Люксембургом та Нідерландами у 1993 р., Ізраїлем у 1995 р., Бельгією у 2000 році.

Спеціальні норми або навіть розділи про комп'ютерні злочини містять усі кримінальні кодекси, ухвалені у світі, починаючи з 1992 р., у тому числі Кримінальні кодекси усіх країн СНД та Балтії [2, с. 22].

На сьогодні в Україні діє низка законів та нормативних документів різних рівнів, що охоплюють питання кібербезпеки держави. Це, зокрема, Закони України «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про основи національної безпеки України». Стратегічними документами у цій сфері є Стратегія національної безпеки України та Доктрина інформаційної безпеки України, а також ратифікована Верховною Радою України «Конвенція про кіберзлочинність». Чинний кримінальний кодекс України встановлює (відповідно до розділу XVI) відповідальність за «злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» (ст. ст. 361–363).

У 2005 р. Україна ратифікувала Конвенцію про кіберзлочинність і таким чином імплементувала положення міжнародного акта у вітчизняне законодавство.

Підписуючи дану конвенція у 2001 р., уряди європейських країн були впевнені у першочерговій необхідності спільної кримінальної політики, спрямованої на захист суспільства від кіберзлочинності, між іншим, шляхом створення відповідного законодавства і налагодження міжнародного співробітництва; усвідомлюючи глибокі зміни, спричинені переходом на цифрові технології, конвергенцією і глобалізацією комп'ютерних мереж, що триває; стурбовані ризиком того, що комп'ютерні мережі та електронна інформація можуть також використовуватися для здійснення кримінальних правопорушень і того, що докази, пов'язані з такими правопорушеннями, можуть зберігатися і передаватися такими мережами.

Відповідно до змісту Конвенції про кіберзлочинність кожна Сторона (країна) вживає такі законодавчі та інші заходи, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за навмисне вчинення, без права на це, протиправних дій за допомогою інформаційно-комунікативних технологій, тобто за злочини у віртуальному просторі [3].

Злочин можна вважати вчиненим через кіберпростір, коли під час його здійснення засоби комп'ютерних технологій використовуються:

- для автоматизації злочинної діяльності;
- для втручання в роботу інших ЗКТ;
- як телекомунікаційний засіб.

Отже, кіберпростір – інформаційне середовище (простір), яке виникає (існує) за допомогою інформаційно-телекомунікаційних систем під час взаємодії людей між собою, взаємодії інформаційно-телекомунікаційних систем та управління людьми цими системами.

Президент України у Посланні до Верховної Ради України 2011 року зазначив, що кібернетичний простір дедалі більше стає полем протистояння між окремими державами, джерелом небезпек для національної інфраструктури з боку військових та розвідувальних структур, організованих злочинних угруповань, що прагнуть використовувати Інтернет і новітні інформаційно-комп'ютерні технології для досягнення своїх підривних або кримінальних цілей [2].

Визначення поняття «кіберзлочини» не означає необхідності їх виділення в окремий розділ Кримінального кодексу, однак дає змогу відокремити їх від інших злочинів за специфічною ознакою – скоєнням через кіберпростір, що необхідно насамперед правоохоронним органам для покращення боротьби з таким явищем. Зокрема, це досягається шляхом створення спеціального оперативного підрозділу з боротьби з «кіберзлочинами», який завдяки своїй виключній спеціалізації своєчасно виявляє та суттєво покращує якість їх розкриття, розслідування й профілактики, тобто забезпечує кібербезпеку усієї держави.

Кібербезпека – це стан захищеності кіберпростору в цілому або окремих його об'єктів інфраструктури від ризику стороннього кібернетичного впливу (кібератак), за якого забезпечується їх сталий розвиток, а також своєчасне виявлення, запобігання і нейтралізація реальних та потенційних загроз особистим, корпоративним та (або) національним інтересам. Відповідно, кіберзахистом є сукупність методів і заходів організаційного, нормативно-правового та технічного характеру, спрямованих на забезпечення кібербезпеки [4].

Закон України «Про ратифікацію Конвенції про кіберзлочинність» від 7 вересня 2005 р. № 2824-IV зі змінами, внесеними Законом України «Про внесення змін до Закону України «Про ратифікацію Конвенції про кіберзлочинність» від 21 вересня 2010 р. № 2532-VI, фактично визначав три органи, які мають повноваження щодо здійснення міжнародного співробітництва у протидії кіберзлочинності: Міністерство юстиції України (щодо запитів судів) та Генеральна прокуратура України (щодо доручень органів досудового слідства) – органи, відповідальні за надсилання запитів про взаємну допомогу, надання на них відповідей, їх виконання або передачу уповноваженим органам, а Міністерство внутрішніх справ України – орган, 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, які обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі [5, с. 54–56].

Переймаючи досвід європейських країн, в Україні в даний час розпочинається процес створення підрозділу поліції, що буде займатися попередженням, запобіганням та боротьбою з кіберзлочинністю. На сьогодні

триває процес формування штату кіберполіцейських, а завершальним перехідним етапом стане вибудовування нового функціоналу кіберполіції та перепідготовка персоналу.

На кіберполіцію в Україні буде покладено наступні завдання:

1. Реалізація державної політики у сфері протидії кіберзлочинності.

2. Протидія кіберзлочинам:

– у сфері використання платіжних систем: (скімінг, кеш-трепінг, кардінг, несанкціоноване списанням коштів з банківських рахунків за допомогою систем дистанційного банківського обслуговування);

– у сфері електронної комерції та господарської діяльності: (фішинг, он-лайн шахрайство);

– у сфері інтелектуальної власності: (піратство, кардшарінг);

– у сфері інформаційної безпеки: (соціальна інженерія, мальваре, протиправний контент, рефайлінг).

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. Забезпечення діяльності мережі контактних пунктів між 90 країнами світу [6].

Отже, основною метою створення кіберполіції в Україні є реформування та розвиток підрозділів МВС України, що забезпечить підготовку та функціонування висококваліфікованих фахівців в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Відбуватиметься поетапне перетворення теперішньої моделі на новітній орган правозахисного призначення, який за своїми технічними та професійними можливостями матиме змогу миттєво реагувати на кіберзлочини та кіберзагрози, а також, відповідно до кращих світових стандартів, проводити міжнародну співпрацю щодо знешкодження транснаціональних злочинних угрупувань у даній сфері [6].

Виконуючи свої функції та завдання, покладені на кіберполіцію, інформування суспільства про будь-які кіберзагрози та їх попередження здійснюється за допомогою новоствореного сайту кіберполіції України – www.cybercrime.gov.ua. Зокрема, використовуючи даний ресурс, можна перевірити на наявність кібератак мобільний телефон, банківський рахунок, зв'язатися з оперативними працівниками даного підрозділу та отримати допомогу чи консультацію.

Нині проблеми протидії кіберзлочинності набувають все більшої актуальності та потребують нагального вирішення. Тому забезпечення

кібербезпеки особи, суспільства та держави входитиме до функціональних обов'язків структурного підрозділу Національної поліції – кіберполіції.

**Список літератури:**

1. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування / Національний інститут стратегічних досліджень при Президентові України : [Електронний ресурс]. – Режим доступу : http/www.niss.gov.ua/articles/454/
2. Додонов В. В. Сравнительное уголовное право. Общая часть: моногр. / В. В. Додонов, под. общ. ред. С. П. Щербы. – М. : Юрлитинформ, 2009. – 448 с.
3. Конвенція про кіберзлочинністьРада Європи; Конвенція, Міжнародний документ від23 листопада 2001 р.
4. Проблеми чинної вітчизняної нормативно-правової бази у сфері боротьби із кіберзлочинністю: основні напрями реформування / Національний інститут стратегічних досліджень при Президентові України: : [Електронний ресурс]. – Режим доступу : http/www.niss.gov.ua/articles/454/
5. Васильєв А. А. Єдиний центральний орган України з міжнародного співробітництва щодо протидії кіберзлочинності / А. А. Васильєв, Д. Є. Пашнєв // МатеріалиМіжнародної науково-практичної конференції (м. Харків, 10 грудня 2013 р.).
6. [Електронний ресурс]. – Режим доступу : https://www.facebook.com/arsen.avakov.1/posts/916452195111554

***Аннотация.****Статья посвящена освещению вопроса обеспечения защиты общества от киберпреступности и правовых основ создания и функционирования подразделения Национальной полиции, занимающегося предотвращением и противодействием киберпреступлений.*

***Ключевые слова:****киберпреступления, киберполиции, кибербезопасность, киберзащита,Конвенция о киберпреступности.*

***Annotation.*** *The article is devoted to coverage of the issue of the protection of society against cybercrime and legal basis for the creation and operation unit of the National Police, which deals with prevention and counteraction to cybercrime.*

***Keywords:*** *cybercrime, kiberpolice, cyber security, cyber defense, the Convention on Cybercrime.*