ДЕРЖАВНЕ РЕГУЛЮВАННЯ ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ В УКРАЇНІ: ПОНЯТТЯ ТА ОСНОВНІ НАПРЯМКИ

STATE REGULATION OF COMBATING CYBERCRIME IN UKRAINE: CONCEPTS AND MAIN DIRECTIONS

УДК 355: 355.1: 355.7
DOI https://doi.org/10.32782/pma2663-5240-2024.40.41

Коцман І.І.
аспірант кафедри публічного управління та адміністрування, Вінницький державний педагогічний університет імені Михайла Коцюбинського, головний юрист в ПАТ «Волочиська Кура»
ORCID ID: 0009-0009-1791-1592

У статті проаналізовано наукові підходи по поняття «кібезлочинінсть» та запропоновано авторське визначення цього поняття. Обґрунтовано, що відсутність єдиного підходу до розуміння поняття «кіберзлочинність» тягне за собою й інші проблеми, в тому числі розбіжності у державному регулюванні кіберзлочинності.

Виділено такі основні характерні риси (ознаки) кіберзлочинності: 1) глобальність та транснаціональність; 2) високий рівень анонімності; 3) швидка еволюція методів і технологій; 4) висока залежність від технологічних прогалин; 5) широкий спектр мотивацій правопорушників. На основі існуючих наукових підходів було запропоновано власне визначення державного регулювання протидії кіберзлочинності, під яким запропоновано розуміти систему правових, організаційних та технічних заходів, що реалізуються державними органами з метою попередження, виявлення, розслідування та усунення наслідків кіберзлочинів.

У статті обґрунтовано, що державне регулювання протидії кіберзлочинності полягає в комплексі заходів, які розробляються та впроваджуються державними органами для забезпечення захисту кіберпростору та боротьби з кіберзлочинами. Зазначено, що це регулювання охоплює декілька основних напрямків: 1) формування нормативно-правової бази; 2) створення нових та удосконалення роботи існуючих правоохоронних органів та їх підрозділів, які ведуть боротьбу із кіберзлочинністю; 3) міжнародна співпраця в цій сфері; 4) розвиток технічної інфраструктури та підвищення обізнаності суспільства у сфері кіберзлочинності; 5) попередження та профілактика кіберзлочинності.

В ході дослідження доведено, що державне регулювання в будь-якій сфері суспільного життя передбачає існування певної системи організаційно-правового забезпечення, а основою для створення цієї системи є правове регулювання суспільних відносин. Підкреслено, що завдяки правовому регулюванню держава має можливість здійснювати вплив на об'єкти управління. До таких засобів правового регулювання належать нормативні та індивідуальні акти, які встановлюють правила поведінки в суспільстві та визначають права й обов'язки конкретних учасників правовідносин.

Ключові слова: *кібезлочинність, кіберзлочин, кібербезпека, державне регулювання протидії кіберзлочинності, публічне управління та адміністрування, напрямки державного регулювання протидії кіберзлочинності.*

The article analyzes scientific approaches to the concept of "cybercrime" and proposes a personal definition of this term. It is substantiated that the lack of a unified approach to understanding the concept of "cybercrime" leads to other issues, including discrepancies in state regulation of cybercrime.

The main characteristics (features) of cybercrime are identified: 1) global and transnational nature; 2) high level of anonymity; 3) rapid evolution of methods and technologies; 4) high dependence on technological gaps; 5) a wide range of offender motivations. Based on existing scientific approaches, the article proposes an original definition of state regulation for combating cybercrime, which is understood as a system of legal, organizational, and technical measures implemented by state authorities to prevent, detect, investigate, and eliminate the consequences of cybercrimes.

The article argues that state regulation of combating cybercrime involves a set of measures developed and implemented by state bodies to ensure the protection of cyberspace and fight against cybercrime. It is noted that this regulation covers several key areas: 1) formation of the legal framework; 2) creation of new and improvement of existing law enforcement agencies and their units that combat cybercrime; 3) international cooperation in this area; 4) development of technical infrastructure and increasing public awareness in the field of cybercrime; 5) prevention and deterrence of cybercrime.

The research proves that state regulation in any area of public life involves the existence of a certain system of organizational and legal support, and the foundation for creating such a system is the legal regulation of public relations. It is emphasized that through legal regulation, the state has the opportunity to influence the objects of governance. Legal regulatory tools include normative and individual acts that establish rules of conduct in society and define the rights and obligations of specific participants in legal relations.

Key words: *cybersecurity, cybersecurity, cybercrime, government regulation against cybercrime, public management and administration, directions of government regulation against cybercrime.*

Вступ. Актуальність дослідження теми державного регулювання протидії кіберзлочинності обумовлена стрімким розвитком інформаційних технологій та зростанням кількості злочинів, що вчиняються у кіберпросторі. Одним із ключових факторів у боротьбі з кіберзлочинністю є ефективне державне регулювання.

Необхідність розробки і вдосконалення правових механізмів, спрямованих на протидію кіберзлочинності, є важливою задачею, адже існуючі традиційні інструменти правового захисту не можуть в повній мірі проблеми кіберпрзлочинності. Крім того, глобальний характер мережі інтернет та відсутність єдиних стандартів у цій сфері ускладнює взає-

модію між державами у питаннях боротьби з кіберзлочинністю.

Мета дослідження – проаналізувати існуючі наукові підходи до поняття «кіберзлочинність», виділити ознаки кіберзлочинності, дати визначення поняття «державне регулювання протидії кіберзлочинності», окреслити основні напрямки протидії кіберзлочинності на державному рівні.

Стан дослідження проблеми. Питання протидії кіберзлочинності досліджувалось з різних точок зору – з соціальної, економічної, точки зору адміністративного, кримінального права тощо. Ґрунтовні дослідження кіберзлочинності зроблено такими вченими, як В.М. Бутузов, В.В. Голіна, Б.М. Головкін, В.Б. Дзюндзюк, Б.В. Дзюндзюк, І.Д. Казанчук, М.О. Кравцова, О.М. Пфо, Г.М. Чернишов, В.П. Яценко та багатьма іншими. В той же час, з точки зору публічного управління та адміністрування проблеми державного регулювання протидії кіберзлочинності майже не розглядаються, що обумовлює необхідність наукових розробок в цій сфері.

Виклад основного матеріалу. Сучасний світ переживає цифрову трансформацію, що веде до появи нових загроз, пов'язаних із використанням інформаційних мереж. Кіберзлочини охоплюють широкий спектр незаконних дій, таких як несанкціонований доступ до інформаційних систем, крадіжка даних, кібер-шпигунство, атаки на критичну інфраструктуру, фінансові махінації, використання шкідливого програмного забезпечення тощо. Все це створює серйозну загрозу для національної безпеки, економіки та приватності громадян. Злочини у кіберпросторі впливають все суспільство, а в умовах воєнного стану кіберпростір стає інструментом, за допомогою якого йде вплив на суспільство, підготовка до вчинення реальних військових дій, тому питання кібербезпеки наразі є ще більш актуальним.

Одним із ключових факторів у боротьбі з кіберзлочинністю є ефективне державне регулювання. Необхідність розробки і вдосконалення механізмів, спрямованих на протидію кіберзлочинності, є важливою задачею, адже традиційні інструменти правового захисту виявляються недостатніми для вирішення проблем у кіберпросторі. Крім того, глобальний характер інтернету та відсутність чітких міжнародних стандартів ускладнює взаємодію між державами у питаннях боротьби з кіберзлочинністю.

Для того, щоб розкрити сутність державного регулювання протидії кіберзлочинності в Україні, варто проаналізувати саме поняття «кіберзлочинність».

Вважається, що термін «кіберзлочинність» вперше виник в американській науковій літературі на початку 1960-х років, в подальшому цей термін стали використовувати й в інших країнах, розуміючи під ним порушення чужих прав та інтересів стосовно автоматизованих систем обробки даних. Як зазначають В.Б. Дзюндюк та Б.В. Дзюндюк, «одним із перших кіберзлочинців є Джон Дрейпер, який в 1970-х роках за допомогою взлому телефонних мереж здійснював свою злочинну діяльність, через що й отримав прізвисько телефонного хакера» [1, с. 3]. Пізніше злочини, що полагали у взломі комп'ютерних мереж, набували більшого поширення.

Тлумачні словники, які містять поняття «кіберзлочин» або «кібезлочинність», містять схожі визначення. Так, етимологічно слово «кібезлочинність» має два кореня – «кібер» (cyber) та «злочиність». Оскільки слово «кібер» походить від грецького слова κυβερ, яке означає приставку «над», тому «кібезлочинність» в деяких випадках розуміють буквально як «надзлочинність».

У Великій українській юридичній енциклопедії під кіберзлочинністю розуміють «сукупність злочинів, що вчиняються за допомогою комп'ютерної мережі чи мережі електрозв'язку, у межах комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку, чи проти комп'ютерної системи або комп'ютерної мережі чи мережі електрозв'язку» [2, с. 207].

В науковій літературі найбільш поширеними є наступні підходи до поняття «кіберзлочинність». Г. М. Чернишов розуміє під кіберзлочинністю «явище, яке виражається у системі злочинів, вчинених у кіберпросторі з використанням та/або проти комп'ютерних даних, мереж або систем, а також інших телекомунікаційних мереж, включаючи Інтернет та технології мобільного зв'язку» [3, с. 160].

Доволі лаконічне визначення пропонує О.М. Пфо, який визначає кіберзлочинність як «незаконні дії, які здійснюються людьми, що використовують інформаційні технології для злочинних цілей» [4, с. 33].

М. О. Кравцова, в свою чергу, кіберзлочинність розглядає як «соціально-правовий феномен, що проявляється в забороненій законом про кримінальну відповідальність предметній діяльності (кримінальній активності) частини населення з використанням електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку» [5, с.12].

Доволі поширеним є підхід, за яким під кіберзлочинністю розуміють «протиправне

втручання в роботу кібернетичних систем, основною управляючою ланкою яких є комп'ютер (наприклад, спотворення інформації про стан об'єкта в каналі зворотного зв'язку, спотворення керуючого сигналу й каналу зв'язку, використання шкідливого програмного забезпечення тощо), створення та використання в злочинних цілях певної кібернетичної (комп'ютерної) системи, використання в злочинних цілях існуючих кібернетичних (комп'ютерних) систем (наприклад комп'ютерних чи телекомунікаційних мереж у шахрайстві, вимаганні тощо)» [6, с. 85].

Проаналізувавши вказані наукові підходи, можна виділити кілька ключових аспектів, що повторюються в різних підходах:

1) кіберпростір як місце вчинення злочинів, оскільки більшість визначень акцентують увагу на тому, що кіберзлочини відбуваються у віртуальному просторі, за допомогою комп'ютерних мереж, інтернету та телекомунікаційних систем;

2) використання інформаційних технологій – центральним елементом кіберзлочинів є використання комп'ютерних та інформаційних технологій для вчинення протиправних дій, як-от шахрайство, вимагання, зламування систем тощо;

3) спрямованість злочинів на інформаційні або комп'ютерні системи – наявні в науковій літературі визначення підкреслюють, що кіберзлочини можуть бути спрямовані не лише на отримання незаконної вигоди, але й на знищення, пошкодження або порушення роботи інформаційних систем;

4) кіберзлочинність як соціально-правовий феномен**,** оскільки кіберзлочинність розглядається як явище, що має соціальний та правовий вимір, оскільки зачіпає значну частину населення і потребує державного регулювання та притягнення винних до відповідальності.

Отже, можна зробити загальний висновок, що кіберзлочинність розуміють як явище, сукупність злочинів, соціально-правовий феномен, протиправне втручання в роботу кібернетичних систем, тощо.

На основі існуючих підходів можна запропонувати таке узагальнююче визначення: *кіберзлочинність* – це сукупність протиправних дій, що здійснюються у кіберпросторі з використанням інформаційних технологій і телекомунікаційних систем, спрямованих на порушення роботи комп'ютерних мереж, крадіжку або спотворення інформації, а також інші незаконні дії, що порушують законодавство і зачіпають інтереси держави, організацій або громадян.

Кіберзлочинність є особливим видом кримінальної активності, який відбувається у кіберпросторі через використання інформаційних технологій, характеризується глобальністю, анонімністю та високим рівнем автоматизації, що дозволяє впливати на велику кількість об'єктів та систем одночасно. Ефективна протидія цьому явищу вимагає вироблення єдиної державної політики і цій сфері, міжнародної співпраці, постійного оновлення технологічних засобів захисту та гнучкості правових механізмів.

Для того, щоб визначити вектор державного регулювання протидії цьому виду злочинності, варто виокремити ознаки, характерні риси кіберзлочинності. Вказане питання є доволі дискусійним, кожний науковець наводить свій перелік ознак, які, на нашу думку, потребують доповнення та удосконалення.

Так, В. М. Бутузов, виділяє такі ознаки кіберзлочинів: «1) ознакою віднесення певних злочинів у сфері високих інформаційних технологій до комп'ютерних є знаряддя вчинення злочину – комп'ютерна техніка. Причому об'єктом посягання є суспільні відносини у сфері автоматизованої обробки інформації; 2) ознакою віднесення злочинів у сфері високих інформаційних технологій до кіберзлочинів є специфічне середовище вчинення злочинів – кіберпростір (середовище комп'ютерних систем та мереж). Причому об'єктом злочинного посягання можуть бути відносини будь-якої галузі людської діяльності, що мають свій прояв у кіберпросторі» [7, с. 119].

Інший підхід пропонують правники – В.В. Голіна та Б.М. Головкін, які виокремлюють такі ознаки кіберзлочинів: «1) ці злочини вчиняються у віртуальному просторі або в межах комп'ютерних мереж. Кіберпростір – це модульований за допомогою комп'ютера кібернетичний простір, в якому містяться дані про осіб, факти, явища, процеси, представлені в математичному, символьному чи іншому вигляді. Ці відомості знаходяться в процесі руху по локальних і глобальних комп'ютерних мережах, зберігаються в пам'яті будь-якого фізичного або віртуального пристрою, спеціально призначених для їх зберігання, переробки та передачі; 2) кіберзлочини вчиняються за допомогою комп'ютерних систем або через використання комп'ютерних мереж та інших засобів доступу до кіберпростору, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних. Таким чином, електронно-обчислювана техніка може виступати як засобом вчинення злочину, так і предметом злочину» [8, с. 126].

Зарубіжні дослідники, зокрема, Сюзан В. Бреннер, пропонує свій перелік ознак

кіберзлочинів: «1) для вчинення таких злочинів не обов'язковим є фізичне зближення суб'єкта злочину та жертви; 2) через автоматизованість кількість об'єктів злочину може вимірюватись тисячами, як наслідок одного злочинного діяння; 3) кіберзлочини вчиняються «моментально», отже, для протидії ним необхідне швидке реагування правоохоронних органів; 4) відсутність сталого алгоритму вчинення дій, що призводять до протиправних наслідків, через недостатню дослідженість» [9, с. 39].

Вбачається, що вказані підходи не в повній мірі розкривають всі характерні риси кіберзлочинності, більшість підходів обмежуються лише правовим аспектом кіберзлочинності, не звертаючи уваги на соціальний характер цього виду злочинів та не враховуючи необхідності державного управління в цій сфері.

Отже, доцільно виділити такі ознаки кіберзлочинності:

1) глобальність та транснаціональність. Кіберзлочинність не знає кордонів, вчинення таких злочинів можливе в будь-якій точці світу, зловмисники можуть атакувати системи з будь-якого куточка планети. Це робить проблему кіберзлочинності особливо складною для регулювання на національному рівні;

2) Високий рівень анонімності. Кіберпростір забезпечує злочинцям високий рівень анонімності, що ускладнює їх виявлення і притягнення до відповідальності. Злочинці часто використовують засоби для приховування своїх слідів, як-от VPN, анонімні браузери або шифрування;

3) Швидка еволюція методів і технологій. Кіберзлочинність постійно удосконалюється, злочинці використовують нові технічні засоби, шкідливе програмне забезпечення і методи соціальної інженерії. Це вимагає постійної адаптації з боку правоохоронних органів і спеціалістів з кібербезпеки;

4) Висока залежність від технологічних прогалин. Багато кіберзлочинів відбуваються через вразливості в програмному забезпеченні або системах захисту. Це робить кібербезпеку особливо важливою складовою на рівні державного регулювання і корпоративної політики;

5) Широкий спектр мотивацій правопорушників. Кіберзлочинці можуть діяти не лише заради фінансової вигоди, а й з політичних, соціальних чи ідеологічних мотивів. Зокрема, такі злочини можуть включати кібершпигунство, тероризм, активізм (хактивізм), а також особисту помсту. В умовах війни для кібератак на інтернет-ресурси державних органів залучаються цілі підрозділи країни-агресора.

Проаналізувавши різні підходи до поняття кіберзлочинів та їх ознак, можна перейти до характеристики державного регулювання протидії кіберзлочинності.

Державне регулювання протидії кіберзлочинності полягає в комплексі заходів, які розробляються та впроваджуються державними органами для забезпечення захисту кіберпростору та боротьби з кіберзлочинами. Це регулювання охоплює декілька основних напрямків: 1) формування нормативно-правової бази; 2) створення нових та удосконалення роботи існуючих правоохоронних органів та їх підрозділів, які ведуть боротьбу із кіберзлочинністю; 3) міжнародна співпраця в цій сфері; 4) розвиток технічної інфраструктури та підвищення обізнаності суспільства у сфері кіберзлочинності; 5) попередження та профілактика кіберзлочинності. Кожний із цих напрямів потребує детального аналізу.

Формування нормативно-правової бази. Нормативно-правове регулювання протидії кіберзлочинності, формування законодавчої бази в цій сфері є необхідним для єдиного розуміння сутності, характерних рис кіберзлочинів, а також створення умов для невідворотності покарання за кіберзлочини. Для ефективної боротьби з кіберзлочинністю важливим є наявність низки законів та інших нормативних актів, які присвячені безпосередньо кіберзлочинності і які регулюють питання кібербезпеки та відповідальність за вчинення кіберзлочинів. До таких законодавчих актів належать закони про захист інформації, персональних даних, а також правові норми, які визначають відповідальність за кіберзлочини на національному рівні. Крім того, розвинені країни співпрацюють для гармонізації свого законодавств у відповідності до міжнародних стандартів, такими як Будапештська конвенція про кіберзлочинність тощо. Не менш важливим є адаптація існуючих правових норм до нових викликів цифрової ери. Необхідно, щоб правові акти, які приймаються в Україні, враховували специфіку кіберзлочинів, що відрізняються від традиційних злочинів за своєю природою та способами вчинення.

Державне регулювання в будь-якій сфері суспільного життя передбачає існування певної системи організаційно-правового забезпечення. Основою для створення цієї системи є правове регулювання суспільнихї відносин. Завдяки правовому регулюванню держава має можливість здійснювати вплив на об'єкти управління. До таких засобів правового регулювання належать нормативні та індивідуальні акти, які встановлюють правила поведінки в суспільстві та визначають права й обов'язки конкретних учасників правовідносин.

Створення нових та удосконалення роботи існуючих правоохоронних органів та їх підрозділів, які ведуть боротьбу із кіберзлочинністю. Для боротьби із кіберзлочинністю замало тільки правових норм, необхідним є створення та підтримка роботи спеціалізованих державних органів**,** що ведуть боротьбу із кіберзлочинністю. У багатьох країнах існують спеціальні підрозділи в правоохоронних органах, які займаються розслідуванням кіберзлочинів. Ці підрозділи мають спеціальні технічні та аналітичні інструменти для відстеження, виявлення та ліквідації загроз у кіберпросторі. Зокрема, в Україні функціонує Департамент кіберполіції Національної поліції України, який є міжрегіональним територіальним підрозділом Національної поліції України, що входить до структури кримінальної поліції Національної поліції та згідно із законодавством України здійснює оперативно-розшукову діяльність [10].

Основними завданнями Департаменту кіберполіції є: 1) участь у формуванні та забезпеченні реалізації державної політики у сфері протидії кіберзлочинності щодо попередження і протидії кримінальним правопорушенням, механізм підготовки, учинення або приховування яких передбачає використання електроннообчислювальних машин (комп'ютерів), систем і комп'ютерних мереж і мереж електрозв'язку; 2) сприяння у порядку, передбаченому чинним законодавством, іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень у сфері інформаційної безпеки, використання платіжних систем, електронної комерції та господарської діяльності; 3) завчасне інформування населення про появу новітніх кіберзлочинів; 4) упровадження 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 країнами світу [10]. На офіційному сайті Департаменту кіберполіції визначено такі пріоритетні напрями роботи цього підрозділу: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах національної цілодобової мережі контактних пунктів. Вбачається, що існуючі завдання кіберполіції потребують свого перегляду та удосконалення з урахуванням виникнення нових видів кіберзлочинів та способів їх вчинення.

Варто погодитись із І.Д. Казанчук та В.П. Яценко, які в своєму дослідженні окреслили такі «пріоритетні напрямки, за якими повинно відбуватись вдосконалення правових засад організації та діяльності підрозділів кіберполіції Національної поліції у сфері забезпечення інформаційної безпеки та протидії кіберзагрозам: 1) оптимізація організаційної структури кіберполіції, у процесі якої особлива увага повинна приділятися визначенню базових вимог до їх діяльності, на основі чого вже повинні формулюватися конкретні функції; 2) обґрунтований розподіл функцій (повноважень) між підрозділами кіберполіції та іншими суб'єктами протидії кіберзагрозам в Україні, створення належних умов для виходу на якісний новий рівень взаємодії між ними та координації їх діяльності у сфері забезпечення інформаційної безпеки; 3) запровадження нових підходів до формування переліку організаційно-правових форм і методів взаємодії всіх суб'єктів протидії правопорушенням в інформаційній сфері та підвищення контролю за якістю їх реалізації; 4) запровадження сучасних механізмів аналітичного і матеріально-технічного забезпечення діяльності кіберполіції, покращення системи заходів, спрямованих на підвищення рівня професіоналізму кіберполіцейських» [11, с. 37].

Крім того, важливою є міжвідомча взаємодія між різними державними органами, такими як міністерства, спецслужби, суди та поліція, для ефективної координації заходів із протидії кіберзлочинності. Для ефективної протидії кіберзлочинності доцільним є створення Центрів кібербезпеки, які можуть виконувати координаційну функцію між державними установами, бізнесом і громадянським суспільством, а також забезпечувати моніторинг і оперативне реагування на кіберзагрози.

Міжнародна співпраця у сфері кіберзлочинності. Ще одним важливим напрямком державного регулювання протидії кіберзлочинності є посилення міжнародної співпраці в цій сфері. Оскільки кіберзлочинність має глобальний характер, держави зобов'язані посилювати співпрацю на міжнародному рівні. Така міжнародна взаємодія включає обмін інформацією, участь у міжнародних угодах, співпрацю з міжнародними правоохоронними організаціями (наприклад, Інтерполом) та спільні операції проти кіберзлочинців. Ефективне міжнародне

співробітництво є критично важливим для успішного переслідування кіберзлочинців, які часто діють поза межами окремих країн.

Варто підкреслити, що кіберзлочинність не є проблемою окремих країн, вона носить транснаціональний характер. Саме тому необхідною є гармонізація міжнародного та національного законодавства у сфері кіберзлочинності, внесенням відповідних змін у кримінальне та кримінальне процесуальне законодавство України, оскільки під час досудового розслідування кіберзлочинів і судового розгляду справ виникають проблеми, зокрема, при оцінці судом електронних доказів тощо. Так, наприклад, Генеральна Асамблея Організації Об'єднаних Націй у своїй резолюції A/73/PV.56 від 17.12.2018 року рекомендувала державам-членам активізувати їх зусилля у боротьбі з кіберзлочинністю і злочинним використанням інформаційних і комунікаційних технологій у всіх його формах та розвивати міжнародне співробітництво в цій сфері, включаючи обмін електронними доказами [12].

Міжнародне співтовариство приділяє значну увагу питанням захисту від кіберзагроз. Останнім часом багато вчених, політиків, глави держав акцентують велику увагу на цій проблемі. Міжнародне співтовариство активно бореться з подоланням даного виду злочинності та розвитком інтерактивного міжнародного захисту від неї. Особливість кіберзлочинності в тому, що вказані злочини часто є міжнародними, тобто злочинці діють у одній державі, в той час як які жертви перебувають у іншій державі. Правоохоронні органи однієї держави не можуть ефективно здійснювати досудове розслідування злочинів, що вчиняються у кіберпросторі, коли злочинці, а також ключові докази знаходяться поза межами їх юрисдикції. В цьому випадку для боротьби з такими злочинами особливе значення має міжнародне співробітництво. Вкрай важливо, щоб в тій країні, до якої направляється запит про екстрадицію або про правову допомогу в розслідувані вказаного кримінального правопорушення, вказане діяння також кваліфікувалось як злочин. Отже, питання гармонізації кримінального законодавства різних країн у цій сфері є вкрай актуальним.

Для подолання проблем, що пов'язані із транснаціональним характером кіберзлочинів, важливо розвивати одночасно два напрями – офіційне міжнародне співробітництво та неформальне міжнародне співробітництво. Офіційне міжнародне співробітництво передбачає укладення багатосторонніх договорів про кіберзлочинність, договорів про взаємодопомогу та екстрадицію. Неформальне міжнародне співробітництво може включати в себе різні форми співробітництва та взаємодії, що зазвичай носять більш практичний та особистий характер та реалізуються на оперативному рівні між органами виконавчої влади.

Розвиток технічної інфраструктури та підвищення обізнаності. Кожна держава повинна інвестувати у розвиток кібербезпекової інфраструктури, що включає як технологічні інструменти для захисту критичних інформаційних систем, так і освітні програми для підвищення рівня обізнаності громадян та компаній щодо кіберзагроз. У межах цих ініціатив держава може проводити інформаційні кампанії, навчання для фахівців та створювати платформи для обміну знаннями між державним та приватним секторами.

Інвестування в дослідження та розробки у сфері кіберзахисту, включаючи розробку нових методів шифрування, системи виявлення вторгнень, аналіз даних для виявлення потенційних загроз тощо. Вказані інвестиції в подальшому допоможуть заощадити значні суми коштів.

Публічно-приватне партнерство є не менш важливим. Співпраця держави та приватного сектору є важливою, оскільки компанії володіють значними ресурсами і передовими технологіями, необхідними для боротьби з кіберзлочинами. Держава може стимулювати впровадження кіберзахисту у бізнес-середовище через надання податкових пільг або інших стимулів.

Ще одним кроком у цьому напрямку є контроль за діяльністю приватних компаній. Державні органи можуть впроваджувати регуляторні механізми, які вимагають від приватних організацій дотримуватися стандартів кібербезпеки. Це може включати обов'язкові вимоги до захисту персональних даних, створення інцидентних команд для швидкого реагування на кібератаки та обов'язкову звітність щодо інцидентів у сфері кібербезпеки.

Попередження та профілактика кіберзлочинності. Попередження та профілактика кіберзлочинності є важливою складовою державного регулювання у сфері кібербезпеки. Цей напрямок включає низку заходів, що спрямовані на зменшення кількості кіберзлочинів та мінімізацію ризиків, пов'язаних з ними. В першу чергу, необхідним є проведення інформаційно-освітніх кампаній, оскільки держава повинна сприяти підвищенню обізнаності населення та бізнесу про кіберзагрози, методи захисту інформації та правила кібергігієни. Ці інформаційні кампанії включають поширення інформації про види кіберзлочинів, їхні можливі наслідки та способи захисту. Важливо

навчати суспільство базовим правилам кібергігієни, таким як використання складних паролів, регулярне оновлення програмного забезпечення та обережність під час використання мережі Інтернет. Представникам бізнесу слід приділяти особливу увагу навчальним тренінгам щодо запобігання фішинговим атакам, витокам даних та методам реагування на кібератаки. Освітні програми повинні охоплювати всі вікові групи та професійні сфери.

Другий важливий крок в профілактиці кіберзлочинності – це захист критичної інфраструктури**.** Держава зобов'язана забезпечувати безпеку найважливіших об'єктів інфраструктури, таких як енергетичні компанії, банки, транспортні системи та державні органи, оскільки їхня робота є важливою для стабільного функціонування суспільства. Одним із завдань є впровадження національних стандартів кібербезпеки, які регламентують захист інформаційних систем цих об'єктів від кібератак. Крім того, важливо розробляти та впроваджувати сучасні технології, що унеможливлюють або ускладнюють здійснення атак на такі системи. Це включає в себе не лише фізичний захист серверів, але й постійний моніторинг кіберпростору для виявлення потенційних загроз.

Ще один крок для протидії кіберзлочинності – це аудит та моніторинг інформаційних систем. Державні та приватні організації повинні регулярно перевіряти свої інформаційні системи на наявність вразливостей. Це досягається через проведення аудитів, у ході яких експерти з кібербезпеки аналізують можливі слабкі місця систем і пропонують заходи для їх усунення. Особливу увагу потрібно звертати на оновлення систем захисту, оскільки технології швидко розвиваються, і нові кіберзагрози виникають постійно. Моніторинг мережі організацій дозволяє вчасно виявляти та нейтралізувати загрози до того, як вони перероструть у серйозні інциденти. Важливим інструментом є впровадження системи управління інформаційною безпекою (СУІБ), яка допомагає організаціям ефективніше реагувати на інциденти.

Для профілактики кіберзлочинності важливу роль відіграють превентивні заходи на державному рівні. Держава повинна не лише впроваджувати законодавчі норми, але й розробляти превентивні стратегії, спрямовані на зниження ризику кіберзлочинів. Це включає розробку систем раннього виявлення загроз, побудову кіберрозвідки та тісну співпрацю з міжнародними організаціями для обміну інформацією про кіберзагрози.

Профілактика кіберзлочинності є багатокомпонентним процесом, який вимагає залучення широкого спектра інструментів, від освітніх кампаній до високотехнологічних рішень для захисту критичної інфраструктури. Це забезпечує більш комплексний підхід до зменшення ризику кіберзлочинів та підвищення рівня кібербезпеки в державі.

Висновки. Під кіберзлочинністю слід розуміти сукупність протиправних дій, що здійснюються у кіберпросторі з використанням інформаційних технологій і телекомунікаційних систем, спрямованих на порушення роботи комп'ютерних мереж, крадіжку або спотворення інформації, а також інші незаконні дії, що порушують законодавство і зачіпають інтереси держави, організацій або громадян. На основі існуючих правових підходів було виокремлено такі ознаки кіберзлочинності: 1) глобальність та транснаціональність; 2) високий рівень анонімності; 3) швидка еволюція методів і технологій**,** 4) висока залежність від технологічних прогалин; 5) широкий спектр мотивацій правопорушників. В ході дослідження було розроблено таке визначення: державне регулювання протидії кіберзлочинності – це система правових, організаційних та технічних заходів, що реалізуються державними органами з метою попередження, виявлення, розслідування та усунення наслідків кіберзлочинів. Було зроблено висновок, що державне регулювання протидії кіберзлочинності полягає в комплексі заходів, які розробляються та впроваджуються державними органами для забезпечення захисту кіберпростору та боротьби з кіберзлочинами. Це регулювання охоплює декілька основних напрямків: 1) формування нормативно-правової бази; 2) створення нових та удосконалення роботи існуючих правоохоронних органів та їх підрозділів, які ведуть боротьбу із кіберзлочинністю; 3) міжнародна співпраця в цій сфері; 4) розвиток технічної інфраструктури та підвищення обізнаності суспільства у сфері кіберзлочинності; 5) попередження та профілактика кіберзлочинності.

Отже, державне регулювання протидії кіберзлочинності має на меті створення безпечного кіберпростору через правові, технічні та організаційні заходи, забезпечуючи захист держави, бізнесу та громадян від загроз у кіберпросторі. Державне регулювання протидії кіберзлочинності є багаторівневим процесом, що охоплює правове, адміністративне, технологічне та міжнародне співробітництво. Воно включає не лише розробку правових норм і забезпечення їх виконання, але й постійне вдосконалення технологій кіберзахисту, розвиток профілактичних заходів і тісну взаємодію з іншими країнами. Держава повинна виступати

лідером у створенні надійної системи захисту інформаційних систем та у боротьбі з новими загрозами у цифровому світі.

ЛІТЕРАТУРА:

1. Дзюндзюк В.Б., Дзюндзюк Б.В. Поява і розвиток кіберзлочинності. *Державне будівництво.* 2013. № 1. С. 1–12. URL: http://www.irbis-nbuv.gov.ua/cgi-bin/irbis_nbuv/cgiirbis_64.exe?I21DBN=LINK&P21DBN=UJRN&Z21ID=&S21REF=10&S21CNR=20&S21STN=1&S21FMT=ASP_meta&C21COM=S&2_S21P03=FILA=&2_S21STR=DeBu_2013_1_3

2. Бабанін С. В. Кіберзлочинність, Комп'ютерна злочинність. Велика українська юридична енциклопедія : у 20 т. Харків, 2019. Том 18. 544 с.

3. Чернишов Г. М. Кіберзлочинність як виклик глобалізації та загроза світовій безпеці: теоретичні основи дослідження. *Прикарпатський юридичний вісник.* 2018. № 3. С. 158-162. URL: http://www.pjv.nuoua.od.ua/v3_2018/34.pdf

4. Пфо О. М. Основні поняття і класифікація кіберзлочинності. *Актуальні задачі та досягнення у галузі кібербезпеки : матеріали Всеукр. наук.-практ. конф., м. Кропивницький, 23-25 листоп. 2016 р*. Кропивницький : КНТУ, 2016. С. 33-34.

5. Кравцова М. О. Кіберзлочинність: кримінологічна характеристика та запобігання органами внутрішніх справ : автореф. дис. … канд. юрид. наук: 12.00.08. Харків, 2016. 16 с.

6. Словник термінів з кібербезпеки: за заг. ред. О. Копана, Є. Скулиша. К. : ВБ «Аванпост-Прим», 2012. 214 с.

7. Бутузов В. Протидія комп'ютерній злочинності в Україні (системно-структурний аналіз) : [монографія]. В. Бутузов. К. : КИТ, 2010. 148 с.

8. Голіна В.В., Головкін Б.М. Кримінологія: Загальна та Особлива частини Навчальний посібник. Х.: Право, 2014. 513 с.

9. Susan W. Brenner. Criminal Threats from Cyberspace. *Greenwood publishing group.* 2010. 281 p. URL: https://api.pageplace.de/preview/DT0400.9780313365478_A23550603/preview-9780313365478_A23550603.pdf

10. Про затвердження Положення про Департамент кіберполіції Національної поліції України: Наказ Національної поліції України від 10.11.2015 № 85 (в редакції наказу Національної поліції України від 07.11.2019 № 1136).

11. Казанчук І.Д., Яценко В.П. Особливості правового регулювання діяльності Національної поліції України у сфері забезпечення інформаційної безпеки в Україні. *Право і безпека.* 2020. № 4 (79). С. 32-38. URL: https://dspace.univd.edu.ua/items/fe1ce6f4-19c6-474b-8902-d1e9fce1910e

12. Протидія використанню інформаційно-комунікаційних технологій у злочинних цілях. Резолюція Генеральної Асамблея Організації Об'єднаних Націй A/73/PV.56 від 17.12.2018 року. URL: https://documents.un.org/doc/undoc/gen/n18/450/53/pdf/n1845053.pdf