КЛАСИЧНИЙ ПРИВАТНИЙ УНІВЕРСИТЕТ

ПВНЗ УНІВЕРСИТЕТ КОРОЛЯ ДАНИЛА

Кваліфікаційна наукова
праця на правах рукопису

БУЯДЖИ СЕРГІЙ АНАТОЛІЙОВИЧ

УДК 349.22

ДИСЕРТАЦІЯ

ПРАВОВЕ РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ: ТЕОРЕТИКО-ПРАВОВИЙ АСПЕКТ

12.00.01 – теорія та історія держави і права;

історія політичних і правових учень

Подається на здобуття наукового ступеня кандидата юридичних наук
(доктора філософії)

Дисертація містить результати власних досліджень. Використання ідей, результатів і текстів інших авторів мають посилання на відповідне джерело

_____

(підпис, ініціали та прізвище здобувача)

Науковий керівник –

кандидат юридичних наук, доцент
Дурнов Євген Сергійович

Київ – 2018

АНОТАЦІЯ

Буяджи С.А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект. – Кваліфікаційна наукова праця на правах рукопису.

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.01 – теорія та історія держави і права; історія політичних і правових учень. – Приватний вищий навчальний заклад Університет Короля Данила, Івано-Франківськ, 2018.

Дисертація присвячена системному та ґрунтовному аналізу особливостей теоретико-правового аспекту правового регулювання боротьби з кіберзлочинністю. У роботі визначено поняття, значення та наведено ознаки боротьби з кіберзлочинністю. Простежено генезис правового регулювання боротьби з кіберзлочинністю. Окрему увагу приділено аналізу елементів механізму правового регулювання боротьби з кіберзлочинністю.

З'ясовано, що стрімке впровадження нових технологій у галузях електроніки, комунікаційних та цифрових технологій наприкінці XX – на початку XXI століття спричинило появу нових суспільних відносин та відповідних проблем, пов'язаних із прагненням людства до розвитку, полегшення праці та покращення умов життєдіяльності. Найбільшого значення у даному процесі набула технологія Інтернет, яка надала фактично безмежні можливості у передачі, поширенні та отриманні інформації, комунікації, виконанні низки дій, незалежно від часу та місця перебування особи. Разом із тим, відкриття нових горизонтів для світового співтовариства нерозривно пов'язане із появою нових форм злочинної діяльності та іншими проявами недобросовісного використання досягнень науково-технічного прогресу.

Встановлено, що міжнародна співпраця у боротьбі з кіберзлочинністю здійснюється в наступних напрямках:

1) прийняття міжнародно-правових механізмів регулювання та взаємодії правоохоронних органів у питаннях боротьби із кіберзлочинністю;

2) гармонізація національних законодавств із міжнародним законодавством;

3) безпосередня співпраця, як офіційна, так і неофіційна;

4) узгодження повноважень при здійсненні боротьби із кіберзлочинністю.

Генезис правового регулювання боротьби з кіберзлочинністю в світі етапізований наступним чином:

1) Етап зародження правового регулювання боротьби з кіберзлочинністю (1986 рік – 1989 рік) – від прийняття першого в історії комп'ютерного закону, до прийняття Рекомендації № R(89)9, яка мала ключове значення для подальшого розвитку законодавства, спрямованого на боротьбу з кіберзлочинністю та виступила у якості поштовху для еволюції кримінального законодавства європейських країн;

2) Етап внесення змін до кримінального законодавства європейських країн (1989 - 2000 рік) - після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день, а кінцевий термін даного періоду ми умовно пов'язуємо із 2000 роком, після якого подальші зміни до національних законодавств уже не характеризувались масовим характером;

3) Етап консолідації європейської спільноти для боротьби із кіберзлочинністю (2000 рік – 2001 рік) - на протязі двох років у міжнародно-правовому законодавстві з'явився ряд актів, які значною мірою мали вплив на боротьбу із кіберзлочинністю. Саме тому даний етап хронологічно обмежений лише двома роками;

4) Сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 рік – наші дні) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, які перебувають на нижчих рівнях розвитку.

Досліджено національне та міжнародно-правове регулювання боротьби з кіберзлочинністю. Визначено перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Розкрито специфіку правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах.

У рамках тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні запропоновано виділено наступні підтенденції:

1) розширення меж розуміння поняття кіберзлочинність;

2) посилення кримінальної відповідальності за вчинення кіберзлочинів;

3) термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання, єдиного термінологічного апарату.

Щодо тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні основними підтенденціями є:

1) ратифікація окремих міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю, які на сьогодні ще не є джерелом вітчизняного права;

2) укладення міжнародних двосторонніх чи багатосторонніх угод з іншими державами;

3) правова допомога іншим державам у питаннях боротьби із кіберзлочинністю;

4) втілення міжнародних стандартів у нормах вітчизняного законодавства.

В тенденції збільшення рівня контролю за користувачами мережі Інтернет виділено наступні підтенденції:

1) встановлення правил користування громадянами кіберпростором;

2) створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором.

Ключові слова: законодавство, правове регулювання, кіберзлочинність, боротьба з кіберзлочинністю, правовий механізм, злочини у кіберпросторі, генезис, Інтернет.

ANNOTATION

Buyagi S.A. Legal regulation of the fight against cybercrime: the theoretical and legal aspect. – The qualifying scientific work on the rights of the manuscript.

The thesis for the degree of Candidate of Sciences, specialty 12.00.01 – theory and history of state and law; history of political and legal studies. – Private higher educational institution King Danylo University, Ivano-Frankivsk, 2018.

The dissertation is devoted to the systematic and thorough analysis of the peculiarities of the theoretical and legal aspect of the legal regulation of the fight against cybercrime. The work defines the concept, meaning and features of the fight against cybercrime. The genesis of legal regulation of the fight against cybercrime is traced. Particular attention is paid to the analysis of elements of the mechanism of legal regulation of combating cybercrime.

It was found that the rapid introduction of new technologies in the fields of electronics, communications and digital technologies at the end of the 20th - the beginning of the 21st century led to the emergence of new social relations and related problems related to the aspiration of mankind for development, labor facilitation and improvement of living conditions. Internet technology, which has virtually endless possibilities for the transmission, distribution and reception of information, communication, and execution of a number of actions, regardless of the time and place of the person, became the most important in this process. At the same time, the opening of new horizons for the world community is inextricably linked with the emergence of new forms of criminal activity and other manifestations of unfair use of scientific and technological progress.

It was established that international cooperation in the fight against cyber crime is carried out in the following directions:

1) adoption of international legal mechanisms for regulation and interaction of law enforcement agencies in the fight against cybercrime;

2) harmonization of national legislation with international law;

3) direct cooperation, both official and informal;

4) coordination of powers in the implementation of the fight against cybercrime.

The genesis of legal regulation of the fight against cybercrime in the world has been phased out as follows:

1) The stage of the birth of the legal regulation of the fight against cybercrime (1986 - 1989) - from the adoption of the first ever computer law, prior to the adoption of Recommendation No. R (89) 9, which was key to the further development of legislation aimed at combating cybercrime and acted as a push for the evolution of the criminal legislation of European countries;

2) The stage of amending the criminal law of European countries (1989-2000) - after 1989, the rapid evolution of the criminal law of European states in the part of the strengthening of the fight against computer crimes began, which to some extent continues to this day, and the deadline we relentably relate this period to the year 2000, after which further changes to national laws were no longer characterized by mass character;

3) Stage of consolidation of the European community for combating cybercrime (2000 - 2001) - within two years in the international legal legislation a number of acts appeared, which to a large extent influenced the fight against cybercrime. That is why this stage is chronologically limited to only two years;

4) The current stage of legal regulation of the fight against cybercrime (2001 - our days) - is characterized by the process of improving the legislation on cybercrime of states that are at lower levels of development.

The national and international legal regulation of struggle against cybercrime is investigated. The prospects and trends of the legal regulation of the fight against

cyber crime in Ukraine are determined. The specifics of legal regulation of the fight against cybercrime in foreign countries are revealed.

Within the framework of the development trend of the domestic normative legal and terminology base in the field of combating cybercrime in Ukraine, the following sub-targets were identified:

1) widening the boundaries of understanding the concept of cybercrime;

2) increasing the criminal liability for committing cybercrime;

3) terminological harmonization in the norms of all regulatory legal acts regulating this issue, a single terminology apparatus.

Regarding the tendency of strengthening international cooperation in the field of combating cybercrime in Ukraine, the main subtensions are:

1) ratification of certain international legal acts in the field of combating cybercrime, which for today are not yet a source of domestic law;

2) the conclusion of international bilateral or multilateral agreements with other states;

3) legal assistance to other states in the fight against cybercrime;

4) the implementation of international standards in the norms of domestic legislation.

In the tendency to increase the level of control over users of the Internet allocated the following sub-tensions:

1) the establishment of rules for the use of citizens by cyberspace;

2) the creation of special control bodies designed to observe and detect violators of the established rules for the use of cyberspace.

Keywords: legislation, legal regulation, cybercrime, fight against cybercrime, legal mechanism, crimes in cyberspace, genesis, Internet.

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Буяджи С.А. Генезис правового регулювання боротьби з кіберзлочинністю в світі. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2014. № 29, ч. 2. Т. 4/2. С. 145-149.

2. Буяджи С.А. Поняття боротьби з кіберзлочинністю. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки».* 2015. № 3-2, Т. 4. С. 53-57.

3. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. *Право України.* 2017. № 9. С. 245-251.

4. Буяджи С.А. Тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія".* 2017. № 2. С. 21-32.

5. Буяджи С.А. Особливості правового регулювання боротьби із кіберзлочинністю у США. *Lex Portus: юридичний науковий журнал.* 2017. № 2 (4). С. 130-142.

6. Буяджи С.А. Положительный опыт правового регулирования борьбы с киберпреступностью в странах ЕС. *Evropsky politicky a pravni diskurz, svazeky, 4 vydani 2017. European political and law discourse.* Volume 4. Issue 4. 2017. P. 41-46.

7. Буяджи С.А. Теоретико-правова характеристика боротьби з кіберзлочинністю. *Актуальні проблеми сучасного правознавства: Матеріали міжнародної науково-практичної конференції (м. Київ, 28-29 січня 2016 р.).* К.: «Науково-дослідний інститут публічного права», 2016. С. 19-22.

8. Буяджи С.А. Структура механізму правового регулювання боротьби з кіберзлочинністю. *Реформування національного та міжнародного права: перспективи та пріоритети: матеріали міжнародної науково-практичної конференції (м. Одеса, 20-21 січня 2017 р.).* Одеса: ГО «Причорноморська фундація права», 2017. С. 34-36.

9. Буяджи С.А. Національне правове регулювання боротьби з кіберзлочинністю. *Актуальні проблеми реформування системи законодавства України: матеріали міжнародної науково-практичної конференції (м. Запоріжжя, 27-28 січня 2017 р.).* Запоріжжя: Запорізька міська громадська організація «Істина», 2017. С. 29-31.

ЗМІСТ

ВСТУП

Кіберзлочинність не є традиційним злочином, а відносно молодим явищем, яке пов’язується із появою та поширенням глобальної мережі Інтернет. Із самого моменту виникнення даний вид злочинності проявив себе зручним для зловмисників. Особлива природа Всесвітньої мережі забезпечила глобальність та анонімність для її користувачів, що безсумнівно постало у якості передумов для появи даного виду злочинності. У свою чергу із поширенням кіберзлочинів пов’язано виникнення потреби правового регулювання цього питання як у світі, так і в Україні.

Протидія будь-якому негативному впливу вимагає формування розуміння сутності проблеми та знання її генезису. Оскільки швидкість розвитку суспільства нерозривно пов’язана з досягненнями науково-технічного прогресу та злочинними проявами, важливим є також звернення до питання історичного розвитку впровадження правових механізмів для боротьби з кіберзлочинністю в світі та Україні.

Збільшення кількості кіберзагроз в нашій державі все актуальнішим робить питання оптимізації правового регулювання даної сфери. В світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності. Окрім того, в сучасних умовах важливою є готовність приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях.

Постійний розвиток правового регулювання боротьби з кіберзлочинністю в Україні є важливим з огляду на наступні фактори. По-перше, на сьогодні практично усі державні та недержавні процеси відбуваються із застосуванням інструментів кіберспростору. По-друге, в умовах неоголошеної війни, у якій вимушена приймати участь Україна, віртуальний простір є одним із фронтів, у якому наша держава має слабкі показники. По-третє, рівень усвідомлення загрози кіберзлочинів та їх

небезпечності у суспільстві все ще є невисоким. За таких умов проблема перспектив правового регулювання боротьби з кіберзлочинністю в Україні є однією із першочергових для наукового дослідження з метою забезпечення належних змін на практиці.

Питання правового регулювання боротьби із кіберзлочинністю розглядали такі видатні вчені, як Дж. Арас, О.О. Баєв, Г.Р. Бєляков, Дж. Блумбекер, В.Л. Бурячок, В.М. Бутузов, Г.П. Власова, В.Я. Вовк, А.В. Войціховський, В.Д. Гавловський, Р.Є. Джансараєва, В.Б. Дзюндзюк, Д.В. Дубов, О.Є. Користін, М.О. Кравцова, М.Ю. Літвінов, Р.В. Лук'янчук, О.В. Манжай, В.В. Марков, М.А. Ожеван, Ю.М. Онищенко, О.В. Орлов, А.А. Протасевич, П.І. Пушкаренко, К.М. Рудой, Є.Д. Скулиш, В.Г. Хахановський, В.В. Чернєй та інші. Варто зазначити, що практично більшість науковців у тій чи іншій мірі досліджували проблематику правового регулювання боротьби із кіберзлочинністю в різних аспектах, однак ними не було досліджено комплексно саме ретроспективний аналіз даного правового явища, тенденцій розвитку та механізму правового регулювання боротьби із кіберзлочинністю. В умовах сьогодення цей напрям науки теорії та історії держави і права набуває особливої актуальності.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана відповідно до науково-дослідної роботи Класичного приватного університету «Актуальні проблеми історії, теорії та філософії держави і права» (номер державної реєстрації 0112U008379). Особистим внеском автора є дослідження генезису правового регулювання боротьби із кіберзлочинністю у світі та в Україні, визначення тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні, розробка пропозицій щодо удосконалення національного правового регулювання боротьби з кіберзлочинністю. Тема роботи відповідає Пріоритетним напрямам розвитку правової науки на 2016–2020 рр., затвердженим постановою Загальних Зборів Національної академії правових наук України від 03.03.2016 р., та перспективним напрямам кандидатських і докторських

дисертацій за юридичними спеціальностями, перелік яких затверджено рішенням Президії Національної академії правових наук України від 18.10.2013 р.

Мета і задачі дослідження. *Метою* дослідження є розробка концептуального розуміння специфіки генезису та тенденцій розвитку і механізму правового регулювання боротьби із кіберзлочинністю.

Для досягнення зазначеної мети поставлено такі *задачі:*

– визначити правову природу боротьби із кіберзлочинністю;

– дослідити генезис правового регулювання боротьби із кіберзлочинністю;

– охарактеризувати структуру механізму правового регулювання боротьби з кіберзлочинністю;

– розкрити та конкретизувати досвід міжнародно-правового регулювання боротьби з кіберзлочинністю;

– з'ясувати специфіку національного правового регулювання боротьби з кіберзлочинністю;

– виокремити тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні;

– виділити особливості правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах.

Об'єкт дослідження – система суспільних відносин у сфері правового регулювання боротьби із злочинністю.

Предмет дослідження – теоретико-правові засади правового регулювання боротьби із кіберзлочинністю.

Методи дослідження. Положення, висновки та рекомендації, що містяться у роботі, достатньою мірою аргументовані, науково обґрунтовані і достовірні. Наукове дослідження побудовано на застосуванні загального системно-структурного методу, основні елементи якого забезпечили високий ефект побудови моделей розв'язання поставлених задач. В основі системи методології наукового аналізу генезису та тенденцій розвитку і механізму

правового регулювання боротьби із кіберзлочинністю лежать наступні методи: діалектичний метод – дає змогу досліджувати внутрішню сутність речей в процесі їх розвитку, а також внутрішніх та зовнішніх суперечностей, зокрема, за допомогою даного методу проаналізовано генезис правового регулювання боротьби із кіберзлочинністю (підрозділ 1.1); історичний метод – сприяє розумінню генезису правового регулювання боротьби із кіберзлочинністю (підрозділ 1.2); системний метод – дозволив здійснити повне та об'єктивне дослідження відповідного конкретно окресленого предмету, зокрема, дав змогу дослідити структуру механізму правового регулювання боротьби з кіберзлочинністю, а також з'ясувати специфіку міжнародного та національного правового регулювання боротьби з кіберзлочинністю (підрозділи 2.1, 2.2, 2.3); порівняльно-правовий метод – використано для аналізу особливостей правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах (підрозділ 3.2); логічні методи і прийоми – дедукція, індукція, аналогія, аналіз, синтез простежуються впродовж здійснення усього наукового аналізу. У науковому дослідженні використовувалися й інші методи пізнання, наприклад, за допомогою логіко-семантичного методу поглиблено понятійний апарат в означеній сфері, зокрема, визначено такі поняття: «боротьба із злочинністю», «кіберзлочини», «боротьба із кіберзлочинністю», «механізм правового регулювання боротьби з кіберзлочинністю» (підрозділи 1.1, 2.1). Застосування структурно-логічного методу та моделювання дозволили виділити перспективи та тенденції розвитку правового регулювання боротьби із кіберзлочинністю (підрозділ 3.1).

Нормативною основою роботи слугують нормативно-правові акти національного законодавства радянського та сучасного періодів, проекти законів й інших нормативних документів. У науковій роботі широко використано нормативно-правову базу ряду зарубіжних країн у зазначеній сфері.

Наукова новизна одержаних результатів полягає в тому, що дисертація є першою спробою комплексно, з використанням сучасних методів пізнання, з урахуванням новітніх досягнень науки теорії та історії держави і права дослідити ретроспективу і тенденції розвитку, а також механізм правового регулювання боротьби із кіберзлочинністю. За результатами дисертаційного дослідження сформульовано авторські основні положення, що виносяться на захист і які містять елементи наукової новизни, зокрема:

уперше:

– науково обґрунтовано поняття «механізм правового регулювання боротьби з кіберзлочинністю» як чітко визначену й організовану систему юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю;

– розкрито детально зміст ознак правового регулювання боротьби із кіберзлочинністю у Європейському Союзі, якими є наступні: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну;

удосконалено:

– характеристику підтенденцій тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні, якими є наступні: 1) ратифікація окремих міжнародних нормативно-правових актів у

сфері боротьби з кіберзлочинністю, які на сьогодні ще не є джерелом вітчизняного права; 2) укладення міжнародних двосторонніх чи багатосторонніх угод з іншими державами; 3) правова допомога іншим державам у питаннях боротьби із кіберзлочинністю; 4) втілення міжнародних стандартів у нормах вітчизняного законодавства;

– аналіз особливостей правового регулювання боротьби із кіберзлочинністю у Франції, до яких віднесено такі: 1) суттєва роль держави у регулюванні суспільних відносин в Інтернеті; 2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів; 3) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз; 4) існування двостороннього діалогу із громадянами та належне роз'яснення їх прав і обов'язків як користувачів Інтернету, надання інструкцій; 5) встановлення курсу на вільне співробітництво із іншими державами шляхом надання доступу до власних кібермереж у разі вчинення на території Франції кіберзлочинів;

– характеристику ознак правового регулювання боротьби із кіберзлочинністю у Білорусії, якими є наступні: 1) наявність спеціального органу із значним досвідом протистояння кіберзлочинності; 2) перелік повноважень даного органу є значно ширшим, ніж у Департаменту кіберполіції Національної поліції України; 3) невелика кількість нормативно-правових актів у сфері правового регулювання боротьби із кіберзлочинністю; 4) встановлення співпраці операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність;

– пропозиції щодо вдосконалення законодавства у сфері правового регулювання боротьби із кіберзлочинністю;

дістало подальший розвиток:

– твердження про те, що міжнародні нормативно-правові акти як складова національного правового регулювання боротьби з кіберзлочинністю, характеризуються наступними ознаками: 1) належність до

системи національного права за умови ратифікації у встановленому Законом порядку; 2) виконання міжнародними нормативно-правовими актами ролі умовних векторів розвитку вітчизняного законодавства; 3) використання для регулювання суспільних відносин нарівні із нормами вітчизняного законодавства; 4) сприяння міжнародному співробітництву у сфері боротьби з кіберзлочинністю;

– генезис правового регулювання боротьби з кіберзлочинністю в світі: 1) етап зародження правового регулювання боротьби з кіберзлочинністю (1986 рік – 1989 рік) – від прийняття першого в історії комп'ютерного закону, до прийняття Рекомендації № R (89) 9, яка мала ключове значення для подальшого розвитку законодавства, спрямованого на боротьбу з кіберзлочинністю та виступила у якості поштовху для еволюції кримінального законодавства європейських країн; 2) етап внесення змін до кримінального законодавства європейських країн (1989 – 2000 рік) – після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день, а кінцевий термін даного періоду автор умовно пов'язує із 2000 роком, після якого подальші зміни до національних законодавств уже не характеризувались масовим характером; 3) етап консолідації європейської спільноти для боротьби із кіберзлочинністю (2000 рік – 2001 рік) – на протязі двох років у міжнародно-правовому законодавстві з'явився ряд актів, які значною мірою мали вплив на боротьбу із кіберзлочинністю. Саме тому даний етап хронологічно обмежений лише двома роками; 4) сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 рік – наші дні) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, які перебувають на нижчих рівнях розвитку.

Практичне значення одержаних результатів полягає в тому, що вони можуть бути використані:

– *у науково-дослідній діяльності* – для подальших загальних і спеціальних наукових досліджень теоретико-правових аспектів правого регулювання боротьби із кіберзлочинністю;

– *у правотворчій діяльності* – при перегляді та вдосконаленні положень чинного законодавства у сфері боротьби із кіберзлочинністю;

– *у правозастосовній діяльності* – результати дослідження сприятимуть вдосконаленню практики застосування норм чинного законодавства у сфері боротьби із кіберзлочинністю;

– *у навчальному процесі* – при підготовці підручників, навчальних посібників, розробці навчальних програм та методичних рекомендацій, а також при викладанні таких навчальних дисциплін, як «Теорія держави і права», «Актуальні проблеми теорії держави і права», «Теорія та практика правозастосування» тощо. Отримані результати дослідження використовуються у навчальному процесі та науковій діяльності Дніпропетровського державного університету внутрішніх справ (довідка від 09.12.2016 р. № 587);

– *в інформаційно-аналітичній сфері* – для розповсюдження інформації про сучасний стан правового регулювання боротьби з кіберзлочинністю серед учених, працівників державних органів, інститутів громадянського суспільства тощо.

Апробація результатів дисертації. Основні результати дослідження обговорювались на кафедрі теорії, історії держави і права та міжнародного права Інституту права імені Володимира Сташиса Класичного приватного університету, де було виконано дисертацію, а також були оприлюднені на міжнародних та всеукраїнських науково-практичних конференціях: «Актуальні проблеми сучасного правознавства» (м. Київ, 2016 р.); «Реформування національного та міжнародного права: перспективи та пріоритети» (м. Одеса, Україна, 2017 р.); «Актуальні проблеми реформування системи законодавства України» (м. Запоріжжя, 2017 р.).

Публікації. Основні результати дисертаційного дослідження відображено у 9 наукових публікаціях, серед яких 5 статей у наукових фахових виданнях України, 1 стаття у науковому періодичному виданні іншої держави, а також 3 тези доповідей у збірниках матеріалів науково-практичних конференцій.

Структура дисертації. Робота складається зі вступу, трьох розділів, що логічно поєднані у 7 підрозділів, висновків і списку використаних джерел. Повний обсяг дисертації становить 203 сторінки, обсяг основного тексту – 183 сторінки. Список використаних джерел складається із 170 найменувань і займає 20 сторінок.

РОЗДІЛ 1.
ЗАГАЛЬНОТЕОРЕТИЧНІ ЗАСАДИ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

1.1 Теоретико-правові основи боротьби з кіберзлочинністю

До недавнього часу рівень кіберзлочинності в нашій державі був мінімальним, оскільки рівень розвитку інформаційних технологій перебував на нижчому рівні, аніж у розвинених країнах світу. Проте, на сьогодні нашу країну можна охарактеризувати з точки зору наявності освіченого молодого покоління, високого рівня безробіття та обмежених можливостей працевлаштування, а події останнього року засвідчили про існування загрози розвитку даного явища до більш глобальних масштабів.

В Україні проблема боротьби із нею ускладнена тим, що сам термін «кіберзлочинність» в офіційних нормативно-правових документах не визначено, навіть не зважаючи на те, що поняття є звичним як для лексикону правоохоронних органів України та держав світу, так і для правової доктрини нашої держави. Застосування сучасних інформаційних технологій в практично усіх сферах суспільного життя, у тому числі державних і недержавних структурах, висуває проблему боротьби з кіберзлочинністю у число основних. Окрім безпосередньої шкоди, можливої від несанкціонованого доступу до інформації, її розповсюдження, модифікації, знищення тощо, кіберзлочинність є джерелом загрози державній безпеці, економіці, правам та інтересам людини. Ступінь загрози, яку несуть комп’ютерні злочини є не до кінця усвідомленою у суспільстві з причини недостатньої наукової розробленості фундаментальних понять, пов’язаних із нею. Тож, вітчизняному законодавцю та дослідникам варто урахувати досвід, що є в України та розвинених країнах світу, адже він є свідченням існування такої загрози у майбутньому для будь-якої держави світу.

Саме тому, актуальність дослідження поняття, сутності та ознак боротьби з кіберзлочинністю обумовлена тим, що розвиток інформаційних технологій зумовлює появу даного деструктивного явища, встановлює прогресивні тенденції розвитку злочинного світу та виникнення нових форм і видів злочинних посягань. Відповідно, належний науковий аналіз, визначення основоположних понять та виділення ознак боротьби з кіберзлочинністю дозволить сформулювати теоретичні основи даного інституту, що збільшить ефективність пошуку інструментів боротьби із досліджуваним явищем.

Злочинці активно використовують у своїй кримінальній діяльності найновіші досягнення інформаційних технологій, що є свідченням того, що дослідження проблем боротьби із кіберзлочинністю повинно мати повсякчасний характер. Аналіз стану наукової розробленості поняття, сутності та ознак боротьби з кіберзлочинністю засвідчив, що на сучасному етапі дане питання є малодослідженим. Так, вітчизняні дослідники переважно звертались до розгляду окремих аспектів зазначеного інституту, передусім пов'язаних із діяльністю компетентних правоохоронних органів та міжнародним співробітництвом у даній сфері. За таких умов ступінь наукової розробленості понятійного апарату боротьби із кіберзлочинністю перебуває на досить низькому рівні. В першу чергу виділимо роботи таких вчених, як: Дж. Арас, О. О. Баєв, Дж. Блумбекер, В. Л. Бурячок, В. М. Бутузов, В. Я. Вовк, А. В. Войціховський, В. Д. Гавловський, Р. Є. Джансараєва, М. О. Кравцова, М. Ю. Літвінов, О. В. Манжай, В. В. Марков, А. А. Протасевич, В. Г. Хахановський, В. В. Чернєй та інших, проте жоден із них не здійснював спеціальне дослідження поняття, сутності та ознак боротьби з кіберзлочинністю. Саме тому, комплексний аналіз даних питань за таких умов є вкрай необхідним.

Глобальна комп'ютерна мережа Інтернет об'єднала мільярди людей по всьому світу та надала унікальні можливості щодо комунікації, поширення та отримання інформації, підтримки ділових відносин тощо. Разом із тим,

мережа є надійним притулком великої кількості злочинців, які завдяки своїй анонімності та безмежності Інтернету, використовують його для здійснення протиправної діяльності. Із урахуванням стрімкої глобалізації кіберзлочинності, очевидним є те, що людство потребує негайної боротьби із даним явищем. У зв'язку із цим, у якості невідкладної проблеми постає створення правових та наукових механізмів протидії комп'ютерним злочинам.

Будь-які терміни із частиною «кібер-» на сьогодні ще не отримали сформованого визначення ні на науковому, ні на нормативно-правовому рівнях та залишаються предметом наукової дискусії. Не є виключенням і поняття кіберзлочинності, яке не розкрито у тому числі і нормами Конвенції «Про кіберзлочинність» від 23.11.2001 року [1]. У даному міжнародному документі містяться вказівки на: 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем; 2) правопорушення, пов'язані з комп'ютерами, 3) правопорушення, пов'язані з порушенням авторських та суміжних прав [1]. Тобто, варто зробити висновок, що кіберзлочинність та міжнародному рівні розуміється як сукупність зазначених злочинів. Проаналізувавши роботи вітчизняних науковців можна резюмувати, що в Україні кіберзлочинність пов'язується передусім із віртуальним простором.

Так, з точки зору Д. П. Біленчука, кіберзлочинністю є злочинність у змодельованому за допомогою комп'ютера інформаційному просторі, в якому перебувають відомості про осіб, предмети, факти, події, явища і процеси, представлені в математичному, символьному або будь-якому іншому виді, й рухи, що перебувають у процесі, по локальних і глобальних комп'ютерних мережах, або відомості, що зберігаються в пам'яті будь-якого фізичного або віртуального устрою, а також іншого носія, спеціально призначеного для їхнього зберігання, обробки й передачі [2, с. 32]. Дане визначення є найбільш наближеним до української кримінально-правової доктрини, оформленої Кримінальним кодексом України [3], проте відмітимо що воно не розкриває

всю сутність поняття «злочинність». Наприклад, О. М. Литвак, вказує у своїй монографії, що злочинністю є відносно масове явище кожного суспільства, що складається з сукупності окреслених кримінальним законом вчинків, скоєних на тій чи іншій території протягом певного часу [4, с. 9]. Таким чином відзначаємо, що Д. П. Біленчук знехтував ознаками масовості кіберзлочинності, територіальності та хронологічності. Це означає, що сукупність кіберзлочнів повинні мати масовий характер, здійснюватись на території України протягом встановленого відрізку часу для того, щоб бути окресленими загальною категорією кіберзлочинності. Звичайно, територіальність у кіберзлочинах є спірним поняттям, адже вони здійснюються у віртуальному просторі. Проте, якщо об'єкт кібератаки знаходиться в Україні, або ж кіберзлочинець здійснює свою деструктивну діяльність на території України, такі діяння у сукупності варто відносити до категорії вітчизняної кіберзлочинності.

О. Ю. Іванченко розуміє кіберзлочинність подібним чином, як сукупність злочинів, що вчиняються у віртуальному просторі за допомогою комп'ютерних систем, шляхом використання комп'ютерних мереж чи інших засобів віртуального простору, в межах комп'ютерних мереж, а також проти комп'ютерних систем, комп'ютерних мереж і комп'ютерних даних [5, с. 173]. Спільною рисою, і відповідно недоліком, концепцій тлумачення явища кіберзлочинності є нехтування авторами ознак злочинності у цілому, акцентуючи увагу на специфіці кіберзлочинів та кіберпростору, як осередку їх вчинення.

Тому, пропонуємо тлумачити кіберзлочинність як сукупність окреслених кримінальним законом вчинків, скоєних на тій чи іншій території або щодо об'єктів, розташованих на ній за відповідний період часу, вчинених у віртуальному просторі шляхом деструктивного впливу на комп'ютерні системи, комп'ютерні мережі і комп'ютерні дані.

На сучасному етапі поняття «боротьба із кіберзлочинністю» є досить незвичним для вітчизняної науки, не зважаючи на те, що злочинні дії із

застосуванням Всесвітньої мережі несуть високий рівень суспільної небезпеки. Сам термін вже не перший рік перебуває у науковому обігу, проте переважно автори нехтують роз'ясненням його сутності та ознак, зосереджуючись в першу чергу на значенні та алгоритмах реалізації. Тому, один із напрямків вирішення проблеми боротьби із кіберзлочинністю вбачається у розробці теоретичної основи даного деструктивного суспільного явища.

Для аналізу поняття боротьби із кіберзлочинністю звернемось до законодавчих актів, які становлять нормативно-правову базу боротьби із комп'ютерними злочинами - Конституції України [6], Конвенції про кіберзлочинність [1], Кримінального кодексу України [3], Кримінального процесуального кодексу України [7] тощо.

В Основному Законі поняття «боротьби із кіберзлочинністю» відсутнє взагалі. Законодавцем у статті 17 Конституції зазначено, що забезпечення інформаційної безпеки України є найважливішою функцією держави та справою всього Українського народу [6], проте мова все ж йде не про протистояння небезпекам, а про забезпечення безпеки. Норми Конвенції «Про кіберзлочинність» від 23.11.2001 року [1], ратифікованої Верховною Радою України 07.09.2005 року [8], містять поняття «боротьба із кіберзлочинністю», проте у них відсутня його дефініція. Нормами Кримінального кодексу України здійснено розподіл окремих видів кіберзлочинів у Розділі XVI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж – статті 361, 362 та 363, Розділі V Особливої частини «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину - статті 163, 176, 177 та Розділі VII «Злочини у сфері господарської діяльності» - стаття 200 [3], проте поняття «боротьба із кіберзлочинністю» також не закріплено. Подібним чином дане питання врегульоване і нормами Кримінального процесуального кодексу

України - стаття 263 врегульовує питання зняття інформації з транспортних телекомунікаційних мереж, стаття 264 - зняття інформації з електронних інформаційних систем, стаття 268 установлення місцезнаходження радіоелектронного засобу тощо [7], проте про «боротьбу із кіберзлочинністю» мова також не йде. Отже, відсутність належного законодавчого закріплення поняття «боротьба із кіберзлочинністю» є однією із причин наявності проблем у його теоретичному розумінні та неоднозначності наукового тлумачення. За таких умов, важливим є аналіз того, яким чином у нормативно-правових джерел розкрито споріднені до досліджуваного нами поняття.

Звертаючись до нормативно-правових актів, що здійснюють регулювання діяльності суб'єктів боротьби із кіберзлочинністю, у положенні про Департамент кіберполіції Національної поліції України вживається термін «протидія кіберзлочинності» [9], проте також без роз'яснення його сутності. Звернемо увагу на термін «протидія», який на перший погляд є синонімічним до поняття «боротьба», проте аналіз наукової доктрини засвідчив проблемність здійснення їх розподілу.

Так, серед вітчизняних науковців висловлюються погляди щодо недоречності використання для позначення політики держави щодо подолання злочинності терміну «боротьба» - зокрема пропонується використання інших термінів, таких як «запобігання», «протидія», «вплив», «попередження», «профілактика», «подолання», «війна» чи, власне, «протидія». Такі позиції переважно обґрунтовуються тим, що у боротьбі обов'язково має бути переможець та переможений, а об'єктивна дійсність свідчить про те, що цілковита перемога над явищем злочинності є неможливою [10, с. 319–322]. Проте, ми все ж залишимось на позиції тих, хто вважає використання терміну «боротьба» доцільнішим. У загальнотеоретичному розумінні, боротьбою є активне противенство, зіткнення між протилежними соціальними групами, станами, протилежними течіями у суспільстві і т. ін. [11, с. 93]. Тобто, боротьбою із кіберзлочинністю

є активне протистояння деструктивній діяльності осіб, які здійснюють злочинні діяння із використанням всесвітньої мережі Інтернет, що вчиняється правоохоронними органами, в Україні – Службою Безпеки України, Департаментом кіберполіції Національної кіберполіції, законодавцями держав та іншими соціальними групами, зацікавленими у подоланні даної проблеми. Боротьба є активною, цілеспрямованою, науково-обґрунтованою діяльністю держави, спрямованої подолати негативне суспільне явище кіберзлочинності, а термін «боротьба» позначає та підкреслює активний характер цієї діяльності, який не є притаманним іншим термінам. Тому, не зважаючи на свою недосяжність, подолання кіберзлочинності є одним із важливих завдань держави і залишатиметься таким і надалі.

У противагу зробленим нами висновкам, аналізуючи тлумачення поняття «протидія», відзначаємо що нею є дія, спрямована проти іншої дії, що перешкоджає їй [11, с. 1173]. Тобто, порівнюючи терміни «боротьба» та «протидія» відзначимо, що не зважаючи на свою спорідненість, їх все ж не варто ототожнювати. Боротьба здійснюється не залежно від вчинення певних деструктивних дій, тобто дане поняття не виникає безпосередньо у якості реакції на кіберзлочин - вона здійснюється постійно, маючи на меті цілковите подолання певного негативного явища. У свою чергу, відштовхуючись від значення терміну «протидія», робимо висновок, що «спрямування проти іншої дії, що перешкоджає» означає, що дана дія виникає у якості відповіді на вчинені дії. Тобто переносячи дане питання у сферу кіберзлочинності, підкреслюємо, що обов’язковою передумовою протидії кіберзлочинності є наявність юридичного факту у вигляді кіберзлочину.

Щодо тлумачення терміну «протидія злочинності» у науковій літературі, то воно не є однозначним. Наприклад, О. М. Бандурка та О. М. Литвинов зазначають, що протидія злочинності є особливим інтегрованим, багаторівневим об’єктом соціального управління, який формує різноманітна

за формами діяльність відповідних суб'єктів, до яких відносяться державні, недержавні органи та установи, громадські формування та окремі громадяни, які взаємодіють у вигляді системи різнорідних заходів, спрямованих на пошук способів, засобів та інших можливостей ефективного впливу на злочинність із метою зниження інтенсивності процесів детермінації злочинності на всіх рівнях, нейтралізації дії її причин та умов для обмеження кількості злочинних проявів до соціально толерантного рівня [12, с. 44-45]. Не в повній мірі погодимось із даною дефініцією, оскільки вона є більш вдалою для позначення боротьби із злочинністю. Виділимо ознаки «протидії злочинності», які вжили науковці у своїй дефініції: 1) багаторівневий характер; 2) виявлення протидії у діяльності компетентних суб'єктів, (державних, недержавних органів та установ, громадських формувань та окремих громадян); 3) дія на злочинність з метою нейтралізації її дії та умов виникнення. Проте, нами встановлено, що таке пояснення підпадає під термін «боротьба». Термін «боротьба із кіберзлочинністю» є загальнішим, оскільки полягає у комплексному застосуванні заходів, які дозволять викорінити даний вид злочинів як явище, тому є більш доцільним стосовно тематики нашого дослідження. Боротьба здійснюється постійно – від моменту виникнення загрози і до повного подолання проблеми. У свою чергу протидія має більш імпульсивний характер та залежить від конкретно вчинених дій. Тож належно зазначаємо, що боротьба із кіберзлочинністю виявляється у двох напрямках: перший – попередження злочинності, другий - виявлення злочинів, встановлення злочинців та їх покарання. У свою чергу, протидія злочинності включає до свого складу лише другий напрям.

Отже, позначення політики держави більш доцільно описує термін «боротьба із кіберзлочинністю», проте вживання терміну «протидія кіберзлочинності» чи «запобігання кіберзлочинності» у контексті діяльності компетентних правоохоронних органів є виправданим, оскільки в цьому полягає сутність їх діяльності – вчасно зреагувати на виникнення загрози суспільному порядку, розшукати винних та притягнути їх до

відповідальності. Відмітимо, що схожої, проте дзеркально протилежної, точки зору притримуються М. Погорецький та В. Шеломенцев. Вченими розглянуто протидію злочинності як систему заходів політичного, економічного, правового та виховного характеру, що здійснюються державними, у тому числі правоохоронними, органами та громадськими організаціями в межах їх повноважень з метою зниження рівня злочинності, а боротьбу - як активну цілеспрямовану діяльність уповноважених державних правоохоронних органів, яка полягає в установленні контролю за злочинністю, зниженні її рівня шляхом розробки та реалізації запобіжно-профілактичних заходів, а також у виявленні, запобіганні й розкритті конкретних злочинів й притягненні до кримінальної відповідальності осіб, які їх вчинили, із застосуванням передбачених законом засобів і заходів [13, с. 41–42]. Оскільки нами встановлено, що боротьба є загальнішим поняттям, вважаємо за необхідне зазначити, що існування подібних суперечностей вимагає детального наукового аналізу позицій вітчизняних вчених стосовно даного питання.

Визначення поняття, сутності та ознак боротьби з кіберзлочинністю потребує здійснення аналізу наукового тлумачення більш загального терміну - боротьби зі злочинністю. Кіберзлочинність є специфічною, проте з точки зору діяльності правоохоронних органів вона в першу чергу представляє собою різновид злочинності. Тож за умов недостатньої уваги науковців до даного питання, нам видається важливим аналіз боротьби із кіберзлочинністю через призму загальніших та об’ємніших понять.

Юридична енциклопедія трактує термін «боротьба зі злочинністю» як протидію злочинності із застосуванням репресивних та не репресивних засобів у двох взаємопов'язаних напрямах: 1) профілактика злочинності та забезпечення невідворотності покарання; 2) виправлення і перевиховання осіб, що скоїли злочини [14, с. 183]. Звернемо увагу на те, що укладачами енциклопедії фактично зроблено ототожнення понять «боротьба» та «протидія», оскільки одне поняття роз’яснюється через інше. Такий підхід

вбачаємо не зовсім вдалим, затим що ми залишаємось на позиції розуміння даних явищ як двох самостійних. Також потребує додаткового доопрацювання перелік напрямків застосування засобів боротьби із злочинністю, який є неповним – вживання термінів «профілактика», «забезпечення невідворотності» чи «перевиховання» не у повній мірі описує сам процес боротьби та спектр діяльності компетентних правоохоронних органів. Тому до даного переліку варто було б додати напрями виявлення злочинів та встановлення злочинців, а також законодавчий напрям.

Відмітимо розподіл дослідниками заходів впливу на репресивні та не репресивні. Репресією є захід державного примусу, покарання [11, с. 1215]. Отже, «репресивний» - це той, що спрямований покарати. Це є свідченням того, що зазначена дефініція влучніше описала б процес боротьби із злочинцями. Злочинність є більш загальним та глобальним явищем, відповідно методи впливу та боротьби із нею є значно специфічнішими.

Характеризуючи дану дефініцію через призму роз’яснення сутності боротьби із кіберзлочинністю, відмітимо, що вона потребує суттєвого доопрацювання. По-перше, профілактика кіберзлочинності є занадто абстрактним явищем, оскільки кіберзлочинці володіють у рази більшими можливостями, ніж більш «традиційні» злочинці, тому запобігання виникненню та поширенню комп’ютерних злочинів на сьогодні є непосильною задачею для держави. По-друге, санкції, встановлені на сьогодні нормами Кримінального кодексу України за вчинення комп’ютерних злочинів є недостатньо суворими. Наприклад, створення чи збут шкідливих програмних чи технічних засобів, призначених для несанкціонованого втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку караються штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян, виправними роботами на строк до двох років, або позбавленням волі на той самий строк [3]. Шкода від таких деструктивних дій кіберзлочинця може бути непоправною, а збитки від його

діяльності значно перевищувати суму ймовірного штрафу. Тому, у цілому відмітимо, що проаналізована нами дефініція є досить поверхневою, та не відповідає вимогам часу з огляду на те, що наприкінці минулого століття кіберзлочинність в Україні ще не встигла сформуватись у самостійне явище та постійну загрозу.

У даному контексті, більш вдалою є позиція І. І. Карпеця, згідно із якою боротьба зі злочинністю є широким збірним поняттям, яке включає в себе заходи організаційного, профілактичного та законодавчого характеру [15, с. 161]. Іншими словами боротьба зі злочинністю є складною системою, яку складають у єдності три підсистеми: організація боротьби зі злочинністю, попередження злочинності і покарання винних та створення нормативно-правової бази правоохоронної діяльності. Певна поверхневість даної дефініції є її найсильнішою стороною, оскільки по-перше, таку позицію можна застосувати для роз'яснення будь-якого виду злочинності, а по-друге, - вона розкриває різнобічний характер поняття «боротьба». Переносячи це визначення у сферу кіберзлочинності, ми отримаємо повноцінне роз'яснення сутності боротьби із нею, яке втім потребуватиме певних специфічних уточнень. Певного зауваження потребує формулювання «широке збірне поняття», яке не є надто вдалим для роз'яснення сутності боротьби із злочинністю.

Також відмітимо, що у обох розглянутих нами позиціях підкреслено комплексний характер явища боротьби із злочинністю. Це є свідченням того, що дане явище характеризується активною та різносторонньою роллю держави і суспільства у його подоланні. Боротьба – це не просто вчинення конкретних дій, а систематичне здійснення комплексу заходів, спрямованих деструктивно впливати на об'єкт протистояння. Оскільки, у загальному розумінні боротьбою є зіткнення протилежних станів та течій, у даному випадку відбувається протистояння закону та його порушників. Україна, як держава у якій встановлено верховенство права, за таких умов використовує повний спектр заходів, спрямованих на подолання об'єкту боротьби.

Загалом, подібна позиція щодо тлумачення поняття «боротьба зі злочинністю» є загальноприйнятою для прихильників даної концепції тлумачення досліджуваного явища і з нею погоджуються в тому числі інші вчені. Наприклад, фактично аналогічної точки зору дотримується Г. А. Аванесов [16, с. 335], а з точки зору А. І. Долгової, боротьба зі злочинністю - це активне зіткнення суспільства зі злочинністю [17, с. 209]. Позиція дослідниці є влучною, відштовхуючись від сутності терміну «боротьба» у цілому, проте злочинність протистоїть не лише суспільству, а й державі, закону, правопорядку тощо. Проте, сам хід думок є безумовно вдалим, у контексті зроблених нами висновків.

Таким чином, дослідивши наукові позиції щодо визначення поняття «боротьба зі злочинністю», ми встановили, що даному питанню приділена недостатня увага з боку науковців. На підставі проведеного дослідження сформулюємо авторську дефініцію поняття «боротьба зі злочинністю», що дозволить нам вдаліше встановити сутність досліджуваного явища – «боротьби із кіберзлочинністю».

Боротьбою зі злочинністю є комплексна активна система заходів, що застосовується у якості реакції держави на протиправну діяльність осіб чи їх груп та входить до компетенції правоохоронних органів та органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми.

Аналіз поняття «боротьба зі злочинністю» дає нам змогу виділити наступні ознаки даного явища, які у контексті дослідження боротьби із кіберзлочинністю постають у якості загальних: 1) активність; 2) цілеспрямованість; 3) збірність; 4) комплексність.

Ознака активності полягає у тому, що боротьбою зі злочинністю є конкретні активні дії, які здійснюються з метою її подолання. На дану особливість вказують переважно вчені, прихильники концепції «боротьби зі злочинністю», проте водночас відзначимо, що подібні позиції датовані ще попереднім століттям [17, с. 209; 16, с. 335]. Вдалість саме зазначеного

формулювання вбачаємо з огляду на те, що лише боротьба становить собою активні дії, в той час як протидія та інші категорії у меншій мірі відповідають цій категорії. Ознака активності в той же час свідчить про те, що боротьба із злочинністю є комплексом дій, які вчиняє держава з метою їх попередження та профілактики.

Ознака активності є притаманною і боротьбі із кіберзлочинністю. Свідченням цьому є створення окремого Департаменту кіберполіції Національної поліції України [9], а також факультету підготовки фахівців для підрозділів боротьби з кіберзлочинністю у Харківському університеті внутрішніх справ у 2013 році [18, с. 6]. Дані кроки, у сукупності із поступовим прийняттям необхідної нормативно-правової бази є свідченням того, що наша держава здійснює активну діяльність та намагається нівелювати ще на початкових етапах негативні для суспільства наслідки від кіберзлочинності. «Активний» означає «енергійний», «діяльний» [11, с. 19]. Тобто, ознака активності боротьби із кіберзлочинністю полягає у тому, що суб'єкти даної діяльності здійснюють передбачені заходи постійно, не залежно від скоєння кожного окремого злочину. Це нескінченний процес, який продовжується до моменту досягнення мети – подолання кіберзлочинності.

Наступною виділеною нами особливістю боротьби із злочинністю є ознака цілеспрямованості. Її зміст полягає у тому, що боротьба зі злочинністю переслідує чітко окреслені завдання, зокрема профілактика злочинності та забезпечення невідворотності покарання, виправлення і перевиховання осіб, що скоїли злочини, створення нормативних передумов діяльності правоохоронних органів. Висновок про необхідність виділення даної ознаки ми зробили на підставі того, що фактично кожна із розглянутих нами позицій розкривала напрямки діяльності держави щодо питання боротьби зі злочинністю. Так, Ю. С. Шемчушенко до таких напрямків відніс профілактику злочинності та забезпечення невідворотності покарання й виправлення і перевиховання осіб, що скоїли злочини [19, с. 88], І. І. Карпець

і Г. А. Аванесов відзначили організаційний, профілактичний та законодавчий напрями [15, с. 161; 16, с. 335]. Це є свідченням того, що боротьба із злочинністю не є абстрактним поняттям, а є складною системою, у якій компетентні правоохоронні органи, законодавець, зацікавлені особи чи групи осіб наділяється завданнями та виконують згідно них особливі функції у сфері боротьби зі злочинністю.

Розглядаючи дану ознаку як загальну відносно боротьби із кіберзлочинністю відмітимо, що вона теж є притаманною правовому інституту, що нами розглядається. Підтвердженням цього може слугувати Положення про Департамент кіберполіції Національної поліції України. Так, оскільки Департамент здійснює забезпечення реалізації державної політики у сфері протидії кіберзлочинності, перед ним поставлено завдання участі у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кіберзлочинам та сприяння іншим підрозділам Національної поліції України у попередженні, виявленні та припиненні кримінальних правопорушень [9]. Іншими словами, цілеспрямованість у боротьби із кіберзлочинністю має вияв у чіткій регламентації функцій компетентних органів з метою досягнення кінцевого завдання – подолання даного деструктивного явища.

Наступною виділеною нами загальною особливістю є ознака збірності, яка у цілому хоч і є неочевидною, проте нам видається необхідним розглянути її детальніше. Зміст даної ознаки ми вбачаємо у тому, що не зважаючи на те, що боротьба зі злочинністю є сукупністю неоднорідних підсистем, досягнення кінцевої мети є неможливим у разі, якщо кожна із них буде існувати та функціонувати відокремлено. І. І. Карпець зазначив, що боротьба зі злочинністю є широким збірним поняттям [15, с. 161]. Попри всю неоднозначність такого формулювання, варто звернути увагу на те, що у процесі боротьби зі злочинністю можуть бути задіяні суб’єкти абсолютно різноманітних сфер. Законодавець здійснює розробку актуальної нормативно-правової бази, компетентні правоохоронні органи здійснюють

попередження злочинності, розслідування та притягнення до відповідальності винних осіб. Окремі особи чи групи осіб у міру своїх можливостей також можуть сприяти цій боротьбі. За таких умов ознака збірності означає, що попри неоднорідність, кожен із суб'єктів, який бере у цьому участь, зосереджений на досягненні спільної мети.

Щодо боротьби із кіберзлочинністю в Україні, за загальним правилом вона здійснюється Департаментом кіберполіції Національної кіберполіції, вітчизняним законодавцем та іншими соціальними групами, зацікавленими у подоланні даної проблеми. За таких умов законодавець здійснює свою діяльність у законодавчому та організаційному напрямках, а Департамент кіберполіції Національної кіберполіції у профілактичному. Інші соціальні групи, зацікавлені у боротьбі із кіберзлочинністю, сприяють даному процесу у міру своїх можливостей.

Останньою ознакою є комплексність боротьби із злочинністю, яка виявляється у поєднанні репресивних та не репресивних заходів для досягнення окреслених цілей. Вона є спорідненою до розглянутої нами ознаки збірності та була виділена нами при аналізі позицій Ю. С. Шемчушенка та І. І. Карпеця [20; 15, с. 161], які хоч і є у певній мірі неоднорідними, проте обидві базуються на комплексності боротьби зі злочинністю. При роз'ясненні даної ознаки ми скористались дефініцією, закріпленою Юридичною енциклопедією, адже вважаємо вдалим поділ підсистем на репресивні та не репресивні. Не менш вдалою є точка зору І. І. Карпеця, який наводить доцільний перелік заходів боротьби зі злочинністю.

Проблема боротьби із кіберзлочинністю також є комплексною. Так, на сьогодні закони мають відповідати вимогам, які пред'являються темпами розвитку сучасних технологій. Правоохоронні органи зобов'язані організовувати та координувати свою діяльність таким чином, щоб максимально зосередитись на вирішенні проблеми комп'ютерної злочинності. Держави світу повинні активно співпрацювати та обмінюватись досвідом, оскільки кіберзлочинність на сьогодні є загрозою не лише

національній безпеці кожної окремої держав, а людству та міжнародному порядку загалом. Не зважаючи на те, що аналіз вітчизняного законодавства засвідчує, що Україна вживає необхідних заходів для профілактики та протидії комп'ютерній злочинності, цього виявляється недостатньо для її повного подолання. Як влучно відзначає В. В. Чернєй, політика боротьби із кіберзлочинністю протягом усього часу вирізнялася крайньою нестабільністю, відсутністю зваженої науково обґрунтованої концепції впливу на це явище [21, с. 8]. Тому, в результаті всі існуючі прогалини у законодавчому регулюванні, координації правоохоронних органів, виявленні та розслідуванні злочинів є у тому числі наслідком недостатньої уваги до даного питання з боку науковців. На державному рівні необхідність налагодження необхідних комплексних зв'язків для подолання кіберзлочинності проголошувалась неодноразово. Сьогодні важливим є залучення до даного процесу аналітиків, практиків, та у першу чергу, науковців.

Ознаки збірності та комплексності є близькими за своєю сутністю, проте розрізняються за наступними критеріями: 1) збірністю є поєднання підсистем, які значно відрізняються за своїми функціями та призначенням, у свою чергу комплексність полягає у взаємодії усіх елементів єдиного цілого із метою досягнення спільної мети; 2) метою збірності є об'єднання низки елементів у єдине ціле, комплексності – встановлення між ними таких взаємозв'язків, завдяки яким сам процес набуде дієвості; 3) збірність є структурним поняттям, а комплексність – функціональним.

На відміну, від дослідженого поняття «боротьби зі злочинністю», «боротьба із кіберзлочинністю» є в меншій мірі висвітленою у наукових джерелах. В першу чергу даний момент варто пов'язати із тим, що саме поняття «кіберзлочинність» є молодим і ще не встигло привернути увагу достатньої кількості вчених. Дана категорія може іменуватись по-різному: зустрічаються терміни «комп'ютерна злочинність», «злочинність у сфері

комп'ютерних технологій», «злочинність у сфері комп'ютерної інформації», проте найбільш розповсюдженим є все ж поняття «кіберзлочинність».

Вчергове зазначимо, що особливою рисою боротьби із кіберзлочинністю є те, що науково-технічний прогрес і розвиток інформаційних технологій є безумовною перевагою кіберзлочинців. Кіберзлочинність є явищем нової цифрової доби, що і робить кіберзлочинців небезпечнішими та ефективнішими за більш традиційних видів злочинців.

Боротьба із кіберзлочинністю пов'язується із вчиненням особливого різновиду правопорушень – кіберзлочинів. У вітчизняній науці існують різні підходи до визначення даного поняття. Найпростіший із розглянутих полягає у аналізі даного поняття як найбільш небезпечного кіберправопорушення, за яке законодавством встановлюється кримінальна відповідальність [22, с. 85-86]. Тобто, основним критерієм визначення зазначеного терміну є рівень суспільної небезпеки, який характеризує вчинене діяння. Проте, поняття «кіберправопорушення» не розкриває сутності злочинної дії та середовища її вчинення. Тому, подібна позиція потребує суттєвої конкретизації.

О. Копатін та Є. Скулишин розглядають кіберзлочин як злочин, пов'язаний із використанням кібернетичних комп'ютерних систем, при чому вченими підкреслюється, що на відміну від комп'ютерного злочину, поняття якого пов'язане з використанням будь-якої комп'ютерної техніки, кіберзлочин є вужчим поняттям, пов'язаним із функціонуванням саме кібернетичних комп'ютерних систем [23, с. 85-86]. Тобто, в зазначеній дефініції, на відміну від попередньої розглянутої, основна увага приділяється підкресленню специфіки та сфери вчинення кіберзлочинів. Із визначення стає зрозумілим, що кіберзлочинами є протиправні діяння, вчинені за допомогою комп'ютерної техніки у кіберпросторі. В цьому і полягає основна відмінність між поняттями «кіберзлочин» та «комп'ютерний злочин». Вчинення комп'ютерних злочинів пов'язується із використанням будь-якої комп'ютерної техніки, що є значно ширшим поняттям, в той час як кіберзлочини вчиняються виключно за допомогою комп'ютерних систем або

через комп'ютерні системи. Тому, дані терміни не можна ототожнювати, оскільки вони співвідносяться як ціле та його частина.

М. Погорецький розглядає кіберзлочини як злочини, які вчиняються за допомогою або через комп'ютерні системи чи пов'язані саме з комп'ютерними системами, тобто із сукупністю пристроїв, із яких один чи більше відповідно до певної програми виконують автоматичну обробку даних [24, с. 90-92]. Така позиція є схожою до попередньо проаналізованої, виходячи із суто технічних аспектів. Кіберзлочини розглядаються як специфічний вид злочинної діяльності, що здійснюється у кібернетичних комп'ютерних системах. Проте, увагу привертає точка зору автора щодо неприпустимості ототожнення кіберзлочинів та інформаційних злочинів. Стверджується, що «інформаційне середовище» є занадто загальним поняттям для сфери використання комп'ютерних систем, що не розкриває суті процесів автоматизованої обробки інформації [24, с. 92]. Іншими словами, далеко не кожен інформаційний злочин можна вважати кіберзлочином. З іншої сторони, кіберзлочини можна вважати складовою інформаційних злочинів, оскільки об'єктом їх вчинення є інформація, що перебуває у комп'ютерних системах. Тобто, кіберзлочини все ж являють собою специфічний різновид злочинів, які містять ознаки інформаційних та комп'ютерних протиправних діянь, проте все ж становлять самостійну групу із притаманними лише їй рисами.

Отже, кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов'язане із використанням комп'ютерної техніки через комп'ютерні системи, або із комп'ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність.

Аналіз робіт вітчизняних науковців засвідчив, що розробка визначення поняття «боротьба із кіберзлочинністю» перебуває на ще нижчому рівні розвитку, аніж «боротьба із злочинністю» загалом. Увагу вітчизняних дослідників привертають різноманітні аспекти даного явища, процесуальні

моменти, нормативно-правова основа його існування, проте понятійний апарат залишається поза увагою. У процесі дослідження нами встановлено, що дефініція поняття «боротьба із кіберзлочинністю» є новою для вітчизняної юридичної науки. Аналіз російських наукових джерел продемонстрував, що їх вчені концентрують свою увагу у цілому на тих самих проблемах, що й українські, а отже визначення поняття «боротьба із кіберзлочинністю» також залишається невстановленим.

Щодо наближених до боротьби із кіберзлочинністю понять, В. Л. Бурячок оперує терміном «кіберборотьба» [25, с. 11]. Дане поняття не у повній мірі є тотожним об'єкту нашого дослідження, оскільки дане явище позбавлене головної деструктивної риси – воно не стосується злочинності. Проте аналіз сутності терміну «кіберборотьба» дозволить вдаліше розібратись у специфіці такого протистояння та виділити специфічні ознаки боротьби із кіберзлочинністю.

З точки зору ученого, кіберборотьбу становить комплекс заходів, спрямованих на здійснення управлінського і/або деструктивного впливу на автоматизовані ІТ-системи протиборчої сторони та захисту від такого впливу власних інформаційно-обчислювальних ресурсів завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань [25, с. 11]. Дана позиція не є правовою, тому дослідник оперує галузевою термінологією, проте безсумнівно при аналізі зазначеної дефініції можливо провести співвідношення із визначенням поняття «боротьба із злочинністю», сформульованим нами. По-перше, звернемо увагу на виділення науковцем комплексного характеру даного явища. По-друге, дослідником встановлено наявність двох сторін, що цілком відповідає нашому аналізу сутності терміну «боротьба». Щодо специфічних рис, ними є наступні: 1) у першу чергу при розгортанні боротьби варто вжити всіх необхідних заходів для попередження деструктивного впливу на власні автоматизовані системи; 2) кіберборотьба здійснюється завдяки використанню спеціально розроблених програмно-

апаратних засобів, а також після проведення системи спеціалізованих навчань. Таким чином, на підставі позиції В. Л. Бурячка, виділяємо наступні спеціальні ознаки боротьби із кіберзлочинністю: 1) можливість зустрічної атаки зі сторони кіберзлочинців; 2) здійснення виключно компетентними суб'єктами, володіючими спеціальними знаннями та необхідними ресурсами.

О. В. Орлов та Ю. М. Онищенко влучно відзначають, що на відміну від всесвітньої мережі, яка є трансграничною, національні законодавства і правоохоронні органи різних країн у своїй діяльності вимушені брати до уваги особливості кордонів, мовні, політичні, релігійні особливості, що впливають на ефективність боротьби зі злочинністю даного виду. Специфічність характеристик вимагає міждержавного підходу до протидії кіберзлочинам, ефективність якого недосяжна без міжнародної співпраці [18, с. 5]. Формування розуміння даного моменту є вкрай важливим у контексті виділення ознак боротьби із кіберзлочинністю. На відміну від інших видів злочинності, кіберзлочин може посягнути на законність і правопорядок певної держави, у якої не буде можливості його розслідувати. В рамках цієї особливості можна виділити одразу декілька ознак боротьби із кіберзлочинністю: 1) ознака міждержавності; 2) ознака міжнародного співробітництва.

Керуючись здійсненим у роботі аналізом, пропонуємо наступну дефініцію: боротьбою із кіберзлочинністю є комплексна, активна, трансгранична, міждержавна система заходів, що застосовується у якості реакції держави на протиправну діяльність осіб чи їх груп у змодельованому за допомогою комп'ютера інформаційному просторі, яка входить до компетенції відділів правоохоронних органів, володіючих спеціальними знаннями та необхідними ресурсами, органу законодавчої влади та за можливості застосування міжнародного співробітництва у цій сфері.

У свою чергу, систему ознак боротьби із кіберзлочинністю варто виразити дворівнево. До загальних, тобто характерних явищу боротьби із

злочинністю загалом, нами віднесено: 1) активність; 2) цілеспрямованість; 3) збірність; 4) комплексність.

У якості спеціальних, а саме характерних виключно боротьбі із кіберзлочинністю, нами у процесі аналізу правової доктрини виділено: 1) ознака можливості зустрічної атаки зі сторони кіберзлочинців; 2) ознака здійснення виключно компетентними суб'єктами, володіючими спеціальними знаннями та необхідними ресурсами; 3) ознака міждержавності; 4) ознака згуртування держав.

Ознака можливості зустрічної атаки зі сторони кіберзлочинців є характерною виключно даному виду злочинності. Її сутність полягає у тому, що у процесі боротьби із кіберзлочинністю суб'єкти у особі відділів правоохоронних органів, володіючих спеціальними знаннями та необхідними ресурсами, органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми повинні подбати про власну безпеку від деструктивного впливу кіберзлочинців завдяки використанню спеціально розроблених програмно-апаратних засобів, а також проведенню системи спеціалізованих навчань.

Часто у якості об'єктів кібератак постають державні органи, при чому такі ситуації були характерними і для новітньої історії України. Наприклад, в грудні 2015 року здійснено кібератаку на енергетичні компанії України, внаслідок чого було вимкнено близько 30 підстанцій, близько 230 тисяч мешканців залишались без світла протягом однієї-шести годин. 6 грудня 2016 року хакерська атака на урядові сайти (Держказначейства України та інших) і на внутрішні мережі держорганів призвела до масштабних затримок бюджетних виплат [26]. Це свідчить про те, що у якості об'єкту кіберзлочину може постати і будь-який суб'єкт боротьби із кіберзлочинністю. Тому, важливо не лише вживати заходів для її подолання, а й завжди бути готовим до зустрічних дій, оскільки інструменти вчинення кіберзлочинів дозволяють здійснювати деструктивні дії проти будь-яких об'єктів.

Наступною ознакою є здійснення боротьби із кіберзлочинністю виключно компетентними суб'єктами, володіючими спеціальними знаннями та необхідними ресурсами. Підтвердженням цього ж існування в Україні спеціального правоохоронного органу боротьби із кіберзлочинністю, підготовка фахівців якого здійснюється на базі вищого навчального закладу системи Міністерства внутрішніх справ. Більше того, на світовому рівні цінуються вітчизняні кіберфахівці, при чому як відмічає директор департаменту Microsoft їх знання вже тривалий час використовуються для вчинення протиправних дій [27, с. 50]. Це є свідченням того, що потенціал України у питанні боротьби із кіберзлочинністю є високим, проте необхідним є залучення всесвітньо визнаних «світлих голів» на сторону правоохоронців. Фахівці відзначають, що проблемами в Україні є і недостатня кількість державних експертів в області комп'ютерно-технічної експертизи, і складнощі з введенням в правове поле досліджень фахівців комерційних організацій [27, с. 50]. Тому у даному контексті варто відзначити наступне: 1) в Україні відсутня проблема компетентних суб'єктів, володіючих спеціальними знаннями та необхідними ресурсами, проте наявна їх нестача у державній та правоохоронній сферах; 2) Україною здійснюються кроки для підготовки компетентних суб'єктів, проте важливим напрямом має стати залучення до боротьби із кіберзлочинністю вже готових фахівців; 3) важливим є залучення до боротьби із кіберзлочинністю фахівців, які не є співробітниками правоохоронних органів, та які володіють необхідною кваліфікацією на комерційній основі.

Наступна ознака - міждержавність боротьби із кіберзлочинністю. Трансграничність, тобто відсутність кордонів, є характерною для Всесвітньої мережі Інтернет у цілому, яка існує незалежно від кордонів, меж, мовних бар'єрів, релігійних особливостей тощо. Таким чином, кіберзлочинність також характеризується відсутністю кордонів, адже кіберзлочини можуть вчинятись із будь-якого місця земної кулі. Такий стан речей зумовлює потребу суб'єктів боротьби із кіберзлочинністю у своїй діяльності керуватись

специфічними принципами, оскільки при боротьбі із кіберзлочинністю варто рахуватись із державними кордонами, мовними відмінностями, релігійними особливостями тощо. Це свідчить про те, що за рахунок виділеної ознаки кіберзлочинність отримує певну перевагу перед правоохоронцями, оскільки дана діяльність характеризується меншою кількістю перепон для свого здійснення. Враховуючи такий чинник даного виду злочинності, як глобалізація, не завжди у держав світу є можливість самостійно протистояти кібернебезпекам.

Такий порядок речей зумовлює існування наступної ознаки боротьби із кіберзлочинністю - згуртування держав. Висока ефективність боротьби із кіберзлочинністю є недосяжною без міжнародної співпраці, тому у якості невідкладної проблеми постає її активізація. Збільшення кількості компетентних служб у зарубіжних країнах зумовлює необхідність переймання їх досвіду, а також звернення за допомогою та сприянням у разі поєднання інтересів кількох держав у конкретних кіберсправах. Чинне місце у такій співпраці належить міжнародно-правовим механізмам регулювання та взаємодії правоохоронних органів у питаннях протидії кіберзлочинам. Україна ще з початку теперішнього століття залучилась до такого співробітництва. Першим кроком даного процесу стала ратифікація Конвенції «Про кіберзлочинність», здійснена 07.09.2005 року [8]. Проте, даний чинник є хоч і важливим, проте не вирішальним, оскільки уданому контексті важливою є загальна гармонізація національного законодавства з урахуванням світових стандартів, та вироблення національних правових механізмів.

Іншими формами міжнародного співробітництва, як відзначає А. В. Войціховський, є офіційна співпраця, наприклад, використовуючи Інтерпол і Європол, так неофіційна, що здійснюється шляхом надання потенційно корисної інформації безпосередньо правоохоронним органам іншої держави. При цьому, важливою проблемою такої співпраці є узгодження повноважень щодо вживання необхідних заходів для боротьби із кіберзлочинністю,

оскільки внутрішнім правом сторін співпраці можуть бути передбачені положення, які суперечать один одному [28, с. 111]. Тож варто підкреслити, що міжнародна співпраця у боротьбі з кіберзлочинністю здійснюється в наступних напрямках: 1) прийняття міжнародно-правових механізмів регулювання та взаємодії правоохоронних органів у питаннях боротьби із кіберзлочинністю; 2) гармонізація національних законодавств із міжнародним законодавством; 3) безпосередня співпраця, як офіційна, так і неофіційна; 4) узгодження повноважень при здійсненні боротьби із кіберзлочинністю.

Таким чином, рівень та темпи зростання кіберзлочинності потребують адекватного реагування не лише на законодавчому та правоохоронному рівнях, а й на науковому. Згідно здійсненого нами дослідження, науковцям варто звернути більше уваги на теоретичні проблеми досліджуваного явища. Боротьбі із кіберзлочинністю присвячено занадто мало комплексних досліджень, тому не дивно, що у суспільстві відсутнє розуміння реальних загроз від поширення даного деструктивного процесу. Кіберзлочинність є специфічним та унікальним явищем, тож логічно, що боротьба із нею теж набула особливих рис. Із метою ефективної боротьби із кіберзлочинністю, варто давати адекватну та об’єктивну оцінку її сутності, ознак, вимог часу та потреб практики.

Кіберзлочинність набуває нових рис та виходить на якісніший організаційний рівень, а враховуючи тенденції розвитку інформаційних технологій суспільна небезпека даного деструктивного явища постійно збільшується. Для України дана проблема раніше не поставала настільки гостро, проте із зміною державного курсу та приєднанням до світового інформаційного простору, кібернебезпека є постійно існуючою. Таким чином, оскільки кіберзлочинність в нашій державі все ще переважно існує як потенційна загроза, важливим на даному етапі є застосування превентивних заходів. Це все зумовлює необхідність створення ефективної системи

запобігання, виявлення та припинення такої діяльності, що стане запорукою успішності боротьби із кіберзлочинністю в Україні.

1.2. Генезис правового регулювання боротьби з кіберзлочинністю в світі та Україні

Кожну людину наділено правом володіння, користування і розпорядження своєю власністю, результатами інтелектуальної та творчої діяльності. У свою чергу обов'язком держави є забезпечення їх охорони та реалізації, оскільки однією із функцій держави є захист інтересів громадян від зовнішніх і внутрішніх небезпек. Останнім часом залежність людства від нових технологій зростає з неймовірною швидкістю. Проте, дана прогресивна тенденція, на жаль, несе в собі і негативні наслідки.

Стрімке впровадження нових технологій у галузях електроніки, комунікаційних та цифрових технологій наприкінці XX – на початку XXI століття спричинило появу нових суспільних відносин та відповідних проблем, пов'язаних із прагненням людства до розвитку, полегшення праці та покращення умов життєдіяльності. Найбільшого значення у даному процесі набула технологія Інтернет, яка надала фактично безмежні можливості у передачі, поширенні та отриманні інформації, комунікації, виконанні низки дій, не залежно від часу та місця перебування особи. Разом із тим, відкриття нових горизонтів для світового співтовариства нерозривно пов'язане із появою нових форм злочинної діяльності та іншими проявами недобросовісного використання досягнень науково-технічного прогресу.

Потреба вдосконалення засад правового регулювання боротьби з кіберзлочинністю є однією із першочергових, тож відповідні правові приписи мають відповідати вимогам часу і сучасних умов. Відповідно, кожен етап становлення даного інституту як у світі, так і в Україні, значним чином позначався на правовій регламентації діяльності у мережі Інтернет та захисті інтересів громадян від кіберзагроз. Саме тому, актуальним є дослідження становлення правового регулювання боротьби з кіберзлочинністю в Україні

та світі, оскільки це дозволить встановити на якому рівні розвитку даний процес перебуває на сьогодні в нашій державі, та провести співвідношення із аналогічними глобальними процесами. Окрім того, побудова вдалого та ефективного механізму правового регулювання боротьби з кіберзлочинністю є неможливою без приділення належної уваги історичним передумовам його виникнення та розвитку.

Дане питання є новим для правової доктрини нашої держави, оскільки до цього моменту комплексне дослідження ґенези вітчизняного та міжнародного законодавства по боротьбі із кіберзлочинністю ще не здійснювалось. Разом з тим, питанню кібербезпеки, кіберзлочинності та їх правового регулювання присвячувалось чимало праць, тож виділимо у першу чергу таких авторів, як: В. Б. Дзюндзюк, О. В. Манжай, Ю. М. Онищенко, О. В. Орлов, П. І. Пушкаренко та інших. Проте питання генезису правового регулювання боротьби з кіберзлочинністю в світі та Україні ними не розглядалось у комплексі, етапи розвитку даного явища не виділялись.

Виникнення кіберзлочинності пов’язується із поширенням так званого віртуального простору, який містить інформацію про осіб, події, явища, процеси тощо, зашифровані у математичному, символьному чи будь-якому іншому вигляді [29, с. 2]. Тому зрозуміло, що кіберзлочинність є відносно новим видом злочинної діяльності, який потребує спеціальних навичок і знань та специфіка якого полягає у тому, що технічні можливості для його вчинення з’явились порівняно нещодавно, а отже варто звернутись до історичних передумов його появи та розвитку.

Виникнення терміну «комп’ютерна злочинність» хронологічно пов’язується із початком 60-х років минулого століття, коли були виявлені перші випадки злочинів, зроблених з використанням електронних обчислювальних машин [30, с. 5]. «Батьківщиною» даного виду злочинності вважаються Сполучені Штати Америки, де у 1945 р. було створено першу електронну обчислювальну машину, одну із ранніх форм комп’ютерів, яка використовувалась для розшифровування німецьких військових кодів, а

згодом й з іншою метою. Те саме має місце і в наш час, коли комп'ютери та мережеві системи використовуються в першу чергу для вирішення завдань інформаційної безпеки, а вже згодом для інших локальних цілей [31, с. 133]. Тому не випадково, що вчинення першого в історії комп'ютерного злочину відбулось у Міннесоті, де у 1966 році було зафіксовано перший випадок використання електронної обчислювальної машини як інструмента при пограбуванні банку [32, с. 79]. У подальшому поява та розповсюдження комп'ютерної техніки та передових технологій постало у якості реальної загрози національній безпеці держав. Дане питання почало турбувати науковців, наприклад починаючи з 1958 року, дані правової статистики Стенфордського дослідницького інституту так характеризують види «комп'ютерних» злочинів XX століття: 1) випадки пошкодження і розкрадання комп'ютерного устаткування, розкрадання інформації; 2) шахрайство або розкрадання грошей, здійснені із застосуванням комп'ютерів; 3) несанкціоноване використання комп'ютерів або розкрадання машинного часу [31, с. 133]. Тобто на той момент на науковому рівні вже було сформовано чітке розуміння про появу нового виду злочинності та про необхідність її подолання. Не зважаючи на оперативну реакцію з боку науковців, все свідчить про те, що держави світу не були готовими до виникнення таких загроз.

На даний момент немає свідчень ні про існування у ті часи відповідних правових інструментів боротьби із кіберзлочинами, ні про покарання винних у вчиненні злочинних діянь, пов'язаних із комп'ютерною та мережевою діяльністю. Відмітимо, що на той момент комп'ютерна злочинність остаточно сформувалась як самостійний елемент кримінальної системи, оскільки 1970-ті роки характеризуються появою перших професійних комп'ютерних злочинців – хакерів. Варто відзначити, що одними із перших хакерів були Стів Возняк та Стів Джобс, які налагодили виробництво пристроїв для злому телефонних мереж [29, с. 3]. Отже, період від початку 60-років XX століття до початку 70-х варто вважати першим, підготовчим,

етапом розвитку кіберзлочинності. Його датування обране з огляду на те, що початковим моментом варто вважати перші випадки злочинів, зроблених з використанням електронних обчислювальних машин. Відповідно наприкінці даного етапу комп'ютерні зловмисники вже представляли із себе організовані злочинні групи, які використовували власні знання для незаконного збагачення та порушення встановленого порядку.

Отже, для першого, початкового етапу, розвитку кіберзлочинності характерні наступні риси: 1) перші випадки злочинів, зроблених з використанням електронних обчислювальних машин; 2) формування організованих злочинних груп, які використовували власні знання для незаконного збагачення та порушення встановленого порядку; 3) відсутність інструментів правового регулювання боротьби з кіберзлочинністю; 4) відсутність випадків покарання комп'ютерних злочинців за їх протиправну діяльність.

Варто відзначити, що на науковому рівні розуміння небезпеки поширення кіберзлочинів отримало свій подальший розвиток і надалі систематизувалось в окремі положення та концепції. Наприклад, Американською асоціацією адвокатів у Далласі в 1979 році були вперше сформульовані основні ознаки комп'ютерних злочинів: 1) використання або спробу використання комп'ютера, обчислювальної системи або мережі комп'ютерів з метою одержання грошей, власності або послуг, під прикриттям фальшивих приводів або помилкових обіцянок, або видаючи себе за іншу особу; 2) навмисну несанкціоновану дію, що має на меті зміну, ушкодження, знищення або викрадення комп'ютера, обчислювальної системи, мережі комп'ютерів або комп'ютерів, що мають системи математичного забезпечення, програм або інформації; 3) навмисне несанкціоноване порушення зв'язку між комп'ютерами, обчислювальними системами або мережами комп'ютерів [32, с. 76]. На той момент явище кіберзлочинів вже поширилось і на територію колишнього СРСР, до складу якого входила і Україна - в 1979 році у Вільнюсі, внаслідок кіберзлочину

була нанесена шкода державі у розмірі 80 тисяч карбованців [32, с. 79]. Тобто, різниця у розвитку комп'ютерної злочинності у світових державах та у Радянському Союзі становила приблизно два десятки років, що є яскравим свідченням наскільки вагомою була і є відмінність у розробці правових інструментів боротьби із кіберзлочинами. Якщо на даному етапі на території більш розвинутих держав вже діяли певні основи законодавства про кіберзлочинність, то для СРСР комп'ютерні злочини постали у якості абсолютно нового явища.

На той момент кіберзлочинність уже значно поширилась світом, а боротьба із нею набула глобальних масштабів. У 1983 році в Сполучених Штатах Америки відбулась історична подія – перший арешт кіберзлочинця, про який стало відомо громадськості. Групою підлітків було здійснено Інтернет-злом близько 60 комп'ютерів. Після арешту один із учасників дав свідчення, тож усі інші члени організованої групи отримали умовний термін покарання [33, с. 86]. Даний момент є важливим у контексті нашого дослідження одразу із ряду причин: 1) арешт та покарання є свідченням того, що на той момент вже існували правові норми, які містили ознаки законодавства про кіберзлочини; 2) умовний строк для злочинців демонструє, що даний вид злочину не вважався таким, який має високий рівень суспільної небезпечності; 3) про кіберзлочини та кіберзлочинців почали повідомляти громадськості, тобто боротьба із кіберзлочинами лише набирала обертів.

Наступна вагома подія, яка має безпосереднє відношення до генезису правового регулювання боротьби з кіберзлочинністю в світі відбулась у 1986 році у Сполучених Штатах Америки – було прийнято перший в історії комп'ютерний закон «The Computer Fraud and Abuse Act», нормами якого здійснено заборону неавторизованого доступу до комп'ютерних систем та отримання секретної військової інформації. Окрім того Законом визначено та захищено три види несекретної інформації: інформація, що належить фінансовим установам, така як інформація про кредитні картки і рахунки;

дані урядових установ та інформацію, яка належить міжнародним чи міжштатовим організаціям [34, с. 5-22]. Важливими наслідками вступу в дію даного нормативно-правового акту є: 1) було заборонено поширення вірусів, які на той момент набули значного поширення; 2) у 1986 році вперше заарештовано хакера - Ллойда Бланкеншипа [35, с. 97]. Таким чином, момент прийняття першого в історії нормативно-правового акту, присвяченого кіберзлочинам пов'яжемо із завершенням другого етапу розвитку.

Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) характеризується наявністю таких основних рис: 1) чітке формування концепції комп'ютерних злочинів на науковому рівні; 2) поширення кіберзлочинності на територію Радянського Союзу, до складу якого входила і Україна; 3) відбувся перший в історії арешт кіберзлочинця, про який стало відомо громадськості – це є свідченням існування на той момент основ законодавства про кіберзлочинність; 4) прийняття в Сполучених Штатах Америки першого у світовій історії «комп'ютерного» закону.

Наступна важлива подія у історії розвитку кіберзлочинності – це так звана «справа Володимира Льовіна», учасника організованої злочинної групи, яка використовуючи Інтернет, спробувала перевести грошові кошти із рахунків банку на власні. До цього моменту вчинення жодного великого міжнародного злочину не розголошувалось громадськості, тож дана справа вважається першою, віднесеною до категорії транснаціональних мережевих комп'ютерних злочинів [36, с. 35]. По-перше, відмітимо дану подію з огляду на те, що вона є початковим моментом нового етапу розвитку кіберзлочинності. По-друге, очевидно, що загострення ситуації із кіберзлочинами відбувалось пропорційно до зростання обсягів інформації, обіг якої забезпечувався завдяки активному функціонуванню глобальної комп'ютерної мережі Інтернет.

Пропонуємо найменувати даний історичний період етапом транснаціональних кіберзлочинів та кібертероризму, оскільки наступний

щабель розвитку комп'ютерної злочинності пов'язується із її виходом на міжнародний рівень та появи ознак цілеспрямованого застосування терору у великих масштабах. Виникнення явища кібертероризму датується 1998 роком, коли 12-річним хакером було здійснено злом комп'ютерної системи, що контролювала водоспуск дамби у штаті Арізона, що у перспективі могло призвести до затоплення одразу двох міст [37, с. 175]. Тож констатуємо, що на третьому етапі відбулось значне загострення ситуації із кіберзлочинами. Вони набули настільки загрозливих форм, що почали загрожувати окрім стабільності світової фінансової системи життю та здоров'ю людей. Проводячи паралелі із тематикою нашого дослідження, даний етап засвідчив необхідність прийняття жорсткіших нормативно-правових мір для боротьби із кіберзлочинністю. Як нами було відмічено, якщо на попередньому етапі кіберзлочинці могли отримати умовне покарання, то нові реалії засвідчили, що подібні санкції не відповідають мірі небезпечності вчинених діянь.

Тому, етап транснаціональних кіберзлочинів та кібертероризму характеризується наступними ознаками: 1) виникнення міжнародної кіберзлочинності; 2) поява нових форм кіберзлочинності, які містили ознаки терору; 3) невідповідність існуючих санкцій за комп'ютерну злочинність небезпечності діянь.

Наразі відбувається останній етап розвитку кіберзлочинності – етап появи нових форм комп'ютерних злочинів. Як відзначає В. Б. Дзюндзюк, серед них варто відзначити наступні: 1) Інтернет-війна – уперше групи комп'ютерних активістів, засуджуючи військові дії Югославії та НАТО, здійснювали злом урядових комп'ютерів та поширювали антивоєнну Інтернет-пропаганду; 2) Інтернет-страйк – групова діяльність, яка призводить до перевантаження Інтернет-сайту на неможливість його відвідування іншими користувачами тощо [29, с. 5-6]. Очевидно, що такий перелік нових форм є далеко невичерпним, проте основна мета його відзначення – продемонструвати, що питання правового регулювання боротьби з кіберзлочинністю в світі потребує постійної еволюції і вдосконалення, адже

комп'ютерні злочинці постійно змінюють напрямки та методи своєї діяльності. Тож, основними ознаками сучасного етапу є: 1) еволюція кіберзлочинності, виникнення її нових форм; 2) спроби законодавців адекватно реагувати на дані зміни.

Отже, внаслідок аналізу правової доктрини, нами виділено наступні етапи процесу розвитку явища кіберзлочинності:

1. Підготовчий етап (початок 60-років - початок 70-х років XX століття) - початковим моментом варто вважати перші випадки злочинів, вчинених із використанням електронних обчислювальних машин, наприкінці комп'ютерні зловмисники вже представляли із себе організовані злочинні групи, які використовували власні знання для незаконного збагачення та порушення встановленого порядку;

2. Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) - початком варто вважати появу хакерів та їх організованих груп, а завершення пов'язати із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого в історії арешту хакера;

3. Етап транснаціональних кіберзлочинів та кібертероризму (1994 рік – початок XXI століття) – початковий момент даного етапу пов'язується із «справою Володимира Льовіна», першим великим міжнародним транснаціональним мережевим комп'ютерним злочином, а кінцева дата обрана умовно - нами здійснено її прив'язку до початку нового століття, у якому не відбулось вагомих історичних подій у розвитку кібертероризму, проте у якому відбувається планомірна еволюція комп'ютерної злочинності;

4. Сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп'ютерних злочинів.

Таким чином, нами встановлено, що генезис розвитку кіберзлочинності та генезис правового регулювання боротьби з кіберзлочинністю не можна ототожнювати. Кіберзлочинність розвивається у відповідності з еволюцією новітніх технологій, тому на сьогоднішній день є сферою, яка постійно на

крок попереду її нормативно-правового регулювання. Беручи за основу етапізацію розвитку кіберзлочинності, відмічаємо, що на перших двох етапах законодавче регулювання даного інституту фактично не здійснювалось взагалі. Так, нами наведено приклад кіберзлочину, внаслідок якого відбулось перше затримання хакерів, проте їх умовне покарання свідчить про відсутність на той момент адекватних інструментів боротьби із комп'ютерними злочинцями. Відповідно, на другому та третьому етапах правове регулювання боротьби з кіберзлочинністю в світі вже відбувалось повноцінно.

Як нами встановлено, 1986 роком датовано прийняття першого в історії комп'ютерного закону - «The Computer Fraud and Abuse Act» в Сполучених Штатах Америки [34, с. 1-56]. Проте, варто відмітити, що на той момент вже відбувалась розробка правової бази, спрямованої на попередження та припинення кіберзлочинів в різних країнах світу. Наприклад, відповідні зміни до вітчизняного кримінального законодавства було внесено Канадою у 1985 році, Німеччиною у 1986 році, Японією у 1987 році, та дещо пізніше - Англією у 1990 році, Ірландією, Португалією та Туреччиною у 1991 році, Люксембургом та Нідерландами у 1993 році, Ізраїлем у 1995 році, Бельгією у 2000 році тощо [38, с. 646]. Значне пришвидшення даного процесу після 1990 року пояснити прийняттям Рекомендації № R(89)9, затвердженої комітетом Міністрів ЄС 13.09.1989 року, розробка якої здійснювалась із 1985 по 1989 рік Спеціальним Комітетом експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами. Роль Рекомендації № R(89)9 є значною, оскільки даний документ здійснив великий вплив на розвиток і зміну законодавства країн Європи. Рекомендація закріплює список правопорушень, який було рекомендовано для розробки єдиної стратегії боротьби із кіберзлочинністю країнами - учасницями Європейського Союзу. Окрім того, пунктами документу відмічено необхідність досягнення міжнародної згоди стосовно з питань криміналізації окремих комп'ютерних злочинів. Рекомендація містить два списки злочинів - «мінімальний» та «додатковий». До мінімального

списку було включено діяння, які обов'язково повинні бути забороненими міжнародним законодавством та підлягають переслідуванню в судовому порядку, а додатковий список сформували правопорушення, за яких досягнення міжнародної згоди не завжди є можливим [39, с. 60]. Таким чином, перший етап генезису правового регулювання боротьби з кіберзлочинністю обмежимо періодом від 1986 року, тобто прийняття першого в історії комп'ютерного закону, до 1989 року, коли відбулось прийняття Рекомендації № R(89)9, яка мала суттєвий вплив на подальший розвиток законодавства про кіберзлочинність та послужила поштовхом для внесення змін до кримінального законодавства у європейських країнах. Тож, після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день.

Підсумовуючи, перший етап генезису правового регулювання боротьби з кіберзлочинністю в світі характеризується наступними ознаками: 1) прийняття першого в історії «комп'ютерного» закону; 2) внесення змін до вітчизняних кримінальних законодавств деякими країнами; 3) прийняття рекомендацій для європейських держав щодо боротьби із кіберзлочинністю, що згодом значною мірою вплинуло на стрімку еволюцію європейських законодавств. Значення початкового етапу полягає у тому, що на момент його початку кіберзлочинність вже набула загрозливих масштабів і стрімко розвивалась. Прийняття перших нормативно-правових актів не вплинуло на зменшення обсягів комп'ютерної злочинності, проте продемонструвало волю провідних держав світу боротись із даним негативним явищем.

Тому 1989 рік на наше переконання, слугує початковою датою наступного етапу генезису правового регулювання боротьби з кіберзлочинністю в світі - внесення змін до кримінального законодавства європейських країн, який умовно продовжувався до 2000 року. Вживання терміну «умовно» обумовлено тим, що даний процес загалом продовжується і по сьогоднішній день. Проте, по-перше, з огляду на зроблений аналіз

динаміки прийняття змін до вітчизняного кримінального законодавства державами на зазначеному етапі, варто зробити висновок, що саме у 2000 році після прийняття Бельгією змін до кримінального законодавства, подальші зміни до національних законодавств уже не мали настільки масового характеру. По-друге, 2000 роком датується початок прийняття важливих міжнародно-правових актів, які на сьогодні становлять основу європейського та світового законодавства про кіберзлочинність.

До таких міжнародно-правових документів у питанні правового регулювання міжнародних відносин у даній сфері є Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40], Віденська декларація про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року [41], Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу [42], Конвенція про кіберзлочинність [1], Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [43], Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації [44], ряд інших документів, таких як рекомендації Ради Європи.

Таким чином, фактично на протязі двох років у міжнародно-правовому законодавстві з’явився ряд актів, які значною мірою мали вплив на боротьбу із кіберзлочинністю. Саме тому третьому етапу генезису правового регулювання боротьби з кіберзлочинністю в світі ми надали назву «консолідація європейської спільноти» та хронологічно обмежили його лише двома роками – 2000-м та 2001-м. На сьогодні даний етап варто вважати ключовим, оскільки на попередніх, співвідносячи темпи розвитку кіберзлочинності та інструментів правового регулювання боротьби із нею, комп’ютерні злочинці завжди були попереду. Проте, починаючи із початку XXI століття, розвинені держави та європейське співтовариство

продемонстрували готовність вжиття жорстких мір для подолання комп'ютерної злочинності як явища.

Отже, третій етап генезису правового регулювання боротьби з кіберзлочинністю в світі характеризується наступними ознаками: 1) динамічна еволюція національних законодавств провідних держав Європи та світу у частині посилення кримінальної відповідальності за вчинення комп'ютерних злочинів; 2) прийняття базових міжнародних нормативно-правових актів, присвячених співробітництву та взаємодопомозі провідних держав світу у питаннях кібербезпеки, які на сьогодні становлять законодавчу основу сфери боротьби із кіберзлочинністю; 3) вихід законодавцями на якісно новий рівень у боротьбі із комп'ютерними злочинцями внаслідок посилення міждержавних зв'язків та розширення змісту поняття «кіберзлочин».

Щодо наступного періоду, який є останнім, на наше переконання ним є сучасний етап правового регулювання боротьби з кіберзлочинністю, який продовжується і на сьогоднішній день. Даний період не можна охарактеризувати з огляду на конкретні вагомі події, які відбулись чи відбуваються – його основною характеристикою є вдосконалення законодавства про кіберзлочинність держав, які щодо даного питання перебувають на декілька кроків позаду розвинених країн. До таких держав, зокрема можна віднести і Україну. Виділяючи конкретні ознаки сучасного етапу, відмітимо наступні: 1) міжнародне законодавство не зазнало суттєвих змін, проте поступово еволюціонує; 2) залучення до боротьби із кіберзлочинністю все більшої кількості країн світу.

Таким чином, дослідження генезису правового регулювання боротьби з кіберзлочинністю в світі потребує виділення власної історичної класифікації. У процесі аналізу наукової доктрини нами встановлено, що досліджуване питання варто етапізувати наступним чином:

1. Етап зародження правового регулювання боротьби з кіберзлочинністю (1986 рік – 1989 рік) – від прийняття першого в історії

комп'ютерного закону, до прийняття Рекомендації № R(89)9, яка мала ключове значення для подальшого розвитку законодавства, спрямованого на боротьбу з кіберзлочинністю та виступила у якості поштовху для еволюції кримінального законодавства європейських країн;

2. Етап внесення змін до кримінального законодавства європейських країн (1989 - 2000 рік) - після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день, а кінцевий термін даного періоду ми умовно пов'язуємо із 2000 роком, після якого подальші зміни до національних законодавств уже не характеризувались масовим характером;

3. Етап консолідації європейської спільноти для боротьби із кіберзлочинністю (2000 рік – 2001 рік) - на протязі двох років у міжнародно-правовому законодавстві з'явився ряд актів, які значною мірою мали вплив на боротьбу із кіберзлочинністю. Саме тому даний етап хронологічно обмежений лише двома роками;

4. Сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 рік – наші дні) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, які перебувають на нижчих рівнях розвитку.

Наша держава перебуває на початковому етапі боротьби із комп'ютерними злочинами, проте цілеспрямована політика щодо правового регулювання боротьби з кіберзлочинністю все ж здійснюється. Тому важливо проаналізувати цей порівняно недовгий шлях вітчизняного законодавця щодо вирішення існуючих проблем із появою та поширенням нових форм злочинності та встановити співвідношення із історією розвитку даного явища на світовому рівні.

У рамках дослідження генезису правового регулювання боротьби з кіберзлочинністю Україні було б доцільно для початку проаналізувати історію розвитку кіберзлочинності в нашій державі, проте аналіз робіт

вітчизняних науковців засвідчив, що вона є фактично відсутньою. Варта уваги так звана «вінницька справа» 1998 року, у якій зловмисник, використавши систему електронних платежів, незаконно переказав понад 80 мільйонів гривень, а на той час ця сума становила приблизно 20 мільйонів доларів, на рахунок одного з латвійських банків [45, с. 89]. Проте, даний випадок так і не увійшов до історії комп'ютерної злочинності України, оскільки через недосконаліть вітчизняного законодавства не був віднесений до кіберзлочинів. Це є підтвердженням того, що на той момент законодавство України у сфері боротьби з кіберзлочинністю було недосконалим, точніше фактично відсутнім.

Нами встановлено, що в той же час у 1998 році в світі розвиток правового регулювання боротьби із кіберзлочинністю перебував на етапі внесення змін до кримінального законодавства європейських країн, на якому відбувалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами. Проте Україна ще не була частиною даного процесу.

До нормативно-правових актів, які врегульовують суспільні відносини у сфері кібербезпеки в Україні слід віднести: Конституцію України [6], Кримінальний кодекс України [3], Конвенцію про кіберзлочинність [1], закони України «Про інформацію» № 2657-XII від 02.10.1992 [46], «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 [47], «Про державну таємницю» № 3855-XII від 21.01.1994 [48], «Про основи національної безпеки України» № 964-IV від 19.06.2003 [49]; численні укази Президента України та інші нормативно-правові акти. Також вагоме значення має новоприйнятий Закон України "Про основні засади забезпечення кібербезпеки України" від 05.10.2017 № 2163-VIII. Із аналізу нормативно-правої бази боротьби із кіберзлочинності в Україні, можемо встановити певні закономірності, які дозволять нам здійснити вдалу етапізацію генезису правового регулювання боротьби з кіберзлочинністю.

Із початку 90-х років XX століття зазначеній проблемі у багатьох країнах світу приділялась значна увага. Проте, Україна у даному контексті в цілому не відноситься до таких держав. Аналізуючи норми прийнятих у 90-х роках минулого століття нормативно-правових актів, відзначаємо, що увага питанню захисту від кіберзлочинів законодавцем не приділялась у належному обсязі. Тому перший етап хронологічно обмежимо 1991 та 2000 роками, періодом від моменту здобуття Україною незалежності і до початку нового століття, коли почали бути помітними тенденції до розвитку законодавства про кіберзлочини. Отже, початковий етап генезису правового регулювання боротьби з кіберзлочинністю в Україні у цілому характеризується наступними ознаками: 1) прийняття нормативно-правових актів, присвячених захисту інформації, які втім фактично не врегульовували сферу кіберзлочинів; 2) відсутність імплементації норм міжнародного законодавства у кіберсфері; 3) брак в Україні гучних справ, пов’язаних із вітчизняними кіберзлочинцями, що в певній мірі може слугувати поясненням ігнорування законодавцем даного питання.

Вважаємо, що поштовхом для стрімкої еволюції стали взяті Україною зобов'язання щодо інтеграції у міжнародну та світову спільноту, наприклад прийняті згідно до Програми інтеграції України в Європейський Союз [50]. Так, Розділ 13 Програми було присвячено інформаційному суспільству.

У 2001 році було прийнято новий Кримінальний кодекс України, у якому: 1) окремі види кіберзлочинів було виділено у Розділі XVI Особливої частини «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем і комп'ютерних мереж – статті 361, 362 та 363; 2) Розділом V Особливої частини «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» зазначені окремі види злочинів, в яких комп'ютерні продукти визначені як засіб злочину - статті 163, 176, 177; 3) Розділом VII «Злочини у сфері господарської діяльності» - стаття 200 [3]. Значення прийняття Кримінального кодексу України можна виразити наступними аспектами: 1) незаконна діяльність у кіберпросторі

була вперше визнана злочином на рівні вітчизняного законодавства; 2) за кіберзлочини було встановлено конкретні санкції; 3) прийняття Кодексу послужило поштовхом для настання наступного етапу генезису правового регулювання боротьби з кіберзлочинністю – етапу прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю.

Паралельно із даним процесом, актуальність проблеми кібербезпеки було зокрема відмічено Указами Президента: «Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень» від 14.07.2000 р. № 891 [51], «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000 [52], «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001 [53] тощо. Разом з тим, відмічаємо, що не зважаючи на значне поліпшення нормативно-правової бази щодо запобігання та регулювання відносин у сфері кіберзлочинності, у цілому її стан залишався та залишається недосконалим, у першу чергу через безсистемність.

У 2003 році було прийнято Закон України «Про основи національної безпеки» від 19.06.2003 № 964-IV, у якому, зокрема, були закріплені поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» та їх віднесення до основних реальних та потенційних загроз національній безпеці України [49]. Тож, підсумуємо закінчення другого етапу генезису правового регулювання боротьби з кіберзлочинністю в Україні саме 2003 роком. По-перше, на даному етапі було здійснено віднесення незаконної діяльності у кіберпросторі до злочинів та встановлено конкретні санкції за їх вчинення. По-друге, була значно розширена нормативно-правова база правового регулювання боротьби з кіберзлочинністю. По-третє, в законодавчий обіг було введено поняття «комп'ютерна злочинність» та «комп'ютерний тероризм». По-четверте, наступні події щодо правового регулювання

боротьби з кіберзлочинністю в Україні пов'язані із ратифікацією міжнародного законодавства, які логічно виділити окремим етапом.

У 2005 році Україною ратифіковано Конвенцію про кіберзлочинність і таким чином імплементовано положення міжнародного акту у вітчизняне законодавство [1]. Норми Конвенції вже частково були розглянуті нами у межах даного підрозділу, тож доцільно відмітимо, що її прийняття послужило початком нового етапу генезису правового регулювання боротьби з кіберзлочинністю в Україні, який триває і по сьогоднішній день. Курс України до євроінтеграції свідчить про подальшу інтеграцію міжнародних правових норм у вітчизняну систему. Стан розвитку законодавства про кіберзлочинність свідчить про те, що дана сфера однозначно потребує удосконалення, а застосування європейського досвіду є доцільним з огляду на рівень його розвитку.

Відзначимо, що на сучасному етапі розвиток кіберзлочинності в нашій державі ще не досяг значних масштабів. Серед суттєвих кібератак варто виділити нещодавнє застосування невідомими зловмисниками вірусу «Petya.A» проти значної кількості стратегічних об'єктів нашої держави. Зокрема, відомо, що одним із шляхів потрапляння вірусу до комп'ютерних мереж було оновлення бухгалтерського програмного забезпечення «M.E.Doc» [54]. Проте, на сьогодні у даних справах все ще ведеться слідство, а винні особи не встановлені.

Аналіз судової практики засвідчує, що на сьогодні в Україні є поширеними такі кіберзлочини, як несанкціоноване втручання в роботу автоматизованих систем, шахрайство, із використанням електронно-обчислювальної техніки, розповсюдження відеопродукції порнографічного характеру у кіберпросторі та інші незаконні операції з використанням електронно-обчислювальної техніки. Тобто, кібертероризм ще не набув значних масштабів в нашій державі, проте останні негативні тенденції свідчать про необхідність переходу правового регулювання боротьби з кіберзлочинністю на наступний етап.

Щодо прикладів вітчизняної судової практики, 21 січня 2016 року Стрийським міськрайонним судом Львівської області було розглянуто справу щодо несанкціонованого втручання в роботу автоматизованих систем, зокрема банкомату. Зловмисники встановили два несанкціоновані пристрої, які мають умовну назву «накладка на банкомат» і призначені для прихованого розміщення на банкоматі з метою отримання інформації з магнітних стрічок банківських карт користувачів та здійснення відеофіксації виконання ними операцій на цифровій клавіатурі банкомату, що призвело до проникнення в автоматизовану систему вказаного банкомату та витоку інформації 45 клієнтів вказаної вище банківської установи, на яких містилась інформація з магнітних стрічок карт та пінкодів клієнтів банку [55]. Оскільки, статтею 361 Кримінального кодексу України передбачено відповідальність за незаконне втручання в роботу електронних обчислювальних машин, зробимо висновок, що вітчизняний законодавець адекватно реагує на подібні загрози. Оскільки правове регулювання подібних питань передбачено нормами вітчизняного законодавства, основною проблемою існування зазначеного негативного явища є недосконаліть систем захисту банків, у результаті чого зловмисники знаходять можливості незаконного збагачення. Тому, зробимо висновок, що законодавець адекватно реагує на наявність проблеми можливості несанкціонованих втручань у кіберпросторі.

Поширеними на сьогодні є випадки шахрайства із використанням електронно-обчислювальної техніки. Так, 22.05.2017 року Першотравневим районним судом міста Чернівці було винесено вирок по справі № 725/85/17 щодо вчинення із корисливих мотивів ряду дій, спрямованих на підготовку та реалізацію шахрайства. Зловмисниця розмістила на Інтернет-сайті \ оголошення про здачу в оренду кімнати, достовірно знаючи, що житла за вказаною адресою у неї не має та наміру здавати кімнату в оренду вона не мала. Особа повідомила потерпілому завідомо неправдиву інформацію, та отримала грошову суму у якості завдатку [56]. У даному випадку злочин

кваліфікувався за статтею 190 Кримінального кодексу України. У даному випадку законодавець не відокремив окремо шахрайство за допомогою електронно-обчислювальної техніки, проте у даному випадку все ж основоположну роль відіграє факт заволодіння чужим майном шляхом обману. Тому, не зважаючи на наявні ознаки кіберзлочину, подібні правопорушення варто кваліфікувати як шахрайство.

Наступним прикладом є вирок Ленінського райсуду міста Кіровограда (нині м. Кропивницький) у справі № 405/1660/14-к. Зловмиснику було пред'явлено обвинувачення у вчиненні розповсюдження відеопродукції порнографічного характеру за допомогою веб-сайту «http://vk.com» [57]. Не зважаючи на те, що даний злочин було кваліфіковано за статтями 300 та 301 Кримінального кодексу України, а саме ввезення, виготовлення, збут і розповсюдження порнографічних предметів та творів, що пропагують культ насильства і жорстокості, расову, національну чи релігійну нетерпимість та дискримінацію, даний проступок все ж має чіткі ознаки кіберзлочинів, адже його вчинення пов’язується із Всесвітньою мережею.

Тому, зробимо наступний висновок: не зважаючи на те, що деякі із проступків, які містять ознаки кіберзлочинів, не кваліфікуються як останні, законодавцем все ж на належному рівні здійснюється правове регулювання тих загроз, які є актуальними на сьогодні. Водночас, останні тенденції свідчать про те, що в подальшому існуючий механізм потребує значного вдосконалення із урахуванням нещодавніх викликів.

Отже, на сучасному етапі правове регулювання боротьби з кіберзлочинністю в Україні характеризується такими особливими рисами: 1) ратифікація міжнародних правових актів; 2) курс України до євроінтеграції зумовлює необхідність подальшого приведення вітчизняного законодавства у відповідність до європейських стандартів; 3) поява тенденції до збільшення загрози кібертероризму в Україні; 4) належне правове регулювання тих кіберзагроз, які на сьогодні є найбільш поширеними в Україні.

Дослідження генезису правового регулювання боротьби з кіберзлочинністю в Україні дозволяє виділити його наступні етапи:

1. Початковий етап (1991 рік – 2000 рік) – не зважаючи на те, що у даний період було прийнято декілька нормативно-правових актів, спрямованих на врегулювання проблем кібербезпеки, питанню захисту від кіберзлочинів законодавцем увага не приділялась у належному обсязі, проте у 2000 році почали бути помітними тенденції до розвитку законодавства про кіберзлочини;

2. Етап прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю (2001 рік – 2005 рік) – його початок пов’язується із прийняттям Кримінального кодексу України, у нормах якого незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства, а за кіберзлочини було встановлено конкретні санкції. Відповідно, закінчення етапу віднесемо до введення у правовий обіг понять «комп'ютерна злочинність» та «комп'ютерний тероризм»;

3. Етап відповідності правового регулювання боротьби з кіберзлочинністю існуючим загрозам (2005 рік – до 27.06.2017 року) - не зважаючи на те, що на даному етапі зроблено небагато, курс України до євроінтеграції вимагає імплементації європейських правових норм у вітчизняне законодавство. Існуючі кіберзагрози були врегульовані належним чином. У цілому, зазначений період характеризується відсутністю вагомих подій у сфері боротьби із кіберзлочинністю;

4. Новітній етап (від 27.06.2017 року) – вірус «Petya.A» продемонстрував неготовність України до боротьби із сучасними кіберзагрозами. Тому, щойно розпочатий етап пов’яжемо із подальшою розробкою інструментів для боротьби із кібертерроризмом.

Отже, комп’ютерна злочинність є проблемою, з якою суспільство зіштовхнулось порівняно нещодавно, проте яка обіцяє постійно зростати та вдосконалюватись. Незважаючи на усі заходи, які приймаються державами, їх усе ще недостатньо. Тому на сьогодні важливим є перегляд усіх існуючих

інструментів та розробка нових, які дозволять надійніше захиститись від кіберзлочинців.

Дослідження розвитку правового регулювання боротьби з кіберзлочинністю в світі та Україні засвідчило, що жодна держава не в змозі протистояти кіберзлочинності самостійно. Аналіз історичних процесів генезису європейського законодавства засвідчив, що основні поштовхи у еволюції правового регулювання боротьби з кіберзлочинністю в зарубіжних країнах були спричинені прийняттям колективних рішень чи рекомендацій. Тому Україна, як держава, яка в світлі нещодавніх подій фактично вперше зіштовхнулась із масовими організованими кібератаками потребує значної активізації діяльності у зазначеній сфері.

Висновки до Розділу 1

1. Боротьбою зі злочинністю є комплексна активна система заходів, що застосовується у якості реакції держави на протиправну діяльність осіб чи їх груп та входить до компетенції правоохоронних органів та органу законодавчої влади за сприяння окремих осіб чи груп осіб, зацікавлених у подоланні даної проблеми.

2. Виділено наступні етапи процесу розвитку явища кіберзлочинності:

1) Підготовчий етап (початок 60-років - початок 70-х років XX століття) - початковим моментом варто вважати перші випадки злочинів, вчинених із використанням електронних обчислювальних машин, наприкінці комп'ютерні зловмисники вже представляли із себе організовані злочинні групи, які використовували власні знання для незаконного збагачення та порушення встановленого порядку;

2) Етап розповсюдження кіберзлочинності (початок 70-х років XX століття – 1986 рік) - початком варто вважати появу хакерів та їх організованих груп, а завершення пов'язати із прийняттям першого в історії нормативно-правового акту, присвяченого кіберзлочинам та першого в історії арешту хакера;

3) Етап транснаціональних кіберзлочинів та кібертероризму (1994 рік – початок XXI століття) – початковий момент даного етапу пов'язується із «справою Володимира Льовіна», першим великим міжнародним транснаціональним мережевим комп'ютерним злочином, а кінцева дата обрана умовно - нами здійснено її прив'язку до початку нового століття, у якому не відбулось вагомих історичних подій у розвитку кібертероризму, проте у якому відбувається планомірна еволюція комп'ютерної злочинності;

4) Сучасний етап кіберзлочинності (XXI століття) – етап появи нових форм комп'ютерних злочинів.

3. Генезис правового регулювання боротьби з кіберзлочинністю в світі етапізований наступним чином: 1) Етап зародження правового регулювання боротьби з кіберзлочинністю (1986 рік – 1989 рік) – від прийняття першого в історії комп'ютерного закону, до прийняття Рекомендації № R(89)9, яка мала ключове значення для подальшого розвитку законодавства, спрямованого на боротьбу з кіберзлочинністю та виступила у якості поштовху для еволюції кримінального законодавства європейських країн; 2) Етап внесення змін до кримінального законодавства європейських країн (1989 - 2000 рік) - після 1989 року розпочалась стрімка еволюція кримінального законодавства європейських держав у частині посилення боротьби із комп'ютерними злочинами, яка у певній мірі продовжується і по сьогоднішній день, а кінцевий термін даного періоду ми умовно пов'язуємо із 2000 роком, після якого подальші зміни до національних законодавств уже не характеризувались масовим характером; 3) Етап консолідації європейської спільноти для боротьби із кіберзлочинністю (2000 рік – 2001 рік) - на протязі двох років у міжнародно-правовому законодавстві з'явився ряд актів, які значною мірою мали вплив на боротьбу із кіберзлочинністю. Саме тому даний етап хронологічно обмежений лише двома роками; 4) Сучасний етап правового регулювання боротьби з кіберзлочинністю (2001 рік – наші дні) – характеризується процесом вдосконалення законодавства про кіберзлочинність держав, які перебувають на нижчих рівнях розвитку.

РОЗДІЛ 2.
МЕХАНІЗМ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

2.1 Структура механізму правового регулювання боротьби з кіберзлочинністю

Стрімкий розвиток науково-технічного прогресу призвів до застосування електронно-обчислювальних машин (комп'ютерів), комп'ютерних мереж та різноманітних систем електронного зв'язку практично в усіх сферах суспільного життя. Разом з тим, внаслідок поширення названих технічних інновацій виникли й негативні соціальні явища, які пов'язані з діяльністю відповідного обладнання та техніки, зокрема інформаційні злочини. За таких умов перед Українською державою постала нагальна необхідність забезпечити ефективну боротьбу з кіберзлочинністю, що, серед іншого, включає й механізм правового регулювання відповідних суспільних відносин.

Зростання кількості інформаційних злочинів, тяжкість завданих ними наслідків, транскордонний характер та інші негативні чинники зумовлюють необхідність запровадження тісної міжнародної співпраці у даній галузі, яка передбачає дієве функціонування як національних, так і міжнародних заходів боротьби з кіберзлочинністю. Тому надзвичайно актуальною теоретичною та практичною проблематикою є питання структури механізму правового регулювання боротьби з кіберзлочинністю та її міжнародно-правового регулювання. Дослідження порушеної тематики дозволяє з'ясувати наявну систему нормативної регламентації суспільних відносин у сфері протидії інформаційним злочинам, виявити прогалини й недоліки наявного нормативно-правового регулювання, визначити пріоритетні напрямки

удосконалення нормативних приписів, а також перспективи міжнародно-правового співробітництва.

Тому потрібно здійснити доктринальний аналіз сучасного стану структури механізму правового регулювання боротьби з кіберзлочинністю та її складових елементів. Особливу увагу доцільно приділити проблемі міжнародного співробітництва: взаємодії правоохоронних органів різних держав, перейнятті спільного досвіду, проведенні спеціальних навчань, оперативному обміні необхідною інформацією та інше, тобто належному міжнародному нормативно-правовому регулюванню боротьби з кіберзлочинністю.

В науковій юридичній літературі наголошується на тому, що поняття «механізм правового регулювання» було розроблено й введено у доктрину права в роки панування радянського права, а одним із його творців називають М.Г. Александрова, який у свій час використовував термін «механізм впливу права на суспільні відносини» [58, с. 183-213]. Щодо власне «механізму правового регулювання», то названа категорія була достатньо детально науково обґрунтована іншим відомим теоретиком права радянського періоду − С.С. Алексєєвим, який запропонував її дефініцію та надав характеристику складових елементів, а також визначив значення для юридичної науки та права загалом [59, с. 146-167]. Разом з тим, подальший розвиток наукової думки у досліджуваному напрямку не обмежився досягненнями вчених-правників радянського періоду. Так на сьогодні в науковій юридичній літературі як з проблем теорії права, так і в межах галузевих юридичних дисциплін, запропоновані та доктринально обґрунтовані інші концепції щодо розуміння досліджуваного правового явища.

С.С. Алексєєв пропонував розглядати «механізм правового регулювання» як взяту в цілому всю сукупність юридичних засобів, за допомогою яких забезпечується правовий вплив на суспільні відносини [60,

с. 222]. Тобто досліджувана категорія визначається певним переліком засобів юридичного інструментарію, які здійснюють вплив на суспільні відносини, що й дозволяє їх нормативно регламентувати. Така позиція вважається класичною у правій науці та має ряд позитивних аспектів, однак і вона не позбавлена окремих недоліків. Наприклад, з аналізу авторської дефініції не зрозуміло з якою метою здійснюється нормативний вплив, що необхідно розуміти під поняттям юридичні засоби тощо.

Схожої наукової позиції дотримується й А.В. Малько, який визначає механізм правового регулювання як систему правових засобів, організованих найбільш послідовним чином [61, с. 625]. Разом з тим, за такого підходу складно розуміти з якою метою здійснюється організація відповідних правових засобів, яким чином забезпечується вплив на них, який і створює найбільш послідовну організацію та інше. Вважаємо, що запропонований автором підхід є надзвичайно спрощеним і не дозволяє повною мірою розкрити сутність досліджуваного поняття.

У підручнику з теорії держави та права за редакцією відомого вченого-правника В.В. Копєйчикова, «механізм правового регулювання» пропонується визначати як сукупність правових засобів, за допомогою яких поведінка суб'єктів суспільних відносин приводиться у відповідність до вимог і дозволів, що містяться у нормах права [62, с. 220]. Тобто у нормах права встановлюються законодавцем певні дозволи та заборони, які є обов'язковими до виконання суб'єктами правових відносин, що й дозволяє регламентувати їх бажану поведінку у суспільному житті. Такий підхід видається більш логічним та послідовним, оскільки нормативні приписи впливають не на самі відносини, які виникають, змінюються та припиняються у суспільстві, а на відповідне суб'єктне коло осіб, їх поведінку, яка й зумовлює трансформацію правовідносин.

На переконання В.М. Хропанюка, «механізм правового регулювання» – це система правових засобів, за допомогою яких упорядкованість суспільних відносин здійснюється у відповідності до цілей і завдань правової держави

[63, с. 341-342]. З аналізу наведеної доктринальної дефініції можна встановити такі її ознаки: 1) являє собою систему правових засобів; 2) забезпечує упорядкованість відносин, які виникають, змінюються та припиняються у суспільстві; 3) відповідає цілям й завданням правової держави. Відмінною авторською рисою розуміння даного правового явища є те, що воно має місце у правовій державі, що викликає певні сумніви, оскільки нормативний вплив на суспільні відносини може мати місце й за інших умов, зокрема, у тоталітарних й інших недемократичних країнах, де механізм правового регулювання наявних, але не відповідає ознакам правової держави.

О.Ф. Скакун досліджувану категорію визначає як систему юридичних засобів, способів та форм, за допомогою яких нормативність права переводиться в упорядкованість суспільних відносин, задовольняються інтереси суб'єктів права, встановлюється та забезпечується правопорядок [64, с. 498]. Таким чином, науковець істотним чином розширює сферу юридичного інструментарію за допомогою якого забезпечується регулюючий вплив норм права на суспільні відносини, а саме: поряд з юридичними засобами, пропонуються юридичні форми й правові способи. Такий авторський підхід видається сумнівним з огляду на те, що розуміється під відповідними формами та способами, тобто чи здатні вони забезпечувати нормативний вплив на відносини, які наявні у суспільному житті, та як співвідносяться з поняттям «правові засоби».

Відомий теоретик та філософ права В.С. Нерсесянц пропонує наступне визначення «механізму правового регулювання» – це механізм абстрактно-загальної правової регуляції, конкретизований та індивідуалізований застосовано до конкретно-визначеного випадку (і форми) прояву юридичної сили діючого права [65, с. 476]. Запропонована вченим дефініція суттєво відрізняється від наявних у доктрині права, оскільки принципово по-іншому визначає досліджувану правову категорію, так її ключовим рисами є: 1) по своїй суті це абстрактних механізм правового впливу; 2) має індивідуально

виражену форму до конкретного випадку застосування правового припису. За таких умов авторська позиція видається помилковою, адже ведучи мову про механізм правового регулювання, мають на увазі чітку та ефективну систему правового інструментарію, який забезпечує нормативний вплив на поведінку невизначеного числа суб'єктів суспільних відносин в усіх подібних випадках, коли має застосовуватися таке нормативне правило.

В науковій юридичній літературі вказується, що плюралізм думок щодо досліджуваного правового поняття дозволяє визначити такі підходи розуміння правової природи категорії «механізм правового регулювання»: 1) інструментальний; 2) діяльнісний; 3) системний та 4) комплексний [66, с. 20-27; 67, с. 7]. Кожна з наведених доктринальних концепцій має як своїх прихильників, так і опонентів, які вказують на «сильні» та «слабкі» сторони названих теоретичних позицій. За таких умов, жодна з них не є правильною та вичерпною, тому для дослідження проблематики структури механізму правового регулювання боротьби з кіберзлочинністю доцільно проаналізувати їх, та визначити раціональні аспекти.

Таким чином, «механізм правового регулювання» як юридична категорія спрямований на впорядкування явищ правової дійсності, забезпечення їх єдності, взаємозв'язку й взаємодії, що виражається у можливості перетворення правових норм у реальний вплив на поведінку суб'єктів суспільних правовідносин. Поняття «механізм правового регулювання» можна у загальному визначити як чітко встановлену та організовану систему юридичного інструментарію, яка забезпечує правовий вплив нормативних приписів на сферу суспільних відносин, що дозволяє регламентувати межі дозволеної та забороненої поведінки учасників відповідного кола суспільних відноси, з метою забезпечення законності та правопорядку у відповідності до потреб та інтересів держави, громадянського суспільства, окремих індивідів тощо.

В галузевих юридичних науках також наявні доктринальні доробки

вчених-правників щодо розуміння відповідного механізму в межах тієї або іншої галузі права або юридичної науки. Так, Л.Б. Зусь вивчаючи питання «механізму кримінально-процесуального регулювання» наголошує, що ним є передбачена структурою кримінально-процесуального права система процесуальних засобів, за допомогою якої забезпечується регулювання суспільних відносин, які виникають у сфері кримінального судочинства. Комплексним засобом такого регулювання є кримінально-процесуальне право, мета функціонування якого саме полягає в ефективному врегулюванні названих відносин [68, с. 35]. Особливістю даного підходу є те, що науковець пропонує визначати як засіб правового регулювання самостійну галузь права – кримінальне процесуальне право, яке забезпечує комплексний нормативний вплив на всю сферу кримінальних процесуальних відносин, в тому числі й на поведінку учасників такого правовідношення. Разом з тим, повністю з наведеними автором міркуваннями погодитися не можна, оскільки галузь права, в першу чергу, це сукупність правових норм, а категорія «механізм правового регулювання» у своїй структурі не обмежується тільки нормативними приписами, а включає до свого обсягу й інші правові явища.

Я.В. Ступник, досліджуючи питання механізму протидії наркозлочинності, запропонував таку його дефініцію – це таке системне утворення (узяту в єдності всю сукупність) норм, принципів, інститутів (державно-правових і суспільно-політичних), форм, методів і засобів (організаційних, правових, економічних, соціально-психологічних) зв’язків і відносин, за допомогою яких забезпечується кримінологічний вплив на специфічні об’єкти для досягнення поставлених цілей. У вузькому розумінні (буквальному) цей механізм являє собою сукупність форм, методів і засобів, за допомогою яких відповідними суб’єктами здійснюється різноманітна діяльність у сфері протидії наркозлочинності [69]. Аналізуючи відповідну дефініцію можна дійти висновку, що в її основі лежить інструментальний підхід, який визначає досліджувану категорію як сукупність засобів

юридичного інструментарію (засоби, форми, способи, принципи, відносини, зв'язки між ними тощо), які забезпечують можливість здійснення впливу на кримінологічні об'єкти для виконання поставлених завдань.

Беручи до уваги наведене, категорію «механізм правового регулювання боротьби з кіберзлочинністю» можна визначити як чітко визначену й організовану систему юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

Дискусійність в частині розуміння правової природи та сутності досліджуваного поняття, породжує й численні доктринальні концепції щодо розуміння структури (внутрішньої будови) даного правового явища. Одним з найбільш об'ємних та громіздких підходів є т.з. «широкий», який передбачає, що до механізму правового регулювання належать так складові елементи як: 1) норма права, безпосередній регулятор поведінки суб'єктів права, що наділяє їх визначеним обсягом взаємних суб'єктивних прав та юридичних обов'язків; 2) нормативно-правовий акт; 3) юридичний факт; 4) правові відносини; 5) тлумачення права; 6) реалізація права; 7) законність, реалізація правових приписів через дотримання нормативно-правових вимог суб'єктами права; 8) правосвідомість, усвідомлення суб'єктами правових приписів; 9) правова культура; 10) правомірна поведінка; 11) протиправна поведінка; 12) юридична відповідальність [70, с. 24-28; 71, с. 119]. Разом з тим, за такого підходу, окремі з наведених складових елементів навряд чи можна віднести до структури досліджуваної правової категорії (наприклад, правосвідомість, правова культура та деякі інші). Також викликає сумнів й можливість значної кількості правових засобів належати до внутрішньої будови досліджуваної категорії.

Діаметрально протилежною наведеній концепції є т.з. «вузьке»

розуміння структури механізму правового регулювання, яке передбачає наявність таких складових одиниць: 1) норми права; 2) нормативно-правові акти; 3) правовідносини; 4) реалізацію права; 5) законність. Кожен з елементів даної системи виконує специфічну функцію у задоволенні інтересів суб'єктів, в регулюванні суспільних відносин, у досягненні ефективності правового регулювання [72, с. 119; 73, с. 42-43]. Такий підхід також не видається ідеальним, оскільки складно зрозуміти навіщо виокремлювати норми права та нормативно-правові акти, де вказані нормативні приписи містяться в окремі складові елементи. Крім того, викликає сумнів доцільність віднесення законності до складу структури механізму правового регулювання, адже більш вірніше визначати верховенство права, яке є ширшим та загальнішим поняттям. Таким чином, концепція «вузького» також є достатньо спірною та слабко аргументованою з доктринальної точки зору.

На думку Ф.Є. Колонтаєвського, слід виділяти такі основні елементи механізму правового регулювання як: 1) нормативна основа; 2) правові відносини; 3) здійснення суб'єктами їх прав і обов'язків [74, с. 15]. З приводу останнього з наведених елементів, то вважаємо, що його виділення є помилковим, оскільки він опосередковує реалізацію поведінки учасників відповідного кола суспільних відносин, тобто мова йде про фактичний зміст правововідношення, яке уже є складовим елементом досліджуваної категорії, а тому його окремий аспект не може бути виділений в самостійний структурний елемент.

На переконання О.П. Коренева, до структури даного механізму належать такі елементи: 1) норми права і його принципи, які виражені у нормативно-правових актах, указах Президента та інших нормативних актах; 2) акти тлумачення норм права, видані уповноваженими на те організаціями; 3) акти застосування норм права; 4) правові відносини [75, с. 40]. Аналізуючи запропонований авторський підхід, варто наголосити на тому, що незрозумілим є потреба у визначенні актів реалізації норм права, оскільки в

цьому випадку також йде мова про здійснення суб'єктами правовідносин своєї поведінки, тобто знову ж таки йдеться про правовідносини, які є самостійними складовим елементам. Також наявні сумніви в необхідності визначенні актів тлумачення норм права як елементів структури механізму правового регулювання, оскільки є значна кількість видів тлумачення й незрозуміло про які з них саме йде мова у таких випадках.

С.В. Бобровник елементи механізму правового регулювання поділяє на: 1) основні та 2) факультативні і пов'язує їх із стадіями механізму правового регулювання. Розмежування обов'язкових та факультативних елементів механізму правового регулювання дає можливість за допомогою норми права контролювати модель обов'язкової, дозволеної поведінки різних суб'єктів правовідносин. Обов'язкова стадія передбачає необхідність врегулювання певних суспільних відносин, які, насамперед, моделюються, виникають та реалізуються в певних суб'єктивних [76, с. 216]. Така позиція заслуговує на увагу, адже всі концепції щодо структури механізму правового регулювання так або інакше намагаються максимально поділити вказану категорію на максимальну кількість складових одиниць, а тому їх класифікація та узагальнення за критерієм обов'язковості є дуже важливим.

С.С. Алексєєв у свій час пропонував виділення трьох основних елементів в механізмі правового регулювання: 1) юридичні норми; 2) правові відносини; 3) акти реалізації прав та обов'язків; та факультативний елемент – акти застосування права [59, с. 146-169]. Схожу позицію висловлював і О.Г. Мурашин, який називає три основних та кілька допоміжних елементів механізму правового регулювання. До основних він відносить: 1) юридичну норму; 2) правовідносини; 3) реалізацію учасниками правовідносин їх суб'єктивних прав і обов'язків. Допоміжними він називає акти застосування права, а нормативною основою названого механізму – систему правових норм [77, с. 18-19]. Однак поведінка суб'єктів суспільних відносин регулюється шляхом визначення нормативними приписами її виду й міри, відповідно до яких вони змушені будувати свою поведінку. Тобто йдеться

про те, що акти реальної поведінки – це фактичний зміст правових відносин, а за таких умов засобом механізму правового регулювання є правові відносини, а акти реалізації права складають їх зміст.

У цілому поділяючи існуючі в теорії права підходи до визначення правових засобів механізму правового регулювання, можна стверджувати, що кожний елемент такого механізму виконує специфічну роль у регулюванні поведінки людей, виникаючих на цій основі суспільних відносин. Тому вважаємо, що до структури механізму правового регулювання боротьби з кіберзлочинністю віднесено такі елементи: 1) норми права; 2) правовідносини; 3) юридичні факти. Правові норми, правовідносини та юридичні факти є взаємопов'язаними і взаємозалежними категоріями.

Правові норми як складові елементи структури механізму правового регулювання боротьби кіберзлочинністю – це закріплені у нормативно-правових актах та міжнародних нормативно-правових договорах правила поведінки, які регулюються відносини, що виникають, припиняються та змінюються у сфері діяльності з подолання інформаційної злочинності, й забезпечуються легальним примусом з боку держав або учасників міжнародних відносин.

Щодо правовідносин як структурного елементу механізму правового регулювання боротьби кіберзлочинністю, то вони опосередковують частину суспільних відносин, які регламентуються правовими нормами законодавства та міжнародних договорів з питань боротьби з інформаційною злочинністю, й забезпечують необхідний регулюючий вплив на поведінку учасників відповідного правовідношення з метою досягнення позитивного правового результату – попередження й профілактику кіберзлочинності, припинення вчинюваних протиправних діянь, співробітництво у сфері розшуку злочинців та інше.

Юридичні факти є важливим самостійним складовим елементом механізму правового регулювання боротьби з кіберзлочинністю, оскільки

вони є як конкретною життєвою обставиною, так і юридичним явищем. Останнє з названого й викликає найбільшу увагу з огляду на здатність факту об'єктивної реальності мати юридичні ознаки та характеристики, передбачені правовою нормою.

Таким чином, забезпечення ефективної боротьби з кіберзлочинністю на сучасному етапі суспільного розвитку вимагає належного міжнародного нормативно-правового регулювання, тому доцільно вивчити сучасний стан відповідної правової бази та визначити основні напрями для удосконалення.

2.2 Особливості міжнародно-правового регулювання боротьби з кіберзлочинністю

Міжнародно-правове регулювання боротьби з кіберзлочинністю відіграє надзвичайно важливу роль, що зумовлено трансграничністю відповідних злочинів, складністю пошуку виконавців та замовників таких протиправних кримінально караних діянь, необхідність застосування сучасних технічних й інформаційних технологій тощо, зумовлюють активізацію до міжнародно-правових актів з цих питань.

У тій чи іншій мірі дана проблематика була предметом дослідження наступних науковців: Р.Г. Бєляков [78], Г.П. Власова [79], О.В. Голубєва [80], С.В. Горова [81], С.В. Демедюк [82], С.Г. Каланча [83], Р.В. Лук'янчук [84], Н.В. Люта [85], В.В. Марков [86], М.В. Менджул [87], Ю.Ю. Орлов [88], К.М. Рудой [89], Н.В. Савчук [90], Т.Л. Сироїд [91], Є.Д. Скулиш [92], В.Г. Хахановський [93] та інші. Тим не менш, досі не було виділено вченими конкретні особливості міжнародно-правового регулювання боротьби з кіберзлочинністю, що й зумовило нагальність даного дослідження.

Джерела міжнародно-правового регулювання відповідного кола суспільних відносин можна поділити на дві великі групи: 1) універсальні джерела та 2) регіональні джерела.

1.Універсальні джерела правового регулювання боротьби з кіберзлочинністю.

В сучасних умовах ООН взяла на себе координуючу роль у розробці як концептуальних, так і правових засад регулювання ключових питань в сфері боротьби з кіберзлочинністю. Так, у 1990 році VIII Конгрес ООН з попередження злочинності і поводження з правопорушниками ухвалив резолюцію, що закликає держави-члени ООН збільшити зусилля із боротьби з комп'ютерною злочинністю, модернізуючи національне карне законодавство, сприяти розвитку в майбутньому структури міжнародних принципів і стандартів запобігання, судового переслідування і покарання в області комп'ютерної злочинності [94]. Зростання відповідного виду злочинності, характеру та тяжкості вчинюваних злочинів та інше вимагає негайної реакції міжнародного співтовариства на відповідні негативні соціальні прояви. Саме під егідою ООН, яка об'єднує найбільшу кількість держав світу доцільно проводити діяльність щодо розробки та запровадження міжнародно-правового регулювання досліджуваних суспільних відносин. Прийняття відповідної резолюції, яка окреслила рамкові домовленості, стало одним з перших кроків на шляху до створення міжнародно-правової бази з проблематики боротьби з кіберзлочинністю.

У 1995 році в Ліоні (Франція) була проведена міжнародна конференція Інтерполу з комп'ютерної злочинності. За підсумками конференції був зроблений висновок, що у більшості країн світу спостерігається усе зростаюче використання інформаційних технології в кримінальній діяльності. Це викликає необхідність постійного вивчення цього кримінального прояву, оскільки розвиток комп'ютерних технології призводить до використання цих інновацій при скоєні комп'ютерних злочинів. Підхід Інтерполу до боротьби з кіберзлочинністю полягає в тому, щоб використовувати досвід його членів у боротьбі із злочинами у сфері інформаційних технологій шляхом функціонування робочих груп або

експертних груп. Робочі групи створюються для вивчення регіонального досвіду і існують в Європі, Азії, Африці і Північній і Південній Америці [95]. Відповідне обговорення сприяло розвитку міжнародно-правового співробітництва у сфері боротьби з кіберзлочинністю, але недоліком відповідного заходу було те, що акцентувалася увага саме на комп'ютерних злочинах, в той час як інформаційні злочини є значно ширшими й охоплюють також й електронні засоби зв'язку, електронні мережі тощо.

У 1997 році міністри внутрішніх справ і міністри юстиції Великої Вісімки на зустрічі у Вашингтоні прийняли «Десять принципів боротьби з високотехнологічними злочинами», що включають, у тому числі, положення про те, що для тих, хто зловживає інформаційними технологіями, не повинно бути ніяких зон безпеки. Правова система повинна забезпечити захист конфіденційності, цілісності і придатності даних і систем від протиправного ушкодження і гарантувати покарання за серйозні правопорушення [96]. Зміст відповідного документу містить досить прогресивні положення, однак його суттєвим недоліком є те, що для повноцінної діяльності з протидії кіберзлочинності потрібно залучення значної кількості держав до відповідних процесів, лише за таких умов можливо досягти необхідного результату. Тому відповідний програмний документ, хоча й був базисом для розробки наступних нормативних документів, проте не відіграє істотної ролі у міжнародно-правовому регулюванні боротьби з інформаційною злочинністю.

Згодом в рамках ООН відповідна діяльність проводилася у таких напрямках як:

1) боротьба із злочинним використанням інформаційних технологій (Резолюції ГА ООН «Боротьба із злочинним використанням інформаційних технологій» № 55/63 від 4 грудня 2000 року, № 56/121 від 19 грудня 2001 року);

2) міжнародна інформаційна безпека (Резолюції ГА ООН «Досягнення в сфері інформації та комунікації в контексті міжнародної безпеки» № 53/70 від 4 грудня 1998 року, № 54/49 від 1 грудня 1999 року, № 55/28 від 20 листопада 2000 року, № 56/19 від 29 листопада 2001 року, № 57/53 від 22 листопада 2002 року, № 58/32 від 8 грудня 2003 року, № 59/61 від 3 грудня 2004 року, № 60/45 від 8 грудня 2005 року, № 61/54 від 6 грудня 2006 року, № 62/17 від 5 грудня 2007 року, № 63/37 від 2 грудня 2008 року, № 64/25 від 2 грудня 2009 року, № 65/41 від 8 грудня 2010 року, № 66/24 від 13 грудня 2011 року);

3) створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур (Резолюції ГА ООН «Створення глобальної культури кібербезпеки і захист найважливіших інформаційних структур» №57/239 від 20 грудня 2002 року, № 58/199 від 23 грудня 2003 року, № 64/211 від 21 грудня 2009 року).

Важливі питання співробітництва держав у боротьбі із злочинним використанням інформаційно-комунікаційних технологій було покладено на Міжнародний союз електрозв'язку. Результатом діяльності стало прийняття вказаним суб'єктом Глобальної програми кібербезпеки [97, с. 174], яка визначила цілі, принципи і стратегії розробки моделей законодавства в сфері боротьби з комп'ютерною злочинністю. В якості першочергових цілей Глобальної програми було визначено:

1) формування стратегій розробки типового законодавства з боротьби із кіберзлочинністю, яке можна застосовувати у глобальному масштабі і яке буде сумісним з чинними національними і регіональними законодавчими актами;

2) формування глобальних стратегій для створення належних національних і регіональних організаційних структур, а також політики в області боротьби із кіберзлочинністю;

3) розробка стратегії для встановлення прийнятних на глобальному рівні мінімальних критеріїв безпеки та схем авторизації апаратних засобів, програмних додатків і систем;

4) розробку стратегій для створення глобальної структури для нагляду, оповіщення і реагування на інциденти для забезпечення міжнародної координа-ції діяльності;

5) розробка глобальних стратегій для створення і утвердження загальної і спеціальної системи цифрової ідентифікації, а також необхідних організаційних структур в цілях визнання цифрових посвідчень особи без врахування географічних кордонів;

6) розробка глобальної стратегії в цілях сприяння розвитку людського і інституційного потенціалів для збільшення знань та ноу-хау;

7) підготовка пропозицій на основі глобальної стратегії, заснованої на участі багатьох зацікавлених сторін, в цілях налагодження міжнародного співробітництва, діалогу та координації діяльності [97, с. 176]. Згодом на виконання запланованих заходів була прийнята низка резолюцій МСЕ, які спрямовувалися спрямована на зміцнення довіри та безпеки при використанні інформаційно-комунікаційних технологій і боротьбі із комп'ютерними злочинами.

Особливості універсального міжнародно-правового регулювання боротьби з кіберзлочинністю є таке: 1) відповідна діяльність акумулюється навколо ООН та її органів або створених за її підтримки суб'єктів; 2) на сьогодні наявні виключно програмні та інші стратегічні документи, які повинні закласти основи міжнародно-правового регулювання відповідного кола відносин; 3) основними напрямами діяльності має бути створення й розробка організаційних та законодавчих заходів протидії кіберзлочинності, а також питання взаємодія у даній сфері діяльності; 4) наявна необхідність у створенні міжнародних спільних органів оперативно-розшукової діяльності

для забезпечення фіксування слідів вчинених злочинів; 5) удосконалення взаємодії між компетентними органами різних держав; 6) існує нагальна потреба розробки й прийняття універсальних конвенцій з відповідних питань, які би забезпечили участь більшості держав у відповідних заходах проти кіберзлочинності.

2.Регіональні джерела правового регулювання боротьби з кіберзлочинністю.

З 1985 по 1989 р. Спеціальний Комітет експертів Ради Європи з питань злочинності, пов'язаної з комп'ютерами, виробив *Рекомендацію №89, затверджену комітетом Міністрів ЄС 13 вересня 1989 року* [98]. Рекомендація містить два списки злочинів – «мінімальний» і «факультативний (додатковий)». «Мінімальний» список включає діяння, які обов'язково мають бути заборонені міжнародним законодавством і підлягають переслідуванню в судовому порядку. «Додатковий» список містить ті правопорушення, по яких досягнення міжнародної згоди представляється скрутним. Вона містить список правопорушень, рекомендований країнам-учасницям ЄС для розробки єдиної карної стратегії, пов'язаної з комп'ютерними злочинами. Також в документі відмічена необхідність досягнення міжнародного консенсусу з питань криміналізації деяких злочинів, пов'язаних з комп'ютерами [98]. Відповідний документ був одним з перших у сфері протидії вчиненню інформаційних злочинів у Європі і його головна роль полягає в тому, що він лежав в основі удосконалення відповідних інститутів кримінального права переважної більшості європейських держав.

Законодавство Європейського Союзу у сфері інформаційної безпеки розвивалося у руслі міжнародних ініціатив Ради Європи, Організації економічного співробітництва і розвитку, Міжнародного Союзу Електрозв'язку, Організації Об'єднаних Націй. Законодавчі заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програм Європейського Союзу –

«Безпечний Інтернет» (1999-2004 рр.), «Безпечний Інтернет Плюс» (2005–2008 рр.), «Безпечний Інтернет 2009-2013 рр.», прийнятих рішеннями Європейського Парламенту і Ради, і переважно були спрямовані на захист персональних даних, сприяння безпечному користуванню Інтернетом, формуванню сприятливого середовища для розвитку європейської Інтернет-індустрії, захист дітей, що користуються Інтернетом і новими інформаційними технологіями. Найважливіші заходи у боротьбі із кіберзлочинністю здійснювалися у рамках програми Європейського Союзу «Попередження і боротьба із злочинністю» і передбачали співробітництво в протидії кіберзлочинності. Складність та чисельність питань інформаційної безпеки сформувала в законодавчих органах Європейського Союзу концептуальне бачення майбутнього міжнародно-правового регулювання виключно на рівні, спрямованому на вирішення кримінальних аспектів, пов’язаних із використанням інформаційно-комунікаційних технологій. В Європейському Союзі не було сприйнято концепцію міжнародної інформаційної безпеки, яка передбачала б комплексне розв’язання проблеми на трьох рівнях міжнародно-правового регулювання – військовому, терористичному і кримінальному.

Провідне місце серед відповідної групи міжнародно-правових документів відведено *Конвенції Ради Європи про кіберзлочинність від 23 листопада 2001 року* (Будапешт) [99]. Наша країна ратифікувала цю Конвенцію 7 вересня 2005 року. На сьогодні це один з найважливіших документів, які регулюють правовідносини у сфері глобальної комп’ютерної мережі і доки єдиний документ такого рівня [99]. Нею на держави покладаються зобов’язання щодо вживання законодавчих та інших заходів, які можуть бути необхідними для встановлення кримінальної відповідальності відповідно до її внутрішнього законодавства за злочини в кіберпросторі.

Ще до підписання Конвенції деякі групи по захисту громадянських прав і провайдери інтернет-послуг приводили серйозні аргументи проти укладення цього договору, який на їх погляд має неясні формулювання і пред'являє провайдерам непосильні вимоги, зокрема відзначається, що Конвенція несе в собі загрозу для норм захисту особи, що встановилися, невиправдано розширює поліцейські функції уряду, а також знижує відповідальність держави в правоохоронній діяльності.

Перший розділ Конвенції присвячений видам діянь, що підлягають криміналізації, так всі злочини в кіберпросторі вона поділяє на 4 групи:

1) у першу групу злочинів, спрямованих проти конфіденційності, цілісності і доступності комп'ютерних даних і систем входять: незаконний доступ (ст. 2), незаконне перехоплення (ст. 3), дія на комп'ютерні дані (ст. 4) або на системи (ст. 5). Також до цієї групи злочинів входить протизаконне використання спеціальних технічних пристроїв (ст. 6). Об'єктом злочину виступають не лише комп'ютерні програми, розроблені або адаптовані для скоєння злочинів, передбачених в ст.ст. 2-5 Конвенцій, але і комп'ютерні паролі, коди доступу і їх аналоги, за допомогою яких може бути отриманий доступ до комп'ютерної системи в цілому або будь-якій її частині (з урахуванням злочинного наміру). Норми ст. 6 Конвенцій застосовні тільки у тому випадку, якщо використання (поширення) спеціальних технічних пристроїв спрямоване на здійснення протиправних діянь.

2) до другої групи входять злочини, пов'язані з використанням комп'ютерних засобів: підлог і шахрайство з використанням комп'ютерних технологій (ст. 7, 8 Конвенцій).

3) третю групу складають злочини, пов'язані з контентом (змістом) даних.

4) до четвертої групи увійшли порушення авторського права і суміжних прав [99]. На початку 2002 року до Конвенції ухвалили протокол,

що додає в перелік злочинів поширення інформації расистського і іншого характеру, що підбурює до насильницьких дій, ненависті або дискримінації окремої особи або групи осіб, що ґрунтуються на расовій, національній, релігійній або етнічній приналежності.

Другий розділ Конвенції освітлює процесуальні аспекти боротьби з кіберзлочинністю. Конвенція пропонує традиційне рішення проблеми юрисдикції: карна юрисдикція визначається відповідно до територіальної ознаки (територія держави; борт судна або літака держави). Проте у разі, якщо злочин скоєний поза територіальною юрисдикцією держави, то застосовується карне законодавство тієї держави, громадянином (підданим) якої є злочинець. Тут виникає неясність: незрозумілий статус кіберпростору - чи поширюється на нього національне законодавство або ні? Таким чином, проблема визначення підвідомчості і осудності злочинів в кіберпросторі як і раніше залишається відкритою. Щоб уникнути можливих подальших суперечок в Конвенції передбачається, що внутрішні закони держав можуть містити інші норми про юрисдикцію. Зважаючи на відсутність кордонів в глобальних мережах, Конвенція уточнює ситуацію колізії юрисдикції декількох держав: у такому разі, згідно п. 5 ст. 22, держави повинні проводити консультації для визначення відповідної юрисдикції для судового переслідування [99]. Конвенція про кіберзлочинність на сьогодні є одним з базових міжнародно-правових актів у сфері права телекомунікацій, рахом з тим, й вона не позбавлена недоліків.

Глава III Конвенції – «Міжнародна співпраця» - присвячена питанням екстрадиції, спільній діяльності держав-учасників у сфері боротьби з комп'ютерними злочинами і досягнення узгодженості для збору доказів в електронній формі [99]. Прийняття Конвенції послужить фундаментом для міжнародного законодавства, що формується, навіть ті країни, які з яких-небудь причин не підписали Конвенцію можуть використовувати досвід, що

накопичується, по правовому регулюванню нової предметної області – кіберпростір.

Отже, Конвенція про кіберзлочинність [1] є одним із найважливіших документів у сфері глобальної комп'ютерної мережі, роль якої у регулюванні боротьби з кіберзлочинністю у державах всього світу є вирішальною. Щодо України, значення даного міжнародного нормативно-правового акту можна виразити наступним чином. По-перше, Конвенцією здійснено розмежування кіберзлочинів залежно від об'єкта посягання на 1) правопорушення проти конфіденційності, цілісності та доступності комп'ютерних даних і систем, 2) правопорушення, пов'язані з комп'ютерами, 3) правопорушення, пов'язані зі змістом, 4) правопорушення, пов'язані з порушенням авторських та суміжних прав. Схожим чином, класифікують такі правопорушення і у національних законодавствах країн-учасниць, зокрема в Розділі XVI Кримінального кодексу України [3]. По-друге, Конвенцією регламентовано процедурні аспекти, такі як умови, запобіжні заходи, обшук і арешт комп'ютерних даних, які зберігаються, збирання даних про рух інформації у реальному масштабі часу, перехоплення даних змісту інформації, юрисдикція тощо. Така систематизація значним чином полегшує діяльність правоохоронних органів держави. По-третє, даним документом встановлено принципи співробітництва країн-учасниць у сфері боротьби з кіберзлочинністю, зокрема – екстрадиції та взаємодопомоги. Відзначимо, що реалізація цього аспекту здійснюється шляхом укладення державами двосторонніх угод. Як вже засвідчив їх аналіз, на практиці Україна надає перевагу реалізації принципу взаємодопомоги. По-четверте, Конвенція надає право учасникам здійснювати доступ до публічно доступних комп'ютерних даних, які зберігаються, не отримуючи дозволу від іншої сторони, що значним чином полегшує розслідування злочинів та дозволяє уникати надмірного затягування оперативно-розшукової діяльності.

Конвенція про кіберзлочинність є важливою основою діяльності Національної поліції України, проте, деякі її положення так і не знайшли відображення у вітчизняному кримінальному законодавстві. Наприклад, виробництво, продаж, придбання для використання, імпорт, оптовий продаж чи інші форми надання в користування комп'ютерних паролів, кодів доступу чи інших аналогічних даних, за допомогою яких може бути отримано доступ до комп'ютерної системи в цілому чи будь-якої її частини з наміром використати їх з метою вчинення комп'ютерних злочинів, придбання дитячої порнографії через комп'ютерну систему та володіння дитячою порнографією, що перебуває в комп'ютерній системі чи на носіях комп'ютерних даних не знайшли свого втілення у вітчизняному кримінальному законодавстві [1]. Проблема полягає у тому, що з однієї сторони правоохоронці наділені правом керування у своїй діяльності нормами Конвенції про кіберзлочинність, проте з іншої – на практиці вони майже не використовують їх, тож перенесення міжнародних стандартів на вітчизняну практику боротьби з кіберзлочинністю є не в повній мірі коректним твердженням. Проте, не зважаючи на такі суперечності, Конвенція про кіберзлочинність все ще залишається одним із найважливіших інструментів національного правового регулювання боротьби із кіберзлочинністю.

Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40] не є нормативно-правовим актом, яким безпосередньо врегульовується питання боротьби із кіберзлочинністю. Проте, комп'ютерна злочинність переважно має транснаціональний характер, є організованою та може набувати ознак тероризму. А отже, прийняття Конвенції, спрямованої на попередження та боротьбу із даними видами злочинних діянь є важливим інструментом у боротьбі з кіберзлочинністю.

Конвенцією Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40] запропоновано ухвалення

законодавчих та інших заходів, спрямованих на заходи проти корупції і відповідальності юридичних осіб за участь останніх у серйозних злочинах, до яких причетна організована злочинність; заходи які можуть забезпечувати можливості конфіскації та арешту доходів від злочинів і розпорядження конфіскованими доходами від злочинів тощо. С. А. Шепетько в даному контексті зазначає, що норми Конвенції не застосовуються щодо правопорушень, які не відносяться до організованої злочинності, розглядаючи, як виняток, лише окремі сфери – особливо комп'ютерних правопорушень, оскільки дана проблема потребує більшої уваги з боку міжнародної спільноти [100, с. 300]. Тобто, у разі якщо кіберзлочин має транснаціональний характер, а саме, планується чи вчиняється в кількох державах, або вчиняється в одній державі, а має істотні наслідки в іншій, можуть бути застосовані норми Конвенції.

Варто відзначити, що загальна кількість міжнародних договорів у сфері співробітництва у кримінальних справах є значною. Ще з моменту проголошення незалежності, Україна активно укладала подібні угоди і на сьогодні співпрацює з кількома десятками держав різних континентів. Проте, більшість із них ніяким чином не регламентують співпрацю у сфері боротьби з кіберзлочинністю, що у цілому не виключає такої можливості у разі виникнення необхідності. Наприклад, Угода між Кабінетом Міністрів України і Урядом Турецької Республіки про співробітництво передбачає надання взаємної допомоги в попередженні й розкритті кіберзлочинів [101]. Це означає, що у разі виникнення такої необхідності правоохоронні органи обох держав зобов'язані всебічно та двосторонньо сприяти діяльності один одному. Для порівняння аналогічна угода із Сполученими Штатами Америки взагалі не містить посилання на сфери співпраці, обмежуючись формулюванням «взаємна допомога у розслідуванні, переслідуванні та запобіганні злочинам, а також у судовому розгляді кримінальних справ» [102]. Це свідчить про те, що конкретна співпраця у сфері боротьби із

кіберзлочинністю не передбачена, проте і не виключена у разі виникнення таких проблемних питань.

Також відмітимо наявність міждержавних угод Генеральної прокуратури України із головними органами прокуратури інших держав. Зокрема, в 2015 році було укладено Угоду про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія у боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом [103]. Подібні угоди були укладені зокрема і з Національною прокуратурою Королівства Нідерланди [104] та державами пострадянського простору. Текст кожного з договорів фактично є тотожним – сторони беруть на себе зобов'язання здійснювати співробітництво в сфері боротьби з кіберзлочинністю шляхом обміну інформацією і документами стосовно таких злочинів. Не зважаючи на дещо усічений перелік напрямів співробітництва, значення таких угод варто виразити наступним чином: 1) Україну як порівняно новоутвореного суб'єкта міжнародних відносин поступово залучають до міждержавних процесів; 2) ураховуючи специфіку злочинності у кіберпросторі, нашій державі гарантована допомога у разі виникнення такої необхідності; 3) іноземні держави вважають вітчизняні правоохоронні органи такими, що можуть посприяти вирішенню їх внутрішніх проблем. Разом з тим, сама сфера реалізації таких угод потребує розширення. Аналіз їх змісту засвідчив, що основною формою співробітництва є надсилання запитів про інформацію. В умовах швидкості вчинення кіберзлочинів даний інструмент може бути неефективним, адже потребує значної кількості часу. А отже, порядок укладення Україною міжнародних угод у сфері взаємної правової допомоги в розслідуванні кіберзлочинів також потребує подальшого удосконалення.

Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації від 1 червня 2001 року [44] покладає на держави зобов'язання

щодо визнання у відповідності з національним законодавством в якості кримінальних злочинів:

1) здійснення неправомірного доступу до комп'ютерної інформації, що охороняється законом, якщо це потягло знищення, блокування, модифікацію або копіювання інформації, порушення роботи ЕОМ, системи ЕОМ або їхньої мережі;

2) створення, використання або поширення шкідливих програм;

3) порушення правил експлуатації ЕОМ, системи ЕОМ або їхньої мережі особою, що має доступ до ЕОМ, системи ЕОМ або їхньої мережі, що потягло знищення, блокування або модифікацію інформації ЕОМ, що охороняється законом, якщо це спричинило суттєву шкоду або тяжкі наслідки;

4) протизаконне використання програм для ЕОМ та баз даних, що є об'єктами авторського права, так само як і присвоєння авторства [44]. Однак для повноцінної реалізації відповідних завдань необхідно було узгодити чіткий перелік відповідних злочинних діянь та покарання за них. На практиці не всі держави, які є учасницями СНД реалізували відповідні завдання, що суттєво знижує протидію інформаційній злочинності, яка потребує комплексного транснаціонального співробітництва.

В *Угоді між урядами держав-членів Шанхайської організації співробітництва про співробітництво в області забезпечення міжнародної інформаційної безпеки, прийнятій 16 червня 2009 року* [105], питання інформаційної злочинності розглянуто в загальному контексті з основними напрямами, принципами, формами і механізмами міжнародного співробітництва. Варто зазначити, що на відміну від попередніх,Угода передбачає новий концептуальний підхід до питань забезпечення міжнародної інформаційної безпеки. Його суть полягає у комплексному забезпеченні міжнародної інформаційної безпеки держав від усіх

інформаційних загроз, що можуть бути спричинені злочинним використанням ІКТ. Виходячи з цих позицій, інформаційна злочинність, разом із п’ятьма іншими, визнана сторонами Угоди в якості основної загрози в області забезпечення міжнародної інформаційної безпеки. Джерелом цієї загрози, відповідно до Угоди, є особи або організації, що здійснюють неправомірне використання інформаційних ресурсів або несанкціоноване втручання в такі ресурси у злочинних цілях [105].

З метою протидії інформаційній злочинності, сторони Угоди погодились співробітничати і проводити свою діяльність у інформаційному просторі таким чином, щоб така діяльність сприяла соціальному і економічному розвитку і була сумісною з задачами підтримки міжнародної безпеки і стабільності, відповідала загальновизнаним принципам міжнародного права. Така діяльність повинна бути сумісною з правом кожної сторони Угоди шукати, отримувати і поширювати інформацію з урахуванням можливих обмежень з причин захисту інтересів національної та суспільної безпеки (ст. 4). Сторони визнали право на захист інформаційних ресурсів і критично важливих структур від неправомірного використання і несанкціонованого втручання, погодились не проводити одна проти одної подібних дій та сприяти одна одній в реалізації цього права [105]. Істотним недоліком відповідного міжнародно-правового документу було те, що не зважаючи на декларування необхідності боротьби з кіберзлочинністю, він не містить реальних заходів. Тобто відсутні зобов’язання держав-учасниць внести зміни в національне законодавство, які би сприяли реальній протидії інформаційний злочинам. Сутність відповідного документу зводиться до характеристик загроз інформаційних злочинів, необхідності консолідації зусиль держав тощо.

В рамках Азійсько-Тихоокеанської економічної співдружності у 2002 році була прийнята «Стратегія кібербезпеки АТЕС», передбачається прийняття зводу законів щодо кібербезпеки та кіберзлочинності, а також

створення національних підрозділів з кіберзлочинності та центрів технологічної допомоги. Ліги арабських держав і Організації американських держав розвивають співробітництво у боротьбі із комп'ютерними злочинами з урахуванням рекомендацій ООН, МСЕ, Ради Європи.

Діяльність *Організації економічного співробітництва і розвитку*, розпочата за тематикою комп'ютерної злочинності ще 1983 року, спрямовується на проведені досліджень, пов'язаних із можливістю гармонізації кримінального законодавства щодо комп'ютерних злочинів. У 1992 році радою ОЕСР було прийнято «Керівні принципи з інформаційної безпеки». У 2002 році нова версія принципів «Керівні принципи ОЕСР із забезпечення безпеки інформаційних систем і мереж: до культури безпеки» була рекомендована Радою ОЕСР. Останні доповіді були присвячені темам боротьби зі спамом (2005 рік), та законодавчих рішень держав щодо проблеми кібертероризму (2007 рік).

Особливостями регіонального міжнародно-правового регулювання протидії кіберзлочинності можна визначити таке: 1) значна увага з боку різноманітних регіональних міжнародних організацій до питань протидії кіберзлочинам; 2) розробка численних регіональних угод про співробітництво у сфері протидії інформаційним злочинам; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. - на початку 2000-х рр.; 4) така діяльність є складовою частиною як міжнародних інформаційних відносин, так і кримінального судочинства.

Проведене доктринальне дослідження дає підстави стверджувати, що для створення умов щодо належної й ефективної діяльності по протидії кіберзлочинності недостатньо ресурсів одного правоохоронного орану або правоохоронних оранні певної держави. Така діяльність повинна мати комплексний характер й передбачати участь багатьох країн, що вимагає необхідного нормативно-правового базису на міжнародному рівні. На

сьогодні відбуваються дії стосовно встановлення засад міжнародної співпраці у сфері протидії кіберзлочинності у рамках як універсальних, так і регіональних договорів. Разом з тим, таких заходів для повноцінної діяльності недостатньо, що вимагає пожвавлення діяльності з боку кожного суб'єкта міжнародного співтовариства з метою створення дієвого механізму міжнародно-правового регулювання протидії кіберзлочинності.

2.3 Національне правове регулювання боротьби з кіберзлочинністю та механізм його забезпечення

Категорії, пов'язані із правовим регулюванням боротьби з кіберзлочинністю, переважно закріплюють основні системні поняття та механізми, та узагальнюють його властивості. Останнім часом вченими приділяється більше уваги аналізу закономірностей побудови та розвитку системи правового регулювання боротьби з кіберзлочинністю із огляду на її внутрішню організацію як складної системи, яку становлять також складні за побудовою підсистеми. Це можна пояснити наявністю незначної кількості робіт, присвячених даній тематиці та актуалізації даного питання на практичному та науковому рівнях.

Дослідження національного правового регулювання боротьби з кіберзлочинністю дозволить встановити сучасний стан регламентації даного інституту, встановити закономірності та позитивні моменти щодо його функціонування. Окрім того, важливим є встановлення того, як саме відбувається втілення механізму його забезпечення для формування розуміння ролі кожного із прийнятих чи ратифікованих нормативно-правових актів і встановлення напрямів для подальшого розвитку даного інституту.

Інститут у процесі свого розвитку має здатність змінюватись чи піддаватись зовнішньому впливу, переходити у якісно новий стан, оновлювати власні елементи чи структуру, при цьому зберігаючи свою цілісність та ідентичність. Постійна еволюція вітчизняного законодавства зумовлює втрату актуальності змісту багатьох наукових праць та розуміння змісту ключових категорій, пов'язаних із національним правовим регулюванням боротьби з кіберзлочинністю. Саме тому, питання національного правового регулювання боротьби з кіберзлочинністю та механізму його забезпечення не втрачає своєї доцільності та завжди залишається актуальним для дослідження.

У вітчизняній науці правове регулювання боротьби з кіберзлочинністю перебуває у колі наукових інтересів дослідників протягом останніх двох десятиліть з моменту формування даного інституту у вітчизняній правовій системі. Варто відмітити, що такі дослідження здійснюються у формах монографій, статей, розділів наукових робіт, аналітичних записок та навіть у публіцистиці. Важливий доробок у розвиток інституту національного правового регулювання боротьби з кіберзлочинністю внесли такі учені, як: В. М. Бутузов, В. В. Василевич, В. Б. Дзюндзюк, Д. В. Дубов, О. Є. Користін, О. С. Луньова, О. В. Манжай, М. А. Ожеван, Ю. М. Онищенко, О. В. Орлов, С. А. Шепетько та інші. Проте, кількість таких робіт є незначною і переважна більшість із них не розкриває належним чином тему нашого дослідження. Тож, питання національного правового регулювання боротьби з кіберзлочинністю та механізму його забезпечення все ще залишаються недослідженими, що і зумовлює актуальність обраної теми.

27 червня Україна зазнала масових кібератак шляхом впливу на комп'ютерні системи невідомого на той момент вірусу. В результаті вірус «Petya.A» або «mbr locker 256» спричинив порушення роботи українських державних підприємств, установ, банків, медіа тощо. Негативний вплив було здійснено навіть на веб-ресурси кіберполіції та Служби спецзв'язку України, що є вагомою проблемою, адже дані органи є суб'єктами боротьби із

кіберзлочинністю у нашій державі [106]. Дана атака продемонструвала недоліки та вразливість національного правового регулювання даної проблеми, а також відсутність у вітчизняній науці відповіді на питання, якими є елементи зазначеного механізму. Тому, важливим є встановлення кожного структурного елементу досліджуваної системи та формування розуміння того, яким чином здійснюється забезпечення її функціонування.

У становленні національного правового регулювання боротьби з кіберзлочинністю найсуттєвішим фактором є виникнення механізму, який дасть можливість запровадження єдиного безперервно діючого порядку у суспільних відносинах та підпорядкувати поведінку людей загальним і однаковим умовам, що диктуються вимогами суспільного життя. Сам термін «регулювання» означає впорядкування чого-небудь, керування чимось, підпорядковуючи його відповідним правилам чи певній системі [107, с. 1207]. Тобто, дане поняття можна роз'яснити як визначення та регламентування поведінки людей, закріплення її меж, та спрямування її розвитку за допомогою встановлення певних норм. Одним із різновидів регулювання є правове, тобто те, що здійснюється за допомогою норм права, які поширюються на усі випадки суспільних відносин певного виду. Іншими словами, правовим регулювання є упорядкування поведінки осіб і керування нею, що здійснюється за допомогою встановлених та санкціонованих державою правил, які поширюються на усі випадки, передбачені відповідними суспільними відносинами, та усіх суб'єктів, що вступили у нормативно-регламентовані суспільні відносини.

На сьогодні у вітчизняній правовій науці відсутня єдність позицій щодо визначення і суті поняття «правове регулювання». Найбільш розповсюдженими наразі є два підходи до розуміння даної категорії – широкий та вузький. Вузький підхід передбачає упорядкування суспільних відносин виключно шляхом застосування нормативних юридичних засобів [108, с. 263]. Таку концепцію вважаємо доцільною для досліджуваного правового інституту, адже боротьба із кіберзлочинністю в усьому світі

здійснюється шляхом прийняття законодавства у відповідній сфері. Проте, важливим є зазначення того, що в силу специфіки даної сфери, злочинці у всесвітній мережі можуть виступати анонімно чи безвідносно до території конкретної держави. Тому, вагому роль у врегулюванні боротьби із кіберзлочинністю в усьому світі відіграють міждержавні угоди, укладені з метою співпраці у даній сфері, та конкретизації норм вітчизняних законодавств. Тож, вузького підходу до правого регулювання даного інституту є недостатньо.

Згідно широкого, до складу системи правового регулювання відносяться усі форми впливу на свідомість та поведінку суб'єктів суспільних відносин, тобто як нормативні, так й індивідуальні. Наприклад, Л. П. Рассказов розглядає індивідуальне регулювання як упорядкування поведінки людей за допомогою разових рішень, що стосуються конкретного випадку чи конкретної особи [109, с. 238]. Тобто, окрім власне нормативно-правових актів, згідно такої концепції до сфери правового регулювання відносяться певні рішення по організації суспільних відносин, які мають додатковий характер та деталізують поведінку їх суб'єктів. Відштовхуючись від сутності досліджуваного поняття, відзначимо, що таку характеристику доцільно надати певним договорам, які укладаються для врегулювання відносин певних суб'єктів. Вважаємо, що ними можуть бути й укладені міжнародні двосторонні чи багатосторонні угоди щодо співпраці із міжнародними організаціями, обміну інформацією, правовою допомогою, відомостями оперативно-розшукового характеру, прийняття працівників правоохоронних органів іноземних держав в Україні тощо.

Формуючи розуміння того, які ж саме інструменти відносяться до сфери правового регулювання боротьби з кіберзлочинністю в нашій державі, варто здійснити звернення до ще одного критерію. Серед різновидів правового регулювання виділяється законодавче регулювання, тобто основне, що передбачає регулювання певного інституту суспільних відносин, та підзаконне, що здійснюється правовими нормами, закріпленими в

підзаконних нормативно-правових актах держави й актах об’єднань громадян [110, с. 263]. Оскільки обидва різновиди можуть бути характерними для сфери регулювання боротьби із кіберзлочинністю, пропонуємо вживати термін «національне правове регулювання боротьби з кіберзлочинністю», що об’єднає всі законні та підзаконні нормативно-правові акти, а також міжнародні договори і угоди, укладені Україною.

Отже, національне правове регулювання боротьби з кіберзлочинністю в Україні – це впорядкування поведінки осіб у кіберпросторі та керування нею, що здійснюється за допомогою встановлених, санкціонованих чи ратифікованих державою законних та підзаконних нормативно-правових актів, а також міжнародних договорів і угод, укладених Україною, які поширюються на усі випадки деструктивної діяльності у кіберпросторі, та усіх суб’єктів, що вступили у нормативно-регламентовані суспільні відносини.

Належне дослідження інструментів національного правового регулювання боротьби з кіберзлочинністю потребує структурування усього масиву законних та підзаконних нормативно-правових актів, а також міжнародних договорів і угод, укладених Україною. Звертаючись до правової доктрини нашої держави, звернемо увагу на те, що таке групування вітчизняними дослідниками наразі не здійснювалось. Наприклад, О. В. Манжай, досліджуючи проблеми нормативно-правового забезпечення боротьби із кіберзлочинністю в Україні, поділяє засоби наступним чином. Передусім виділено Основний Закон [6] та Конвенцію про кіберзлочинність [1] як основні нормативно-правові акти у даній сфері. До другої групи віднесено норми Кримінального кодексу України [3] та Кримінального процесуального кодексу України [7], закони України «Про інформацію» № 2657-XII від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994 тощо. Третю групу становить нормативно-правове забезпечення роботи підрозділів, які безпосередньо виконують функції з протидії порушенням у кіберпросторі

[38, с. 646-649]. Із такою класифікацією погодимось не в повній мірі. По-перше, потрібно відзначити, що Конвенція про кіберзлочинність є не єдиним міжнародним нормативно-правовим актом, ратифікованим нашою державою. Тому, аналізуючи національне правове регулювання боротьби з кіберзлочинністю варто ширше розкрити дану групу. По-друге, взагалі знехтувано підзаконними нормативно-правовими актами, які є нечисленними, проте все ж відіграють вагому роль у регулюванні досліджуваного інституту. По-третє, сам перелік законодавчих актів є неповним та потребує суттєвого доповнення. Із позитивних рис даної позиції відзначимо виокремлення в єдину групу нормативно-правових актів, які врегульовують діяльність органів, що виконують функції з протидії порушенням у кіберпросторі.

О. С. Луньова, досліджуючи аспекти правового регулювання розслідування кіберзлочинів в Україні, критерієм групування нормативно-правових актів обрала хронологічний порядок їх прийняття, що є не доцільним підходом у даному випадку [111, с. 107-109]. Такий підхід не є вдалим, адже ускладнює можливість здійснити групування та не дає змоги виділити характерні особливості кожної з груп. На наше переконання подібна класифікація є можливою лише за умови виділення характерних особливостей правового регулювання розслідування кіберзлочинів на кожному окремому історичному етапі, що не було здійснено дослідницею.

О. В. Орлов та Ю. М. Онищенко, досліджуючи нормативно-правові засади боротьби з кіберзлочинністю, взагалі обмежились наступною вказівкою: «Правовою основою по протидії комп'ютерної злочинності на національному рівні є Кримінальний кодекс України» [112, с. 22]. Тобто, у цілому, не зважаючи на те, що вітчизняні дослідники постійно звертають увагу на правове регулювання боротьби з кіберзлочинністю та механізм його забезпечення, рівень дослідження даних питань залишається вкрай низьким та полягає переважно у зазначенні переліку нормативно-правових актів, які приймались в Україні у різні історичні епохи. Більш доцільним вбачаємо

чітке групування усього законодавчого масиву за спільним критерієм та виділення характерних рис кожної із груп.

Загалом, вдалою позицією вбачаємо виділення семи форм правових актів: правовий звичай; закон (нормативно-правовий акт); правовий прецедент; нормативно-правовий договір; правова доктрина; релігійно-правова норма; міжнародно-правовий акт [113, с. 19]. Проте, наразі не кожен із них є представленим у регулюванні досліджуваного інституту. Наприклад, правові звичаї у даній сфері відсутні в силу її відносної молодості. Правові прецеденти є рівноцінним джерелом права лише у англосаксонській системі права, яка не є характерною для України. Правова доктрина у зазначеній сфері не є розвинутою належним чином, щоб бути віднесеною до механізмів національного правового регулювання боротьби із кіберзлочинністю, а релігійно-правові норми не мають жодного відношення до досліджуваного інституту.

Таким чином, варто виділити наступних три групи інструментів національного правового регулювання боротьби із кіберзлочинністю:

1) нормативно-правовий акт – у зазначеній сфері представлені як на законному, так і підзаконному рівнях;

2) нормативно-правовий договір – договори, укладені Україною з іншими державами світу у сфері боротьби із кіберзлочинністю;

3) міжнародний нормативно-правовий акт – угоди, укладені одразу кількома суб'єктами міжнародного права, ратифіковані в Україні.

Найбільшою за об'ємом групою є перша – нормативно правові акти, що здійснюють правове регулювання боротьби з кіберзлочинністю. Виділяючи лише окремі з них, відзначимо роль наступних: Конституція України, Кримінальний кодекс України, Закони України «Про інформацію» № 2657-XII від 02.10.1992, «Про захист інформації в інформаційно-телекомунікаційних системах» № 80/94-ВР від 05.07.1994, «Про державну таємницю» № 3855-XII від 21.01.1994, «Про основи національної безпеки України» № 964-IV від 19.06.2003 тощо. Проте, їх значний масив та

різноплановість свідчить про необхідність виділення окремих підвидів в рамках даної групи. Нами запропоновано здійснити поділ першої категорії на наступні різновиди:

1) законні нормативно-правові акти, що здійснюють правове регулювання боротьби з кіберзлочинністю та підзаконні нормативно-правові акти, які приймаються на основі законів, спрямовані на їх виконання та не суперечать їх змісту;

2) нормативно-правові акти, що врегульовують діяльність органів, які здійснюють боротьбу із кіберзлочинністю.

Розпочнемо із аналізу норм Конституції України, зокрема статті 17 [6]. Так, у ній зокрема зазначено наступне: забезпечення інформаційної безпеки України є однією із найважливіших функцій держави та справою всього Українського народу [6]. Формулювання «одна із найважливіших функцій держави» свідчить про те, що забезпечення інформаційної безпеки визнається одним із пріоритетних напрямків забезпечення національної безпеки України, на одному рівні із суверенітетом, територіальною цілісністю чи економічною безпекою.

Наявність даного положення свідчить про те, що на державному рівні існує усвідомлення ролі інформаційних та кібертехнологій у сучасному світі. Тому держава не просто бере на себе обов'язок здійснювати захист громадян від негативного впливу, а й делегує повноваження по протидії даному явищу громадянам. Тобто, у разі виникнення загрози кожна особа власними силами зобов'язана протидіяти кіберзлочинцям. В свою чергу держава забезпечує захист шляхом створення компетентних органів та прийняття необхідного законодавства.

Таким чином, закріплення даної норми в Основному Законі є важливою передумовою розбудови усієї системи боротьби із кіберзлочинністю. Не зважаючи на те, що саме формулювання «інформаційна безпека» не є досконалим, аналізована конституційна норма визнається одним із головних

інструментів національного правового регулювання досліджуваного інституту.

Наступний нормативно-правовий акт, що є важливою складовою правового регулювання боротьби з кіберзлочинністю – Кримінальний кодекс України [3]. Прийнятий у 2001 році, даний нормативно-правовий акт Розділом XVI вперше передбачив кримінальну відповідальність за злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж (статті 361, 362 та 363), фактично легалізувавши кримінальну відповідальність за протиправні діяння в зазначеній сфері. Щодо інших розділів, Розділом V «Злочини проти виборчих, трудових та інших особистих прав і свобод людини і громадянина» (статті 163, 176, 177) визначено деякі види злочинів, в яких закріплено поняття комп'ютерних продуктів як засобу злочину, а у Розділі VII «Злочини у сфері господарської діяльності» статтею 200 врегульовано питання незаконних дій з документами на переказ, платіжними картками та іншими засобами доступу до банківських рахунків, електронними грошима, обладнанням для їх виготовлення [3]. Тобто, значення Кримінального кодексу України як інструменту національного правового регулювання боротьби з кіберзлочинністю полягає у тому, що ним було вперше визнано злочином протиправну діяльність у кіберпросторі. Окрім того, даний нормативно-правовий акт є гарантією притягнення зловмисників до відповідальності та застосування до них санкцій. До прийняття даного законодавчого акту протиправні діяння у кіберпросторі взагалі не визначались злочинами. Саме тому, до 2001 року досвід України у боротьбі з кіберзлочинністю був мінімальним, а більшість протиправних діянь не визнавались такими, що мають високий рівень небезпечності для суспільства. Тому, значення Кримінального кодексу України варто виразити передусім як перший нормативно-правовий акт, що дозволив сформувати окремий інститут боротьби із кіберзлочинністю.

Норми чинного Кримінального процесуального кодексу [7] характеризуються своєю неоднозначністю з точки зору регулювання боротьби із кіберзлочинністю. З однієї сторони, ним закріплено такі норми, як стаття 263 - зняття інформації з транспортних телекомунікаційних мереж, стаття 264 - зняття інформації з електронних інформаційних систем та стаття 268 - установлення місцезнаходження радіоелектронного засобу, які безумовно мають вплив на регулювання боротьби із кіберзлочинністю. З іншої - аналіз статті 84, якою встановлено поняття доказів у кримінальному процесі, засвідчив що у ній відсутнє положення, яке б розширювало сутність даного явища за допомогою доказів у електронній формі. Іншими словами, на сьогодні в Україні фактично немає можливості залучати як докази наявність протиправних діянь, пов'язаних із інформацією у електронному вигляді, що є об'єктом вчинення кіберзлочинів. У такому випадку єдиним можливим варіантом доказування у кримінальній справі про кіберзлочини є висновок комп'ютерно-технічної експертизи, передбачена нормами Закону України «Про судову експертизу» від 25.02.1994 № 4038-XII [114]. Тому, зробимо висновок про недосконаліть чинного кримінального процесуального законодавства у врегулюванні питань, пов'язаних із процесом доказування в справах про кіберзлочини, проте сама наявність відповідних статей є безумовно важливим та позитивним аспектом у контексті боротьби із кіберзлочинністю.

Правове регулювання є недосконалим, проте все ж демонструє готовність держави до протистояння даному негативному явищу. Проте наявність подібних прогалин засвідчує той об'єм роботи, який ще варто реалізувати вітчизняному законодавцю. Боротьба із кіберзлочинністю є неможливою в умовах відсутності можливостей здійснювати ефективну та оперативну доказову діяльність. Тому, подальший розвиток національного правового регулювання боротьби із кіберзлочинністю пов'яжемо в тому числі із передбачення можливості залучати як докази протиправних діянь, пов'язаних із інформацією у електронному вигляді.

Щодо інших нормативно-правових актів, відзначимо прийняття Закону України «Про основи національної безпеки» від 19.06.2003 № 964-IV, у якому були закріплені поняття «комп'ютерна злочинність» та «комп'ютерний тероризм» та їх віднесення до основних реальних та потенційних загроз національній безпеці України [49]. Законом визначено, що на сучасному етапі одними з основних реальних та потенційних загроз національній безпеці України, стабільності в суспільстві, в інформаційній сфері є комп’ютерна злочинність та комп’ютерний тероризм. Важливим моментом є те, що одним із основних напрямів державної політики з питань національної безпеки України визначено вдосконалення державного регулювання розвитку інформаційної сфери шляхом створення нормативно-правових та економічних передумов для розвитку національної інформаційної інфраструктури та ресурсів, впровадження новітніх технологій у цій сфері, наповнення внутрішнього та світового інформаційного простору достовірною інформацією про Україну [49]. Щодо недоліків, даного нормативно-правового акта відзначимо, що комп’ютерна злочинність та тероризм є лише одним із різновидів кіберзлочинів, тобто врегулювання досліджуваного інституту в Законі здійснюється не в повній мірі. Проте, у цілому варто відзначити, що прийняття Закону стало одним із поштовхів до розвитку досліджуваного інституту, а отже його роль у національному правовому регулюванні боротьби із кіберзлочинністю є цілком позитивною.

В 1994 році було прийнято Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» від 05.07.1994 № 80/94-ВР [47], у якому врегульовано відносини у сфері захисту інформації в інформаційних, телекомунікаційних та інформаційно-телекомунікаційних системах. Так, об’єктами захисту даним законом визначено інформацію, яка обробляється в системі, та програмне забезпечення, яке призначене для обробки цієї інформації [47]. Хоча, як і у попередніх випадках, мова не іде про кіберзлочинність, чи кіберзлочини у широкому розумінні, основні положення даного Закону дозволяють віднести його до переліку найважливіших

інструментів національного правового регулювання боротьби з кіберзлочинністю.

Для системи права характерною є наявність таких нормативних актів, які приймають на основі і на виконання законів та не суперечать їм. Дана категорія дістала назву підзаконних нормативно-правових актів, які є широко розповсюдженими і у сфері боротьби із кіберзлочинністю. Актуальність проблеми кібербезпеки було зокрема відмічено Указами Президента: «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000, «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001, «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. за № 1193/2001 [115], «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» № 96/2016 [116] тощо.

Зокрема, Указом Президента України «Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні» від 31.07.2000 р. № 928/2000 [52] передбачено, що у зв’язку з прийняттям курсу розвитку мережі Інтернет в нашій державі, основними завданнями щодо цього визначено гарантування інформаційної безпеки держави та вдосконалення правового регулювання діяльності суб'єктів інформаційних відносин. Указом Президента України «Про деякі заходи щодо захисту державних інформаційних ресурсів у мережі передачі даних» від 24.09.2001 р. № 891/2001 [53] визначались завдання для органів виконавчої влади для підвищення рівня захисту державних інформаційних ресурсів та забезпечення інформаційної безпеки держави. Указом Президента України «Про заходи щодо вдосконалення державної інформаційної політики та забезпечення інформаційної безпеки України» від 6 грудня 2001 р. за №

1193/2001 [115] передбачалось розроблення Концепції національної інформаційної політики та інформаційної безпеки України, здійснення заходів щодо оптимізації системи державних органів, які реалізують інформаційну політику та вжиття заходів стосовно першочергової реалізації та повноцінного фінансування найактуальніших із них та інших важливих заходів забезпечення інформаційної безпеки. Проте, найважливішим моментом даного Указу вважаємо ініціацію встановлення кримінальної відповідальності за незаконне втручання в роботу телекомунікаційного обладнання та передбачення створення Міжвідомчого центру з питань боротьби із комп'ютерною злочинністю. Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» № 96/2016 [116] було затверджено Стратегію кібербезпеки України, яка визначає подальший вектор щодо створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави. Тобто, майбутній розвиток досліджуваного інституту пов'язується із реалізацією заходів, передбачених даним Указом.

Отже, роль підзаконних нормативно-правових актів полягає у деталізації відповідних правовідносин та їх регламентації. В досліджуваній сфері їх вплив виявляється у встановленні завдань, які дозволять досягти основну мету боротьби із кіберзлочинності – створити безпечні умови для користувачів та встановити захист інформаційної інфраструктури. Роль зазначених підзаконних нормативно-правових актів полягає у визначенні заходів щодо попередження та боротьби із кіберзлочинністю, та встановлення напрямів подальшого розвитку питань, пов'язаних із досліджуваним інститутом. Тобто, прийняття даних елементів механізму обумовлене необхідністю конкретизації відповідних правовідносин, та встановлення першочергових завдань механізму правового регулювання.

Запропонований перелік нормативно-правових актів, що здійснюють правове регулювання боротьби з кіберзлочинністю, є далеко не повним, тож

його розширення є цілком можливим. Проте, нами виділено об'єктивно найголовніші джерела згідно виділеному критерію. Виділяючи їх ознаки, відзначимо, що на сьогодні регламентація питань, пов'язаних із регулюванням ними боротьби із кіберзлочинністю, здійснюється ними не у повному обсязі. Ознаками національних нормативно-правових актів, що здійснюють правове регулювання боротьби з кіберзлочинністю, є:

1) системність – на сьогодні створену розгалужену систему законних та підзаконних нормативно-правових актів, які в єдності забезпечують кібербезпеку України на даному етапі. Система функціонує наступним чином: Конституцією України забезпечення кібербезпеки України визначено однією із найважливіших функцій держави. Кримінальним кодексом України визначено негативні діяння, пов'язані із даним явищем, за які встановлено кримінальну відповідальність, та санкції для правопорушників. Численні Закони України регламентують суспільні відносини у даній сфері. Підзаконні нормативно-правові акти закріплюють механізми регламентації таких відносин та вектори подальшого розвитку усієї сфери. Тобто, правове регулювання боротьби із кіберзлочинністю є можливим лише за умови системного втілення приписів проаналізованих законодавчих актів;

2) всеохопливість – нормативно-правові акти, прийняті у дані сфері, охоплюють регламентацію питань кібербезпеки держави, кіберпростору, захист прав та інтересів громадян, протидія комп'ютерній злочинності та комп'ютерному тероризму тощо. Тобто, боротьба із кіберзлочинністю є процесом, який передбачає комплексне застосування заходів, а нормативно-правове регулювання забезпечує закріплення відповідних механізмів;

3) перспективність – деякі підзаконні нормативно-правові акти прийнято з метою встановлення векторів для подальшої еволюції зазначеної сфери. Тому, сучасний стан національного правового регулювання боротьби із кіберзлочинністю свідчить про те, що даний інституту все ще перебуває на початкових етапах свого розвитку;

4) деталізація - боротьба із кіберзлочинністю водночас розглядається у декількох аспектах: як протиправне діяння, передбачене нормами Кримінального кодексу України, що спричинило шкоду громадянам України; як напрям державної політики; як загроза національній безпеці; як один із способів консолідації громадян тощо.

Враховуючи, що на сьогодні все ще несформованим є єдине розуміння того, що ж являє собою кіберзлочинність, відмітимо що регламентація даного інституту все ж здійснюється на високому рівні. Проте, нагальною проблемою є відсутність узгодження між такими нормативно-правовими актами та відсутність єдиного понятійного апарату, що повинно бути усунено найближчими роками.

Наступною підкатегорією нормативно-правових актів є ті, що врегульовують діяльність органів, які здійснюють боротьбу із кіберзлочинністю. До їх переліку варто віднести Службу Безпеки України, Державну службу спеціального зв'язку та захисту інформації України, Національний Банк України інші органи, які залучені до цього питання. Проте, в першу чергу потребує виділення спеціально створений правоохоронний орган, який виконує особливі функції у даній сфері.

Вперше такий орган з'явився в Україні в 2011 році, яким датовано заснування Департаменту по боротьбі з кіберзлочинністю МВС України, а його територіальні підрозділи почали створюватись у 2012 році [111, с. 108]. Специфіка даного органу полягала у тому, що в його практичній діяльності від працівників потребувались знання як правових аспектів, так й інформаційних технологій, принципів роботи кібермереж та пристроїв, а також останніх розробок інформаційної сфери. До завдань Управління відносилось організаційне та практичне забезпечення реалізації державної політики щодо попередження та протидії злочинам і правопорушенням, що вчиняються з використанням інформаційних технологій та телекомунікаційних мереж, а також протидії легалізації доходів, отриманих від таких злочинів і правопорушень [111, с. 108]. Проте, профункціонував

даний орган недовго і на сьогодні вже не існує. Замість нього відповідно до Положення про Департамент кіберполіції Національної Поліції України, затвердженого наказом Національної поліції від 10.11.2015 № 85, було створено Департамент кіберполіції як міжрегіональний територіальний орган. Даний орган перебуває ще на початковому етапі свого розвитку, а його завданнями на сьогодні визначено: 1) участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням із використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку; 2) сприяння іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [117]. Зрозуміло, що такого переліку на сьогодні не достатньо, проте даний орган все ще перебуває на етапі становлення, тож зробимо припущення, що у майбутньому його буде розширено. Щодо правової основи діяльності даного органу, перш за все варто відзначити Закон України «Про національну поліцію» від 2 липня 2015 року № 580-VIII [118]. Не зважаючи на те, що даний нормативно-правовий акт взагалі не містить положень, присвячених боротьбі із кіберзлочинністю, він все ж має визначальне значення для Департаменту, оскільки закріплює правові засади організації та діяльності Національної поліції України. Відмітимо, що для подальшого розвитку досліджуваного органу важливим є передбачення окремих елементів регулювання боротьби із кіберзлочинністю, зокрема у розділі, присвяченому поліційним заходам.

Окрім Департаменту кіберполіції Національної Поліції України, важливим суб'єктом боротьби із кіберзлочинністю є Служба Безпеки України. СБУ передусім виконує функції із задоволення та захисту інформаційних потреб громадян, юридичних осіб та держави. Аналізуючи норми Закону України «Про Службу Безпеки України» від 25.03.1992 № 2229-XII [119], звернемо увагу на те, що поняття «кіберзлочинність» чи «комп'ютерна злочинність» там не вживаються взагалі. Проте, звертаючись до обов'язків даного органу, у статті 24 зазначеного Закону, можна зробити

висновок, що окремі її положення поширюються і на кіберсферу. Наприклад, здійснення відповідно до законодавства профілактики правопорушень у сфері державної безпеки чи забезпечення захисту державного суверенітету, конституційного ладу і територіальної цілісності України від протиправних посягань з боку окремих осіб та їх об'єднань тощо. Не зважаючи на те , що у відповідних положеннях мова не йде безпосередньо про кіберзлочини, зрозуміло, що одним із напрямків загроз державній безпеці є саме зазначені види злочинів.

Тож зробимо висновок, що завдання, які стоять перед Службою Безпеки України щодо боротьби із кіберзлочинністю є не менш важливими, аніж завдання Департаменту кіберполіції Національної Поліції України, проте значно всеохоплюючими і поширюють на питання захисту державного суверенітету, конституційного ладу, територіальної цілісності, економічного, науково-технічного та іншого потенціалу України, законних інтересів держави та прав громадян тощо. Тому, нормативно-правові акти, які врегульовують діяльність Служби Безпеки України також варто віднести до досліджуваної категорії.

Державна служба спеціального зв’язку та захисту інформації України здійснює діяльність по забезпеченні національної безпеки України від зовнішніх і внутрішніх загроз у сфері зв’язку. Аналіз норм Закону України «Про Державну службу спеціального зв'язку та захисту інформації України» [120] засвідчує, що даний орган не здійснює безпосередньо боротьбу із кіберзлочинністю, проте одним із його обов’язків є «забезпечення функціонування, безпеки та розвитку Національної системи конфіденційного зв’язку» [120]. Тобто, боротьба із кіберзлочинністю у даному випадку здійснюється шляхом попередження можливості злочинних діянь та забезпечення безпеки систем зв’язку. А отже, є підстави в рамках підкатегорії нормативно-правових актів, що врегульовують діяльність органів, які здійснюють боротьбу із кіберзлочинністю, розглядати

законодавство, яке врегульовує діяльність Державної служби спеціального зв'язку та захисту інформації України.

Роль Національного Банку України в забезпеченні національного правового регулювання боротьби з кіберзлочинністю полягає передусім у врегулюванні питань зберігання, захисту, використання та розкриття інформації, що становить банківську таємницю, а також протидіє фінансовому тероризму та злочинності із платіжними системами [121]. Тобто, є підстави стверджувати, що даний орган також займає важливе місце у системі органів боротьби із кіберзлочинністю.

Наступні проаналізовані нормативно-правові акти є підзаконними та стосуються утворення Департаменту кіберполіції та окремих аспектів регулювання діяльності Національної поліції загалом. Виділяємо передусім законодавство, що стосується діяльності даного правоохоронного органу, оскільки саме Департамент кіберполіції здійснює безпосередню боротьбу із кіберзлочинністю. Що стосується інших органів, їх роль є епізодичною і стосується лише окремих елементів даної боротьби. Тому, саме підзаконні нормативно-правові акти, які стосуються Департаменту кіберполіції, мають визначальне значення для механізму забезпечення національного правового регулювання боротьби з кіберзлочинністю.

Так, Постановою Кабінету Міністрів України від 13 жовтня 2015 року № 831 [122] закріплено статус Департаменту кіберполіції як міжрегіонального територіального органу Національної поліції, а Наказом Національної поліції України від 07.11.2015 № 10 затверджено чинний штат даного органу [123]. Тобто, такі нормативно-правові акти у цілому не мають суттєвого впливу на національне правове регулювання боротьби із кіберзлочинністю, проте легалізують Департамент кіберполіції та його працівників його як головного суб'єкта боротьби з кіберзлочинністю у нашій державі. Основоположне значення для його діяльності відіграє Наказ Національної поліції України від 10.11.2015 № 85 «Про затвердження Положення про Департамент кіберполіції Національної поліції України» [9].

Зокрема, Положенням встановлено завдання та функції даного органу, його права й організацію діяльності. Тому, у цілому можна зробити висновок, що не зважаючи на недосконаліть окремих норм та сумнівний перелік завдань, діяльність даного органу все ж є регламентованою належним чином, що свідчить про перспективність подальшого вдосконалення роботи Департаменту. Серед окремих прогалин, відзначимо не чітке окреслення регламентації діяльності Департаменту кіберполіції у ситуаціях, що потребують співпраці із іншими державами та не вирішення питання двосторонньої взаємодії поліції із провайдерами. Також незрозумілою є роль даного органу у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням із використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку. Тому, на підставі здійсненого аналізу виділимо наступні ознаки нормативно-правових актів, що врегульовують діяльність органів, які здійснюють боротьбу із кіберзлочинністю:

1) спрямованість на регламентацію діяльності Департаменту кіберполіції Національної поліції України, Служби Безпеки України, Державної служби спеціального зв'язку та захисту інформації України, Національного Банку України тощо;

2) вагомість ролі підзаконних нормативно-правових актів;

3) комплексне поєднання векторів попередження та протидії кіберзлочинності.

У цілому ж підсумовуючи дану групу джерел національного правового регулювання боротьби з кіберзлочинністю доцільно відзначити її загальну недосконаліть та неузгодженість. Головною проблемою є те, що нормативно-правові акти як інструменти правового регулювання так і не утворили єдину систему. Основні законодавчі та підзаконні акти були прийняті на різних етапах генезису інституту боротьби із кіберзлочинністю в Україні та згодом не були адаптованими то тих змін у розумінні даного явища, які мали місце у процесі його розвитку. Тому однакові явища можуть

мати різні назви або широке та вузьке розуміння водночас. У той же час є підстави стверджувати, що державою належним чином виконуються положення статті 17 Конституції України [6] щодо встановлення забезпечення інформаційної безпеки України як однієї із найважливіших функцій держави та справи усього Українського народу, оскільки дане питання є законодавчо врегульованим, компетентний орган створено, його діяльність регламентовано, а у суспільстві існує розуміння небезпеки від злочинів у кіберзлочинів.

Наступним елементом національного правового регулювання боротьби з кіберзлочинністю є міжнародні договори, укладені Україною з іншими державами світу у сфері боротьби із кіберзлочинністю. Зробимо припущення, що поштовхом до розвитку міждержавних відносин стали взяті Україною зобов'язання щодо інтеграції у міжнародну та світову спільноту, наприклад прийняті згідно до Програми інтеграції України в Європейський Союз [50], оскільки з того моменту нашою державою було укладено низку угод щодо співпраці у даній сфері.

Ознаками міжнародних договорів як елементу національного правового регулювання боротьби із кіберзлочинністю є:

1) їх укладення як правоохоронними органами, так і Кабінетом Міністрів України;

2) обмежене коло питань щодо яких здійснюється співпраця;

3) безпосереднє поширення лише деяких із них на сферу боротьби із кіберзлочинністю, хоча відсутність прямих вказівок не є виключенням такої можливості.

Тому, у цілому зробимо висновок про те, що міжнародні договори є важливим елементом національного правового регулювання боротьби із кіберзлочинністю. Дане негативне явище не має кордонів, а отже на практиці правоохоронні органи часто стикаються із ситуаціями, які перебувають поза межами юрисдикції нашої держави. Саме у таких випадках виникає потреба міжнародної співпраці, яка забезпечується шляхом укладення угод. Таким

чином, правове регулювання боротьби із кіберзлочинністю в нашій державі є неможливим без сприяння правоохоронних органів іноземних держав.

Міжнародний нормативно-правовий акт, тобто угода, укладена кількома суб’єктами міжнародного права та ратифікована в Україні є важливим з огляду на те, що без надання згоди уповноваженим органом законодавчої влади на обов'язковість такого документу, він не набуде юридичної сили в нашій державі та не вважатиметься частиною вітчизняного законодавства.

З початку XXI століття країнами світу було прийнято ряд міжнародних нормативно-правових актів, які становлять основу європейського та світового законодавства про кіберзлочинність. Деякі із них були ратифіковані нашою державою, а отже є частиною української правової системи: Конвенція про кіберзлочинність [1], ратифікована Україною 7 вересня 2005 року [8] та Додатковий протокол до неї, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи [43] й Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40], ратифікована 04.02.2004 [124]. Вартою уваги є також Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації [44], проте наміри України щодо виходу зі складу даної організації зменшують фактичну роль даного міжнародного документу у національному правовому регулюванні боротьби з кіберзлочинністю.

Зокрема, міжнародні нормативно-правові акти як складова національного правового регулювання боротьби з кіберзлочинністю, характеризуються наступними ознаками:

1) належність до системи національного права за умови ратифікації у встановленому Законом порядку;

2) виконання міжнародними нормативно-правовими актами ролі умовних векторів розвитку вітчизняного законодавства;

3) використання для регулювання суспільних відносин нарівні із нормами вітчизняного законодавства;

4) сприяння міжнародному співробітництву у сфері боротьби з кіберзлочинністю.

Підсумовуючи аналіз зазначеної групи варто відзначити вагому роль проаналізованих нормативно-правових актів у національних правових системах низки європейських, і не лише, держав. Ратифікація подібних міжнародних документів суттєвим чином наближає Україну до інтеграції у світові геополітичні процеси. На сьогодні неможливим є розвиток держави без імплементації всесвітньо визнаних правових стандартів. Тому, обраний нашою державою курс значним чином посилює роль досліджуваного інструменту в процесі національного правового регулювання боротьби із кіберзлочинністю.

Разом з тим, нормативність права має бути переведеною у площину упорядкування суспільних відносин з метою задоволення інтересів їх учасників. Тому, наступним важливим питанням для встановлення є механізм правового регулювання боротьби із кіберзлочинністю. С. Д. Сорокін розглядає механізм правового регулювання як юридичну процедуру, за допомогою якої правове регулювання породжує юридичні наслідки [125, с. 34]. Не в повній мірі погодимось із формулюванням «юридична процедура», проте відзначимо вдале висвітлення сутності даного явища. Більш доцільним вбачаємо розуміння механізму правового регулювання як певної системи правових засобів. Тобто, механізмом національного правового регулювання боротьби із кіберзлочинністю є сукупність правових засобів, за допомогою яких правові норми, що забезпечують протидію даному негативному явищу переходять у площину безпосередньої реалізації.

На підставі зроблених висновків, стадіями механізму правового регулювання боротьби із кіберзлочинністю є:

1. Правова регламентація відносин боротьби із кіберзлочинністю – визначення у правових формах змісту і меж поведінки суб'єктів правовідносин у кіберпросторі, їх прав, обов'язків, відповідальності. На даній стадії відбувається формування нормативно-правової бази механізму правового регулювання боротьби із кіберзлочинністю. Відштовхуючись від сутності встановлених інструментів національного правового регулювання боротьби із кіберзлочинністю, перша стадія реалізовується двома шляхами – шляхом законодавчої діяльності органів державної влади, або ж шляхом ратифікації міжнародних нормативних актів.

2. Виникнення у суб'єктів правовідносин боротьби із кіберзлочинністю прав та обов'язків – необхідний юридичний факт вчинення кіберзлочину, внаслідок чого суб'єкти боротьби із кіберзлочинністю наділяються обов'язком відновлення порушених правовідносин, та правами, регламентованими законними, а також підзаконними нормативно-правовими актами. Так, правами Департаменту кіберполіції [126, с. 66] є: 1) здійснювати оперативно-розшукову діяльність, спрямовану на виявлення та припинення злочинів у сфері протидії кіберзлочинності, а також комплексне використання джерел оперативної інформації, можливостей оперативних підрозділів та застосування оперативно-технічних засобів під час провадження в оперативно-розшукових справах, контроль за використанням коштів, призначених для проведення цієї роботи; 2) здійснювати оперативно-технічні заходи за оперативно-розшуковими справами, що знаходяться в їх провадженні; 3) в установленому порядку запитувати та отримувати від посадових осіб органів внутрішніх справ і органів державної влади документи, довідкові та інші матеріали (у письмовій або усній формі), необхідні для прийняття рішень з питань забезпечення реалізації державної політики у сфері протидії кіберзлочинності; 4) користуватися в установленому законодавством порядку базами даних Національної поліції України, МВС та інших державних органів з питань, що належать до компетенції Департаменту, а також інші права, передбачені законодавством

[9]. Тобто, правами та обов'язками суб'єктів правовідносин боротьби із кіберзлочинністю є нормативно закріплений обсяг правомочностей, яких вони зобов'язані дотримуватись у процесі здійснення службової діяльності. При цьому, сама сутність регламентованих прав свідчить про те, що вони безпосередньо пов'язані із вчиненням кожного конкретного кіберзлочину, тобто використовуються внаслідок факту вчинення проступку, передбаченого нормами чинного кримінального законодавства.

3. Реалізація прав і обов'язків суб'єкта боротьби із кіберзлочинністю – здійснюється шляхом припинення протиправної поведінки, відновлення порушених прав та притягнення винних осіб до відповідальності. Припинення протиправних дій може бути добровільним, або ж примусовим, проте головним його наслідком є поява можливості відновлення становища, яке існувало раніше. Надалі судом здійснюється ліквідація наслідків такої поведінки, та встановлення санкцій для правопорушника. Також на даному етапі можливою є реалізація міжнародної правосуб'єктності України, передбачена нормами міжнародного законодавства, виражена у формах екстрадиції чи обміном інформації із правоохоронними органами інших держав.

Отже, дослідивши нормативно-правову базу національного правового регулювання боротьби з кіберзлочинністю та механізму її забезпечення, нами встановлено наступні особливості сучасного стану даного інституту:

1. Наявність системи національного правового регулювання боротьби з кіберзлочинністю, проте недостатній рівень єдності її елементів, що полягає у відмінностях в термінології, наявності розбіжностей у формулюваннях, прогалин та інших проблем;

2. Комбінування у правовій системі норм вітчизняного законодавства та міжнародних правових актів, ратифікованих нашою державою;

3. Наявність міжнародних договорів щодо двосторонньої співпраці у сфері правового регулювання боротьби з кіберзлочинністю.

4. Існування Стратегії кібербезпеки України, що визначає подальший розвиток національного правового регулювання боротьби із кіберзлочинністю.

Підсумовуючи вищедосліджене, національне правове регулювання боротьби з кіберзлочинністю становлять нормативно-правові акти, прийняті порівняно нещодавно. Проте, більшість із них вже потребують оновлення та приведення у відповідність до сучасних умов та міжнародних правових стандартів. Обраний курс до тісного співробітництва з провідними європейськими державами та участі у різноманітних міжнародних організаціях вимагає наближення рівня та змісту вітчизняного законодавства до європейських аналогів. Сьогоднішня нормативно-правова база боротьби із кіберзлочинністю місцями не відповідає динаміці розвитку сучасних суспільних відносин, а тому важливим та актуальним питанням підвищення рівня узгодженості норм чинного законодавства. В той же час, національне правове регулювання боротьби з кіберзлочинністю характеризується високим рівнем деталізації та охопленням значного об'єму суспільних відносин. Вирішення даної проблеми вважається одним із пріоритетних напрямків державної політики, тож еволюція законодавчих інструментів відбувається постійно. Прийняття Стратегії кібербезпеки України свідчить про те, майбутнє інституту правового регулювання боротьби з кіберзлочинністю пов'язується із поліпшенням умов для безпечного функціонування кіберпростору.

Висновки до Розділу 2

1. Механізм правового регулювання боротьби з кіберзлочинністю – це чітко визначена й організована система юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану

поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

2. Особливостями універсального міжнародно-правового регулювання боротьби з кіберзлочинністю є наступні: 1) відповідна діяльність акумулюється навколо ООН та її органів або створених за її підтримки суб'єктів; 2) на сьогодні наявні виключно програмні та інші стратегічні документи, які повинні закласти основи міжнародно-правового регулювання відповідного кола відносин; 3) основними напрямами діяльності має бути створення й розробка організаційних та законодавчих заходів протидії кіберзлочинності, а також питання взаємодія у даній сфері діяльності; 4) наявна необхідність у створенні міжнародних спільних органів оперативно-розшукової діяльності для забезпечення фіксування слідів вчинених злочинів; 5) удосконалення взаємодії між компетентними органами різних держав; 6) існує нагальна потреба розробки й прийняття універсальних конвенцій з відповідних питань, які би забезпечили участь більшості держав у відповідних заходах проти кіберзлочинності.

3. Особливостями регіонального міжнародно-правового регулювання протидії кіберзлочинності є такі: 1) значна увага з боку різноманітних регіональних міжнародних організацій до питань протидії кіберзлочинам; 2) розробка численних регіональних угод про співробітництво у сфері протидії інформаційним злочинам; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. - на початку 2000-х рр.; 4) така діяльність є складовою частиною як міжнародних інформаційних відносин, так і кримінального судочинства.

4. Міжнародні нормативно-правові акти як складова національного правового регулювання боротьби з кіберзлочинністю, характеризуються наступними ознаками:

1) належність до системи національного права за умови ратифікації у встановленому Законом порядку;

2) виконання міжнародними нормативно-правовими актами ролі умовних векторів розвитку вітчизняного законодавства;

3) використання для регулювання суспільних відносин нарівні із нормами вітчизняного законодавства;

4) сприяння міжнародному співробітництву у сфері боротьби з кіберзлочинністю.

5. Особливостями нормативно-правової бази національного правового регулювання боротьби з кіберзлочинністю є наступні:

1. Наявність системи національного правового регулювання боротьби з кіберзлочинністю, проте недостатній рівень єдності її елементів, що полягає у відмінностях в термінології, наявності розбіжностей у формулюваннях, прогалин та інших проблем;

2. Комбінування у правовій системі норм вітчизняного законодавства та міжнародних правових актів, ратифікованих нашою державою;

3. Наявність міжнародних договорів щодо двосторонньої співпраці у сфері правового регулювання боротьби з кіберзлочинністю.

4. Існування Стратегії кібербезпеки України, що визначає подальший розвиток національного правового регулювання боротьби із кіберзлочинністю.

РОЗДІЛ 3.
ОПТИМІЗАЦІЯ ПРАВОВОГО РЕГУЛЮВАННЯ БОРОТЬБИ З КІБЕРЗЛОЧИННІСТЮ

3.1 Перспективи та тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні

По мірі збільшення кількості кіберзагроз в нашій державі, все актуальнішим стає питання правового регулювання даної сфери. В світлі євроінтеграційних процесів важливою для України є демонстрація того, що ми готові протистояти загрозам найстрімкіше зростаючому виду злочинності та, що вітчизняне законодавство належним чином регламентує відповідні правовідносини у кіберпросторі. Окрім того, в сучасних умовах важливою є демонстрація готовності приймати необхідні зміни, що відповідатимуть стандартам, встановленим на європейському та світовому рівнях. Тож, за умов, коли сфера віртуального простору та злочинів в ньому продовжує розвиватись, питання перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні є одним з основних в силу своєї важливості та рівня урегульованості.

Постійний розвиток правового регулювання боротьби з кіберзлочинністю в Україні є важливим з огляду на наступні фактори. По-перше, на сьогодні практично усі державні та недержавні процеси відбуваються із застосуванням інструментів кіберспростору. По-друге, в умовах неоголошеної війни, у якій вимушена приймати участь Україна, віртуальний простір є одним із фронтів, у якому наша держава в силу відставання в сфері інформаційних технологій все ще не демонструє внутрішньо та зовнішньополітичні успіхи. По-третє, рівень усвідомлення загрози кіберзлочинів та їх небезпечності у суспільстві все ще є невисоким. За таких умов проблема перспектив та тенденцій розвитку правового

регулювання боротьби з кіберзлочинністю в Україні є однією із першочергових для дослідження.

У контексті збільшення актуальності питань, пов'язаних з боротьбою із кіберзлочинністю, в Україні важливими були останні декілька років, коли ми почали спостерігати тенденцію підвищення ролі та значення кібербезпеки в суспільному житті. Тож, ключовими факторами розвитку правового регулювання боротьби з кіберзлочинністю в Україні є збільшення активності громадян в Інтернет просторі, активізація діяльності кіберзлочинців та необхідність імплементації міжнародних правових норм у вітчизняному законодавстві для боротьби із даним негативним явищем. В той же час, звертаючись до наукової доктрини, варто відзначити недостатню увагу до даного питання з боку саме вчених-правовиків. Переважна більшість робіт у даній тематиці охоплюють тенденції поширення кіберзлочинів, або ж є не в повній мірі актуальними на сьогодні. Це є проблемою, оскільки досліджуване питання у цілому постійно перебуває в сфері наукових інтересів вітчизняних дослідників, проте ніколи не втрачає доцільності дослідження.

Розуміння терміну «перспективи» зводиться до бачення майбутніх подій, а сутність понятт «тенденція» полягає у позначенні певних мінливих та недовготривалих явищ, а отже тенденції та перспективи на кожному хронологічному етапі мають здатність змінюватись. Саме тому необхідним є встановлення тих співвідношень та властивостей, які є характерними на сьогодні та будуть актуальними найближчим часом. Відзначимо, що дослідженням питання перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні займались вчені різноманітних сфер вітчизняної науки, зокрема правової та економічної. Серед них виділимо таких як: Ю. М. Батурин, В. Л. Бурячок, В. Б. Вєхов, В. О. Голубєв, Н. Ф. Казакова, О. Ф. Мельников, Ю. М. Онищенко, О. В. Орлов, Б. В. Романюк, Ю. Є. Якубівська та багато інших. Водночас, правовий аспект в проаналізованих роботах є не завжди присутнім. Тож, постійний розвиток інформаційних технологій та нормативно-правової бази їх реалізації, а також

важливість дослідження тих тенденцій, які є доцільними саме на даному етапі розвитку нашої держави, зумовлюють важливість дослідження виділеної проблеми.

Аналіз робіт вітчизняних вчених продемонстрував, що чіткий та актуальний перелік як перспектив розвитку правового регулювання боротьби з кіберзлочинністю в Україні, так і тенденцій наразі відсутній. Дана сфера занадто стрімко розвивається, тому виділення певних доцільних на даному етапі концепцій є неможливим. Проте, до окремих аспектів вітчизняні науковці все ж звертаються, тому видається можливим проаналізувати найвдаліші з них та сформулювати єдину систему перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні станом на сьогодні.

Наприклад, О. О. Йона та М. Ф. Казакова, аналізуючи світові тенденції боротьби з кіберзлочинністю, відмічають позитивний характер таких тенденцій в Україні. Зокрема, вченими відмічено як один зі стратегічних напрямків налагодження в Україні системи співробітництва з іншими державами, що обумовлено необхідністю обміну досвідом на міжнародному рівні [127, с. 60]. Із такою позицією та виділеною тенденцією варто погодитись, з огляду на те, що Україна прагне стати частиною європейських та світових процесів. За таких умов співпраця із більш досвідченими в даному питанні країнами є вкрай необхідною. Оскільки на світовому рівні боротьба із кіберзлочинністю розпочалась майже на десятиліття раніше, ніж в Україні, перейняття досвіду розвинутіших країн очевидно ще довгий час передуватиме в переліку основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в нашій державі. Також відмітимо, що процес консолідації європейської спільноти для боротьби із кіберзлочинністю розпочався на початку поточного століття і на сьогодні вже прийнято значний масив міжнародних нормативно-правових актів. До виконання частини з них Україна вже приєдналась шляхом ратифікації, проте

ряд угод, протоколів та рекомендацій все ще не є джерелами вітчизняного законодавства.

Щодо питання співробітництва також доцільно відзначити, що О. О. Йона та Н. Ф. Казакова вбачають необхідність координації питань співробітництва кожною країною відповідно до розробленої та чинної у ній стратегії кібербезпеки [127, с. 60]. Тобто, визначення тенденцій є не просто питанням, яке перебуває виключно у сфері наукових інтересів дослідників у певній країні [128, с. 38]. Нагальні тенденції повинні бути закріпленими на законодавчому рівні. Аналізована стаття О. О. Йона та Н. Ф. Казакова датована 2013 роком, коли в Україні така стратегія ще перебувала на стадії розробки, проте, у 2016 році її було затверджено Указом Президента України «Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України»» [116]. У контексті досліджуваної теми, необхідним є аналіз її норм з метою встановлення тих напрямів розвитку інституту правового регулювання боротьби з кіберзлочинністю в Україні, які виділив законодавець.

Так, частина 4 Стратегії дістала назву «Пріоритети та напрями забезпечення кібербезпеки України». Аналіз її норм засвідчив, що важливим моментом є встановлення того, чи є можливим ототожнення понять «пріоритети та напрями» й «тенденції та перспективи». Великий тлумачний словник української мови роз'яснює тенденції, як «напрям розвитку чого-небудь» [11, с. 1440]. Тобто, згідно тематики нашого дослідження його цілком можливо роз'яснити як напрям розвитку та забезпечення правового регулювання боротьби з кіберзлочинністю в Україні. У свою чергу, пріоритет тлумачиться як провідне значення чого-небудь [130, с. 168]. Іншими словами, стосовно перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні - це певні першочергові положення, які стосуються забезпечення кібербезпеки України. У цілому, в нас є підстави стверджувати про пріоритетність тенденцій, оскільки з-поміж усього масиву можливих векторів, варто опиратись на ті, що є першочерговими в сучасних

умовах. А тому, пріоритети та напрями забезпечення кібербезпеки України цілком можливо тлумачити як законодавчо закріплені напрямки боротьби з кіберзлочинністю в Україні. Проте, не кожен з них безпосередньо відноситься до сфери правового регулювання. Так, Радою національної безпеки і оборони України виділено наступні пріоритетні напрямки: 1) розвиток безпечного, стабільного і надійного кіберпростору, що полягає у тому числі в розробці державної політики у сфері кібербезпеки, та досягненні відповідності зі стандартами ЄС та НАТО; створенні вітчизняної нормативно-правової та термінологічної бази у цій сфері, гармонізації нормативних документів зі стандартами ЄС та НАТО; розвитку міжнародного співробітництва у сфері забезпечення кібербезпеки, поглибленні співпраці України з ЄС та НАТО; 2) напрямки кіберзахисту державних електронних інформаційних ресурсів та інформаційної інфраструктури; критичної інфраструктури розвитку потенціалу сектору безпеки і оборони у сфері забезпечення кібербезпеки та боротьби з кіберзлочинністю мають організаційний, процесуальний та технологічний характер, тож аналіз передбачених заходів засвідчив недоцільність їх віднесення до сфери правового регулювання боротьби з кіберзлочинністю [116]. Аналіз норм даної стратегії дає підстави зазначити наступне - напрям розвитку безпечного, стабільного і надійного кіберпростору не в повній мірі є тенденцією розвитку правового регулювання боротьби з кіберзлочинністю в Україні, проте аналіз заходів, які ним передбачено, засвідчив його вагому роль. Як нами вже неодноразово відмічалось, в сучасних умовах необхідність створення вітчизняної нормативно-правової є важливим і нагальним питанням, яке поступово реалізовується протягом майже двох останніх десятиліть. Водночас, кіберзлочинність також не стоїть на місці, тому з кожним роком Україна стикається із все більшими й серйознішими проблемами. Щодо питання міжнародного співробітництва, в даному напрямі обидві тенденції вживаються комплексно. Погодимось, що за своєю сутністю вони є близькими, проте не варто здійснювати їх поєднання, оскільки для

розвитку вітчизняного законодавства використання зарубіжного досвіду не є першочерговим, так як важливим є слідування власній стратегії, що ураховує ті питання, які є нагальними для сьогодення. Можливість ознайомлення із досвідом країн, які працюють в зазначеному напрямку не перший рік дозволить зробити такі механізми більш придатними та актуальними, проте повне копіювання в силу специфіки кожної з окремих держав є неможливим. Також доцільно відзначити, що закріплений Радою національної безпеки і оборони України напрям з-поміж іншого включає і гармонізацію нормативних документів зі стандартами ЄС та НАТО, що доцільніше віднести до тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у цій сфері, оскільки міжнародні нормативно-правові акти, ратифіковані Верховною Радою України, є важливим джерелом вітчизняного права.

Останніми роками звичними є дискусії щодо доповнення Кримінального кодексу України статтями про злочини в комп'ютерній сфері, а також щодо значного посилення покарань [130; 131; 132; 133; 134; 135]. В даному контексті варто зазначити, що за останні роки до Розділу XVI даного нормативно-правого акту вже вносились зміни декілька разів, в тому числі й щодо зміни санкцій статей Кримінального кодексу України, виключення та доповнення Розділу новими статями [136; 137]. Проте, враховуючи безперервний розвиток інформаційних технологій та форм вчинення кіберзлочинів, варто розуміти, що можливим є настання моменту, коли чинні санкції не відповідатимуть негативним наслідкам шкідливих діянь кіберзлочинців. Саме тому логічним вбачаємо виділення такої тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні, як доповнення Кримінального кодексу України статтями про кіберзлочини та посилення покарання за їх вчинення.

В. В. Марков, аналізуючи питання зарубіжного досвіду протидії кіберзлочинності, зазначає, що до основних проблем виявлення, розкриття та розслідування «транскордонних» злочинів з використанням глобальної

мережі Інтернет варто віднести територіальну розподільність слідів злочину та зберігання їх протягом невеликого проміжку часу [138, с. 108]. Іншими словами, при визначенні місця вчинення здійснення кіберзлочинів можливе виникнення проблем, оскільки злочинці у всесвітній мережі можуть виступати анонімно, а будь-які докази чи сліди протиправної діяльності безслідно видаляються. Тому, для розслідування таких злочинів необхідною є взаємодія оперативних підрозділів на усіх рівнях, в тому числі і на міждержавному рівні із представниками правоохоронних органів інших країн. Тобто, з огляду на зазначені проблеми, можна спостерігати перспективу до ліквідації кордонів між державами у питаннях боротьби з кіберзлочинністю.

Вперше це проявилась на початку XXI століття, коли було прийнято ряд міжнародних нормативно-правових актів, які і на сьогодні становлять основу європейського та світового законодавства про кіберзлочинність: Конвенцію Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року; Віденську декларацію про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року; Конвенцію про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу [42]; Конвенцію про кіберзлочинність, ратифіковану Україною 7 вересня 2005 року; Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи; Угоду про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації; різноманітні рекомендації Ради Європи. Це стало першим кроком в об’єднанні зусиль міжнародної спільноти у питанні боротьби із кіберзлочинності та розвитку правового регулювання боротьби із неї. Наступний крок полягав у прийнятті міждержавних угод щодо співробітництва і багатосторонньому сприянні протидії кіберзлочинності. Тобто тенденція по встановленню співпраці на міжнародному рівні

розвивалась поступово і на сьогодні вже потребує переходу на якісно новий рівень. Як нами встановлено в даній роботі, серйозні зміни у законодавчому регулюванні переважно пов’язуються із виникненням нових форм кіберзлочинності.

Наприклад, прийняття Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності від 15.11.2000 року [40] можна пов’язати із виходом кіберзлочинності на новий транснаціональний рівень в середині 90-х років XX століття. Сама Конвенція не є негайною реакцією міжнародної спільноти на виникнення даної загрози, а швидше адекватною та належним чином розробленою протидією транснаціональним кіберзлочинам. Віденська декларацію про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року [41] вже відштовхуючись від самої назви є нормативно-правовим актом, спрямованим на об’єднання держав світу у боротьбі із злочинами, не характерними для попередніх історичних епох. У самому тексті документу йдеться про «вчинення серйозних злочинів, які мають глобальний характер», їх «транснаціональність» та на необхідність боротьби із ними. Враховуючи, що Декларація була прийнята в той же період, що й Конвенція ООН, це є ще одним свідченням серйозного росту масштабів злочинності, у тому числі й у кіберпросторі, в той період. Тобто, на підставі цих прикладів зробимо висновок, що увага міжнародної спільноти до проблеми виникнення нових форм злочинів спричинила суттєві зміні у міжнародному правовому регулюванні боротьби із кіберзлочинністю.

Тож, побудову системи перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні варто здійснюватись із обов’язковим урахуванням наступних положень: 1) в нашій державі розпочато процес інтеграції міжнародних нормативно-правових актів у сфері боротьби із кіберзлочинністю у вітчизняне законодавство; 2) Україна співпрацює, проте все ще не досить активно, із зарубіжними державами у питаннях, пов’язаних із розслідуванням кіберзлочинів. Тому, подальший

розвиток даного інституту варто пов’язати із вдосконаленням законодавчої бази та підвищенням взаємодії відповідних підрозділів органів внутрішніх справ на міжнародному рівні – із правоохоронними органами інших держав, що полягатиме у наданні всесторонньої допомоги в питаннях подолання кіберзлочинності.

Також звернемо увагу на одну із негативних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні, виділену О. Вінером у статті, присвяченій тенденціям розвитку кібербезпеки - збільшення рівня контролю за користувачами мережі Інтернет [139]. Цілком вірогідно, що рано чи пізно питання кібербезпеки та прав і свобод людини і громадянина перетнуться і законодавцю доведеться робити вибір: посилити захист приватного життя громадян в мережі Інтернет чи посилити доступ спецслужб до особистих даних користувачів з метою забезпечення безпеки у державі. Тому, цілком вірогідним є посилення заходів щодо підвищення ефективності спецслужб шляхом нормативного та фактичного зменшення обсягу прав і свобод, якими наділяються громадяни України.

Таким чином, аналіз наукової доктрини нашої держави дозволив виділити три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні:

1) тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні;

2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні;

3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

Окрім проаналізованих позицій, вважаємо за необхідне доповнити перелік основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні підтенденціями, які деталізовуватимуть їх зміст.

Так, у рамках тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні

запропоновано виділити наступні підтенденції: 1) розширення меж розуміння поняття кіберзлочинність; 2) посилення кримінальної відповідальності за вчинення кіберзлочинів; 3) термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання, єдиного термінологічного апарату.

Щодо тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні основними підтенденціями є: 1) ратифікація тих міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю, які на сьогодні ще не є джерелом вітчизняного права; 2) укладення міжнародних двосторонніх чи багатосторонніх угод з іншими державами; 3) правова допомога іншим державам у питаннях боротьби із кіберзлочинністю; 4) втілення міжнародних стандартів у нормах вітчизняного законодавства.

В тенденції збільшення рівня контролю за користувачами мережі Інтернет виділимо наступні підтенденції: 1) встановлення правил користування громадянами кіберпростором; 2) створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором.

Для розуміння того, які заходи необхідні для розвитку правового регулювання боротьби з кіберзлочинністю в Україні, варто належним чином розкрити кожну із виділених тенденцій.

Тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні полягає у прямій залежності наших успіхів та розвитку від тієї законодавчої бази, що врегульовує питання кіберзлочинності. Будь-які суспільні відносини, як у реальному, так і у віртуальному світі мають бути належним чином регламентовані та захищені нормами законодавства.

Як нами встановлено в даній роботі, на сьогодні наша держава перебуває на третьому етапі генезису правового регулювання боротьби з кіберзлочинністю, проте усі існуючі проблеми все ще не вирішено. Чинні

загрози мають різноманітне походження – кримінальне, політичне, терористичне, пропагандистське і їх перелік з кожним роком розширюється. А отже, контроль та запобігання негативних явищ вимагає від держави інтенсивніших дій щодо вдосконалення нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю. Зокрема, було доцільним здійснення централізованої діяльності у наступних напрямках: 1) розширення меж розуміння поняття кіберзлочинність; 2) посилення відповідальності за вчинення кіберзлочинів; 3) встановлення єдиного термінологічного апарату у вітчизняному законодавстві тощо.

Перш за все відзначимо, що деякі важливі кроки для розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні вже зроблено, зокрема прийнято вже згадувану Стратегію кібербезпеки України [116]. Проте, не зважаючи на усе, наша держава залишається вразливою до кібервпливу. Причину цьому варто шукати у тому, що вітчизняні закони, які врегульовують питання кіберпростору та злочинних посягань у ньому, є недостатньо розробленими. У Кримінальному кодексі України передбачено Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку» [3]. Проте, станом на сьогодні він містить лише шість статей: стаття 361 - несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку; стаття 361-1 - створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут; стаття 361-2 - несанкціоновані збут або розповсюдження інформації з обмеженим доступом, яка зберігається в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або на носіях такої інформації; стаття 362 - несанкціоновані дії з інформацією, яка оброблюється в електронно-обчислювальних машинах (комп'ютерах), автоматизованих системах, комп'ютерних мережах або

зберігається на носіях такої інформації, вчинені особою, яка має право доступу до неї; стаття 363 - порушення правил експлуатації електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється; стаття 363-1 - перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку або порядку чи правил захисту інформації, яка в них оброблюється [3]. Очевидно, що розвиток комп'ютерних технологій дозволяє зловмисникам здійснювати кіберзлочини фактично безкарно, оскільки кримінальне законодавство у такому вигляді є неадаптованим до нових форм злочинів у сфері інформаційних технологій. Наведемо актуальний приклад – в умовах гібридної війни Україна щодня отримує атаки на інформаційний простір. Поширення неправдивої інформації, створення ситуацій, що викликають паніку, провокування ненависті тощо. Це далеко неповний перелік заходів, що є елементами негативного інформаційного впливу на кіберпростір України. Сьогодні інформація є одним із видів зброї, що застосовується проти громадян України. Проте, Кримінальний кодекс України ніяким чином не регламентує дану протиправну діяльність у інформаційному просторі.

Для вирішення даної проблеми в першу чергу варто розширити зміст Розділу XVI. Безліч сучасних кіберзлочинів на сьогодні залишаються поза правовим врегулюванням, наприклад поширення неправдивої інформації, створення ситуацій, що викликають паніку за допомогою комп'ютерних мереж, провокування ненависті за допомогою комп'ютерних мереж, використання спеціальних шкідливих комп'ютерних програм тощо. Їх регламентація у нормах Кримінального кодексу України [3] дозволить по-перше, осучаснити розуміння поняття «кіберзлочинність», оскільки з розвитком сучасних технологій, кіберзлочинці постійно знаходять нові шляхи для здійснення протиправної діяльності. По-друге, дасть змогу

врегулювати вже наявні на сьогодні загрози та продемонструє готовність держави адекватно реагувати на небезпеки. По-третє, при розширенні змісту Розділу XVI необхідним є звернення до збільшення санкцій за вчинення відповідних злочинів. Аналіз статей 361-363[1] Кримінального кодексу України засвідчив, що санкції передбачені ними є в цілому схожими: мінімальне покарання за вчинення злочинів у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку встановлено на рівні від п’ятисот до тисячі неоподатковуваних мінімумів доходів громадян, а максимальне – позбавлення волі на строк від двох до п’яти років. Розвиток даного виду злочинності свідчить про те, що таких санкцій на сьогодні не достатньо. В сучасних умовах кіберзлочинність несе загрозу не просто окремим суб’єктам, а державі в цілому.

Наступною проблемою є відсутність єдиного понятійного апарату, що має вияв у вільному трактуванні ключових понять – кіберзлочинів, кібербезпеки, кіберпростору тощо у нормах вітчизняного законодавства. Наприклад, у Кримінальному кодексі України законодавець оперує такими поняттями, як «злочини у сфері використання електронно-обчислювальних машин», «комп’ютерні системи», «комп’ютерні мережі», «мережі електрозв’язку» тощо [3]. Водночас, Законом України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV подібна до кіберзлочинності термінологія не вживається взагалі. Кіберзлочини роз’яснюються як складова частина технологічного тероризму, оскільки ними є у тому числі злочини, які «вчиняються з терористичною метою із застосуванням комп'ютерних систем та комунікаційних мереж» [140]. Тобто, в даному випадку законодавцем взагалі проігноровано вживання загальноприйнятої на міжнародному рівні та у вітчизняній науці термінології. В Законі України «Про основи національної безпеки України» від 19.06.2003 № 964-IV [47] містяться терміни «комп’ютерна злочинність» та «комп’ютерний тероризм». Тобто, у трьох проаналізованих нами нормативно-правових актах одні й ті самі явища

позначені трьома різноманітними варіантами термінології. А отже, на підставі цього варто зробити наступні висновки:

1) в нормах вітчизняного законодавства відсутній єдиний термінологічний апарат - для подолання даної теоретичної прогалини варто внести зміни до усіх нормативно-правових актів, які здійснюють правове регулювання боротьби з кіберзлочинністю в Україні. Найбільш доцільним вбачається саме використання термінології із частиною «кібер-», яка на сьогодні ще не отримала сформованого визначення на нормативно-правовому рівні. Проте, в міжнародних нормативно-правових актах даний вид злочинності позначається саме так – свідченням тому є прийняття Конвенції про кіберзлочинність від 23.11.2001 року [1];

2) законодавець оперує визначеннями, дефініції яким не надано взагалі, а чинні терміни є численними та не узгодженими між собою – це стосується тих визначень, які закріплено в законодавстві станом на сьогодні: «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку», «комп'ютерна злочинність», «комп'ютерний тероризм» тощо. Проте, більш доцільним є прийняття єдиного термінологічного апарату із його подальшим роз'ясненням в правових нормах. На науковому рівні розуміння цієї проблеми сформувалось вже давно, тож розробка необхідної термінології постійно перебуває у сфері наукових інтересів вітчизняних дослідників.

Відповідно, зроблений аналіз дає підстави здійснити узагальнення наявних на сьогодні проблем вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні: 1) вузький спектр злочинних діянь, за які передбачено покарання у нормах Кримінального кодексу України; 2) проблеми понятійного апарату, пов'язані із вільним використанням великої кількості термінів, не узгоджених між собою; 3) чинне законодавство про боротьбу з кіберзлочинністю в Україні не в повній мірі відповідає вимогам часу.

А отже, в рамках даної тенденції вбачаємо доцільним у майбутньому проведення наступних дій:

1) Формування єдиної системи нормативного забезпечення протидії кіберзлочинності на загальнодержавному рівні. Це можна здійснити шляхом прийняття нормативно-правових актів, які стосуватимуться виключно кібербезпеки нашої держави. Наприклад, таку систему може сформувати Закон України «Про боротьбу із кіберзлочинністю», який закріпить та узагальнить усі ключові поняття досліджуваного інституту, та низка підзаконних нормативно-правових актів, які передбачатимуть механізми реалізації його норм;

2) Розширення Розділу XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» Кримінального кодексу України статтями «Поширення неправдивої інформації», «Провокування ненависті і нетерпимості за допомогою комп'ютерних мереж» тощо. Пропонуємо сформулювати дані статті наступним чином, і при цьому зазначимо, що при встановленні міри покарань ми орієнтувались на орієнтовні значення санкцій статей Розділу XVI Кримінального кодексу України [3]:

- «Поширення неправдивої інформації. 1. Поширення у мережі Інтернет неправдивої інформації, що спричиняє паніку серед населення, - карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до шести років»;

- «Провокування ненависті і нетерпимості за допомогою комп'ютерних мереж. 1. Поширення у мережі Інтернет інформації, що провокує ненависть і нетерпимість серед населення, - карається штрафом від шестисот до тисячі неоподатковуваних мінімумів доходів громадян або виправними роботами на строк до двох років. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до шести років»;

3) Створення необхідного понятійного апарату, термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання – у нормах Кримінального кодексу України, Закону України «Про основи національної безпеки України» від 19.06.2003 № 964-IV, Закону України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV тощо, а також новоприйнятих нормативно-правових актах закріпити єдиний термінологічний апарат – «кіберпростір», «кібермережі», «кібербезпека», «кіберзлочинність», «кібертероризм», «кіберзлочинець», «кібертерорист» тощо:

- Кримінальний кодекс України [3]: Розділ XVI «Злочини у сфері використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку» запропоновано перейменувати на «Злочини у сфері кібербезпеки», в статтях даного розділу терміни «злочини у сфері використання електронно-обчислювальних машин», «комп'ютерні системи», «комп'ютерні мережі», «мережі електрозв'язку» замінити на «злочини у кіберпросторі», «кіберпростір», «кібермережі» тощо;

- Закон України «Про боротьбу з тероризмом» від 20.03.2003 № 638-IV [140]: у статті 1 встановити поняття кібертероризму як «суспільно небезпечної діяльності, яка полягає у вчиненні злочинів з терористичною метою із застосуванням кібермереж»;

- Закон України «Про основи національної безпеки України» від 19.06.2003 № 964-IV [47]: у статті 7 терміни «комп'ютерна злочинність» та «комп'ютерний тероризм» замінити на «кіберзлочинність» та «кібертероризм».

Наступною тенденцією, виділеною нами, є посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні. Потреба міжнародного співробітництва стосовно нашої держави має трьохаспектний характер. По-перше, в умовах формування інституту правового регулювання боротьби з кіберзлочинністю в Україні важливим є звернення до досвіду тих держав, які його успішно втілили у вітчизняних правових системах, із

урахуванням сильних сторін та проблем, які супроводжували даний процес. По-друге, потреба у міжнародному співробітництві з'явилась передусім внаслідок масової появи транснаціональних комп'ютерних злочинів, складність яких свідчить про те, що жодна держава не здатна їх подолати, покладаючись виключно на власні сили. По-третє, прагнення України до євроінтеграції неможливо втілити без встановлення міцних зв'язків із європейськими державами, в тому числі і у питанні кібербезпеки.

О. В. Орлов та Ю. М. Онищенко доцільно відзначають, що до форм міжнародної співпраці відноситься видача кіберзлочинців, надання взаємної правової допомоги, взаємне видання судових рішень, співпраця між правоохоронними органами [112, с. 20]. Оскільки в силу нестійкого характеру доказів у справах про кіберзлочини, важливими є терміновість та своєчасність встановлення міждержавних зв'язків у кожній окремій кіберсправі, тож у питаннях розслідування екстериторіальних кіберзлочинах варто звертатись до традиційних форми співпраці. О. В. Орлов та Ю. М. Онищенко відзначають важливу роль офіційних прохань про надання взаємної правової допомоги [112, с. 20], проте очевиднішим є прийняття двосторонніх чи багатосторонніх документів про співпрацю. Прикладами таких угод є прийняті у 2001 році Угода про співробітництво держав-учасниць Співдружності Незалежних Держав у боротьбі із злочинами у сфері комп'ютерної інформації [44] та Конвенція про кіберзлочинність [1]. Тож важливість ролі міжнародних нормативно-правових актів за таких умов є очевидною.

Конвенція про кіберзлочинність [1] є одним із найважливіших документів у сфері глобальної комп'ютерної мережі та на сьогодні єдиним документом такого рівня, що була ратифікована Україною 7 вересня 2005 року [8]. Міжнародному співробітництву країн учасниць у сфері боротьби з кіберзлочинністю присвячено окремий розділ, у якому висвітлено принципи: 1) екстрадиції (стаття 24); 2) взаємодопомоги (статті 25 та 26) [1]. Це означає, що на міжнародному рівні можливим є не лише дозвіл на оперативно-

розшукову діяльність на території інших держав, а й надання будь-якої необхідної допомоги, у тому числі й передачі однією державою іншій особи, що підозрюється або обвинувачується в скоєнні злочину, або ж засудженого злочинця. Це є свідченням того, на якому рівні на сьогодні перебувають встановлені міжнародні домовленості щодо співпраці держав у сфері боротьби із кіберзлочинністю, оскільки лише скоординовані зусилля можуть надати переваги державам у встановленні інформаційної безпеки держав та кожного окремого громадянина.

Тож, у процесі аналізу наукової літератури нами встановлено наступні проблеми, що негативним чином впливають на міжнародне співробітництво у сфері боротьби з кіберзлочинністю в Україні: 1) відносна молодість даного інституту в Україні, а отже необхідність удосконалення вітчизняного законодавства до загальноприйнятих світових стандартів; 2) незначна кількість міждержавних угод у сфері боротьби із кіберзлочинністю, укладених Україною, та міжнародних нормативно-правових актів, ратифікованих нашою державою.

А тому, втілення тенденції посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні вбачаємо у наступних діях:

1) Ратифікація окремих міжнародних нормативно-правових актів у сфері боротьби з кіберзлочинністю – наприклад:

I) Віденська декларація про злочинність і правосуддя: відповіді на виклики XXI століття (ООН) від 17.04.2000 року [41] – Україна є однією із засновниць Організації Об’єднаних Націй. Зазначений документ символізує об’єднання членів даної організації у протидії новим формам злочинності, що з’явились наприкінці XX століття. Тому, важливою є участь України у даному процесі та отримання належної допомоги у розслідуванні транснаціональних кіберзлочинів;

II) у разі завершення процесу євроінтеграції, важливим кроком є ратифікація Конвенції про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу [42] – для того, щоб

взаємодопомога між державами-членами у справах про кіберзлочини надавалась швидко й ефективно, а Україна була складовою даного процесу;

2) Укладення міжнародних двосторонніх чи багатосторонніх угод – зокрема із державами-сусідами України, а враховуючи євроінтеграційне прагнення нашої держави - із європейськими країнами;

3) Надсилання правової допомоги іншим державам у кримінальних справах, обмін відомостями оперативно-розшукового характеру з іншими державами у справах про кіберзлочини, виїзд членів слідчо-оперативних груп за кордон та прийняття працівників правоохоронних органів іноземних держав в Україні для проведення слідчих і оперативно-розшукових дій – такі дії можуть здійснюватись лише за умови укладення угод з іншими державами;

4) Здійснення детального наукового аналізу міжнародного законодавства та аналіз досвіду інших країн у сфері боротьби з кіберзлочинністю.

Тенденція збільшення рівня контролю за користувачами мережі Інтернет полягає у зміні балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина в інтересах держави. Дана тенденція у цілому є вкрай негативним явищем, проте за умови досягнення кіберзлочинністю катастрофічних масштабів, подібне рішення може виступити у якості основного вирішення поставлених перед державою завдань.

Впродовж останніх десятиліть було сформовано концептуальне розуміння боротьби з кіберзлочинами та захистом інтересів держави в інформаційній сфері як забезпечення належного і стійкого балансу між правоохоронними інтересами та повагою до основних прав і свобод людини й громадянина. При цьому, звичайно і на сьогодні існує можливість використання інформаційних технологій на шкоду основним правам і свободам людини. З точки зору І. М. Забари, така шкода може виражатись у використанні інформаційної інфраструктури для здійснення неправомірного

доступу до інформації; неправомірному поширенні інформації; порушенні конфіденційності, цілісності та доступності інформації, комп'ютерних даних і систем; протизаконному використанні програм та баз даних, що є об'єктами інтелектуальної власності; поширенні інформації, що розпалює міжнаціональну, міжрасову та міжконфесійну ворожнечу, расистських та ксенофобських писемних матеріалів, зображень або будь-якої іншої демонстрації ідей або теорій, які пропагують, сприяють або підбурюють до ненависті, дискримінації, насильства [141, с. 3]. Загалом, питання пошуку балансу між приватними і публічними інтересами є одним із невирішених в повній мірі в Україні. Так, на сьогодні у низці законодавчих актів визнається пріоритет приватних інтересів, зокрема у Конституції України [6], у статті 32 якої встановлюється недопущення збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини. Відповідно, із положеннями даної статті узгоджуються норми інших актів вітчизняного законодавства, у тому числі і Закону України «Про інформацію» № 2657-XII від 02.10.1992 [46], Цивільного кодексу України [142] тощо. Водночас, вітчизняні науковці доцільно відзначають, що у низці законодавчих актів визнається пріоритет приватних інтересів, оскільки «приватний інтерес (як індивідуальний, так і колективний) потребує не лише захисту зі сторони держави і суспільства, але й забезпечення його суспільної спрямованості і соціальної відповідальності» [143, с. 33]. Тобто, друга група нормативно-правових актів складається із законодавчих актів, у яких встановлюється пріоритет публічного інтересу над приватним. Іншими словами, в першу чергу здійснюється забезпечення фундаментальних засад функціонування держави та суспільства, а приватні інтереси забезпечуються по мірі настання такої необхідності. Тому, у питаннях, пов'язаних із кібербезпекою, питання балансу між правами людини та потребами й інтересами суспільства і держави є одним із основних у даній сфері в світлі прийняття останніх рішень Радою

національної безпеки і оборони України. Наприклад, 15.05.2017 р. Президентом України було підписано Указ №133/2017, яким введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [144]. Зокрема, цим Указом в тому числі і з метою забезпечення кібербезпеки Інтернет-провайдери повинні заборонити доступ до низки російських ресурсів. Це є підтвердженням того, що контроль за користувачами мережі Інтернет це не просто перспектива, а чинний інструмент забезпечення кібербезпеки, який і в подальшому буде реалізовуватись у вітчизняному законодавстві.

Як влучно зазначає С. В. Савченко, ускладнення суспільних відносин в Україні обумовлює різні форми співвідношення приватних і публічних інтересів, що істотно ускладнює їх реалізацію, внаслідок чого в правових відносинах простежується їх протистояння і навіть конфлікти [145, с. 56]. Саме такий конфлікт на сьогодні спостерігається в Україні, оскільки інтерес держави домінує над інтересами громадян, що значним чином викликає їх невдоволення. Проте, якщо навіть поверхнево звернутись до досвіду зарубіжних держав, можна зробити висновок, що подібний контроль є звичним явищем. Наприклад, у Сполучених Штатах Америки необхідні закони приймаються по мірі появи такої необхідності [146, с. 24]. Тому, в різні часи в державі були прийняті обмеження щодо захисту авторських прав, доступу до інформації та її розповсюдження, встановлені серйозні вимоги до надавачів Інтернет-послуг. У Франції діють обмеження щодо публікації особливих категорій матеріалів, а власники веб-ресурсів підлягають реєстрації [147, с. 88]. З однієї сторони, такі обмеження не є тотожними із прийнятими в Україні, проте обидві ситуації об’єднує факт встановлення контролю та обмеження можливості громадян вільно розпоряджатись благами кіберпростору.

Однією із держав із подібним до щойно встановленого в Україні контролю, є Китай. Для даної держави характерними є обмеження доступу

для користувачів на окремі веб-ресурси та контрольований вхід до мережі. Проте, стрімкий розвиток науково-технічних технологій на сьогодні дозволяє обійти ці перешкоди і як зазначає Н. В. Савчук, на сьогодні для ефективний і повний контроль в даній державі є проблематичним [146, с. 28]. Подібна ситуація спостерігається і в Україні, оскільки не зважаючи на виконання провайдерами вимог Ради національної безпеки і оборони України, у користувачів Інтернету залишаються можливості для обходу цих заборон. А отже, зробимо висновок, що до проблем втілення такої тенденції варто віднести: 1) необхідність переосмислення сутності конституційних прав та свобод людини і громадянина; 2) проникнення держави у приватне життя громадян; 3) посилення контролю, що негативним чином відіб'ється на суспільстві; 4) обмеження можливостей людини вільно розпоряджатись благами науково-технічного прогресу.

Сама ж тенденція збільшення рівня контролю за користувачами мережі Інтернет повинна втілюватись наступним чином:

1) Встановлення правил користування громадянами кіберпростором - наприклад як і у випадку з прийняттям Указу Президента України №133/2017, яким введено в дію рішення Ради національної безпеки і оборони України від 28 квітня 2017 року «Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)» [144], яким заборонено доступ до окремих Інтернет ресурсів. Схожим чином буде здійснюватись регулювання й інших питань, пов'язаних із контролем за користувачами мережі Інтернет;

2) Створення спеціальних органів контролю, покликаних спостерігати та виявляти порушників встановлених правил користування кіберпростором – на сьогодні таким органом є Департамент кіберполіції Національної поліції України, проте збільшення обсягу контролю потребуватиме розширення такої мережі.

На відміну від тенденцій, розвитку правового регулювання боротьби з кіберзлочинністю в Україні, які є явищем, що узагальнюють напрямки

розвитку відповідного інституту, визначені на сьогодні, перспективи є можливостями, що мають чи можуть бути реалізованими в майбутньому. Ураховуючи існуючі тенденції, та виділені нами у процесі дослідження проблеми, основною перспективою ми вбачаємо ліквідацію кордонів між державами у питаннях боротьби з кіберзлочинністю.

Кіберзлочинність – це міжнародна проблема, оскільки кіберпростір, як об’єкт її посягання, не обмежується державними кордонами. Саме тому для протидії цим негативним явищам мають бути залучені усі без виключення країни світу, безвідносно географічного положення, рівня соціально-економічного та технічного розвитку, а також рівня прийнятого національного законодавства. Саме тому більш розвинені у технологічному відношенні держави повинні мати можливість допомагати менш розвиненим у питаннях запобігання та розслідування кіберзлочинів.

Міжнародним правом передбачена низка підстав для визначення юрисдикції за територіальним принципом чи принципом громадянства. Більшість з них є закріпленими в міжнародних нормативно-правових актах, присвяченим запобіганню кіберзлочинності. Разом з тим, присутні і норми, які надають суб’єктам міжнародного права певну свободу у таких правовідносинах. Наприклад, в Конвенції про кіберзлочинність присутня норма, яка надає право учасникам на здійснення доступу до публічно доступних комп'ютерних даних, які зберігаються, не отримуючи дозволу від іншої сторони, не зважаючи на те, де такі дані знаходяться географічно; або здійснювати доступ або отримувати за допомогою комп'ютерної системи, яка знаходиться на її території, комп'ютерні дані, які зберігаються і знаходяться в іншій стороні, якщо сторона отримує законну і добровільну згоду особи, яка має законні повноваження розкривати дані такій стороні за допомогою такої комп'ютерної системи [1]. Існування такої норми значно спрощує міждержавні відносини та зменшує рівень бюрократизації у відносинах, де час відіграє вагому роль. Тому вважаємо статтю 32 Конвенції про

кіберзлочинність важливою передумовою реалізації досліджуваної тенденції у майбутньому.

Наявність лише однієї такої норми свідчить про нерозвиненість правової бази попередження та регулювання негативного явища кіберзлочинності, не зважаючи на те, що з точки зору усіх країн Європи їхнє національне законодавство забезпечує достатню основу для криміналізації і переслідування екстериторіальних кіберзлочинів. О. В. Орлов та Ю. М. Онищенко в даному контексті відзначають, що в законодавстві численних країн закріплено ідею про те, що для визнання територіальної юрисдикції всередині країни повинно бути здійснено не обов'язково «весь» злочин. Тобто, територіальна прив'язка може бути здійснена щодо елементів, наслідків діяння чи місцеперебування комп'ютерних систем або даних, які використовувалися для скоєння злочину. При виникненні конфліктів між державами, вони вирішуються шляхом проведення взаємних консультацій [112, с. 19]. Іншими словами, на сьогодні країни не вбачають необхідності у встановленні додаткових мір встановлення юрисдикції у кіберпросторі. За теперішніх умов є достатніми форми юрисдикції за територіальною ознакою та згідно громадянству, що практично завжди може забезпечити достатній зв'язок між кіберзлочинами та хоча б однією державою. Проте, розвиток кіберзлочинів та поява нових інструментів протиправного впливу на суспільний порядок можуть докорінно все змінити. Як ми вже відмічали, специфіка кіберзлочинів полягає у тому, що знищення будь-яких доказів чи слідів протиправної діяльності є можливим у найкоротші строки. За умови, коли дана можливість ще зменшиться, світова спільнота потребуватиме швидких дій, а ліквідація кордонів між державами у питаннях боротьби з кіберзлочинністю здатна забезпечити цю швидкість.

Проблеми втілення даної перспективи на сьогодні вбачаємо в наступному: 1) загальна незацікавленість держав світу до подібних дій; 2) поки що наявна можливість протистояти кіберзлочинності у той спосіб, який дозволяє чинне законодавство про боротьбу із кіберзлочинністю; 3)

«відкриття» кордонів для правоохоронців може призвести до розширення свободи дій у зловмисників; 4) така концепція потребує чіткої взаємодії між правоохоронними органами усіх держав.

Дана перспектива є можливою за умови втілення наступних завдань:

1) Стандарти законодавства про боротьбу із кіберзлочинністю державами світу мають бути єдиними для усіх країн світу – як нами встановлено, на сьогодні у міжнародному праві наявний значний масив нормативно-правових актів, що регламентують боротьбу з кіберзлочинністю. Проте, їх дія поширюється лише на окремі групи країн та існує низка бюрократичних перепон, що не дозволяють оперативно розслідувати випадки кіберзлочинів, здійснених з території інших держав чи за участі іноземних громадян. Тому, головним завданням є залучення до даного процесу якомога більшої кількості країн та пришвидшення процесу ратифікації ними усіх необхідних нормативно-правових актів;

2) Забезпечення обміну інформацією щодо кібертерористичних організацій та кібертерористів, у тому числі їх особистими та біографічними даними – такий напрям можна реалізувати шляхом створення єдиної бази даних для спецслужб світу та забезпечити автоматизований обмін даними між правоохоронними органами країн щодо осіб, які мають судімість за вчинення кіберзлочинів чи підозрюються у здійсненні шкідливої протиправної діяльності у кіберпросторі;

3) Чітка регламентація координування відповідних підрозділів правоохоронних органів усіма державами, що буде здійснюватися за допомогою прийнятого законодавства – іншими словами, основним завданням є забезпечення оперативності реагування правоохоронців різних держав на кіберзагрози. Такий напрям можливо реалізувати шляхом внесення змін до Конвенції про кіберзлочинність [1]. Так, на сьогодні даним міжнародним нормативно-правовим актом передбачено можливість міжнародного співробітництва у сфері боротьби із кіберзлочинністю без укладання міжнародних угод. Наприклад, сьогодні кожна сторона надає одна

іншій взаємну допомогу у найширшому обсязі з метою розслідування або переслідування кіберзлочинів, а держави, які не є сторонами Конвенції вимушені для початку надсилати запити про таку допомогу, які можуть бути відхиленими за бажанням іншої держави. Тому, першим і головним завданням є забезпечення ратифікації Конвенції про кіберзлочинність [1] усіма державами світу. По-друге, необхідним є прийняття єдиного законодавства, що регламентуватиме діяльність підрозділів правоохоронних органів усіх держав. Таким нормативно-правовим актом може бути Конвенція проти транснаціональної кіберзлочинності, мета якої полягатиме у сприянні співробітництву в справі більш ефективного попередження та боротьби із транснаціональною організованою злочинністю та боротьби з нею.

Таким чином, на сучасному етапі проблема кіберзлочинності набула глобального виміру та являє собою серйозну загрозу усім без винятку суспільним відносинам у державі. Тож, встановлення перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні є питанням, що не втрачає актуальності.

Тенденції є явищем, що являють собою сукупність напрямів розвитку правового регулювання боротьби з кіберзлочинністю в Україні. Дослідження засвідчило, що на сьогодні нашою державою ведеться активна діяльність щодо покращення існуючої ситуації з кібербезпекою. В умовах курсу до євроінтеграції та реальних кіберзагроз, вітчизняному законодавцю варто все ж посилити діяльність у даному напрямку. Як засвідчило дослідження, національне законодавство все ще перебуває на недостатньому рівні для вирішення поточних проблем, а співробітництво з іншими державами у даному напрямі потребує посилення. Окрім того, стратегічним напрямом є встановлення часткового контролю над кіберпростором. Всесвітня мережа характеризується відсутністю кордонів та анонімністю, проте окремі напрями очікуваних загроз можливо передбачити, що і може бути віднесено

до об’єктів державного регламентування користування Інтернетом. Більше того, подібні процеси уже розпочато.

Перспективи розвитку правового регулювання боротьби з кіберзлочинністю в Україні, як категорія, що узагальнює те, що має чи може бути реалізоване в майбутньому, у цілому перебуває поза увагою вчених-правовиків. Майбутній розвиток досліджуваного інституту вбачаємо у вирішенні існуючих на сьогодні проблем, таких як проблеми нормативного та понятійного характеру, неможливість реалізації досвіду зарубіжних держав, без вирішення внутрішніх соціально-економічних проблем, проблеми недостатнього наукового аналізу даного питання тощо. Оскільки кіберпростір не має меж, усі існуючі проблеми мають вирішуватись на міждержавному рівні. Тож, дослідження перспектив та тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні продемонструвало, що еволюція даного інституту має бути багатовекторною, оскільки проблем у його регламентації залишається чимало.

3.2 Специфіка правового регулювання боротьби з кіберзлочинністю у зарубіжних країнах

Одним із пріоритетних напрямів удосконалення вітчизняної правової системи є впровадження міжнародних концепцій, принципів та ідей. В умовах євроінтеграційних процесів важливою є заміна застарілих способів та методів у регулювання суспільних відносин та виконання конкретних вимог, які поставлені перед Україною. Актуальність дослідження зарубіжного досвіду організації та функціонування системи правового регулювання боротьби із кіберзлочинністю зумовлена загостренням ситуації із збільшенням об’ємів злочинної діяльності у кібермережах та відсутністю у нашої держави значних успіхів в даній сфері останнім часом. Масштаби мережі Інтернет свідчать про те, що окремі елементи кіберзлочинності не можуть обмежуватись територією певної держави, тому в будь-якому

випадку національне законодавство повинно відповідати загальноприйнятим стандартам у даній сфері для можливості здійснювати міжнародне співробітництво. Більше того, процес становлення системи правового регулювання боротьби із кіберзлочинністю є неможливим без урахування досягнень та помилок, допущених іноземними державами при формуванні даного інституту.

Розвиток правового регулювання боротьби із кіберзлочинністю в Україні перебуває на активній стадії протягом останніх двох десятиліть. У багатьох зарубіжних країнах дана система працює вже давно та має позитивні результати, хоча кіберзлочинність на цей момент все ж опереджає за рівнем розвитку інструменти протидії їй. Тому, аналізуючи сучасні вітчизняні реалії, можна відмітити незавершеність даного процесу в Україні та потребу у подальших перетвореннях. За таких умов набувають актуальності питання позитивного та негативного досвіду інших держав, що є цілком доцільним вектором розвитку досліджуваного інституту. Саме тому, досвід інших країн у даній сфері є корисним для нашої країни і становить важливу тему для дослідження.

Проблематика аналізу правового регулювання боротьби із кіберзлочинністю у зарубіжних країнах досить часто обговорюється фахівцями, проте дане питання не належить до числа досліджених належним чином. Поза увагою переважно залишається встановлення позитивного досвіду більш досвідчених держав та можливості його імплементації у вітчизняну правову систему. Окремі проблеми розглядались такими дослідниками, як Дж. Арас, Дж. Блумбекер, М. О. Будаков, С. В. Бреннер, В. М. Бутузов, М. Вертузаева, М. М. Галамба, М. Д. Гудман, Д. Д. Елліотт, А. Калюжний, В. В. Коваленко, Я. Ю. Кондратьєв, Б. А. Кормич, А. Левін, Ю. М. Максименко, В. В. Марков, А. І. Марущак, Г. В. Новицький, Ю. М. Онищенко, О. В. Орлов, А. Л. Осипенко, Т. Л. Путмен, Т. Л. Сироїд, В. С. Сідак, Р. Ю. Сень, І. М. Сопілко та іншими. Проте, питання особливостей правового регулювання боротьби із кіберзлочинністю у зарубіжних країнах

та шляхів запозичення позитивного досвіду в Україну потребує більш комплексного та деталізованого підходу, що і зумовлює актуальність обраної теми дослідження.

При виборі країн, чий досвід є корисним для України, варто відштовхуватись від наступних критеріїв: 1) стратегічним партнером України є Сполучені Штати Америки, які останніми роками надають значну правову та фінансову допомогу Україні, тож доцільним є встановлення їх досвіду, з огляду на рівень розвитку даної держави; 2) євроінтеграційні перспективи України безпосередньо залежать від ступеня втілення європейських стандартів у вітчизняну правову систему; 3) важливим є звернення до досвіду деяких сусідніх держав, в першу чергу колишніх учасників Союзу Радянських Соціалістичних Республік, для порівняння рівнів розвитку даного інституту та встановлення позитивних моментів, на сьогодні не втілених в Україні.

Розпочнемо із досвіду Сполучених Штатів Америки, як держави, що зазнає значного негативного впливу від кіберзлочинців, та є однією із перших в історії, що зайнялась розробкою відповідних нормативно-правових актів. Як доречно відзначає Н. В. Савчук, американська політика у сфері кіберпростору має значний вплив на країни європейського співтовариства [146, с. 25], а отже дослідження її досвіду є важливим питанням у контексті тематики нашого дослідження. Серед норм Національної стратегії внутрішньої безпеки США, прийнятої в 2015 році, особливий інтерес представляє розділ «Кіберзахист», у змісті якого наголошується на необхідності захисту від кібератак на теренах кіберпростору. Сполучені Штати Америки, проголошуючи себе батьківщиною Інтернету, взяли на себе відповідальність перед усім мережевим світом за забезпечення безпеки в кіберпросторі. Окрім того, проголошено курс на посилення законодавчої бази та підвищення стандартів захисту прав та інтересів громадян [148, с. 12]. Тому, Сполучені Штати Америки є однією із першочергових держав для дослідження досвіду. В даній країні постійно здійснюється активна

діяльність з протидії таким негативним явищам, як кіберзлочинність, значна увага приділяється безпеці громадян у цілому. США є однім із головних об'єктів кіберзлочинців із усього світу, тож досвід даної держави є корисним для розробки правових інструментів, спрямованих на протистояння даному негативному явищу.

Не зважаючи на вищесказане, у Сполучених Штатах Америки переважає концепція саморегулювання мережі Інтернет, а отже спеціальне законодавство у даній сфері представлено лише кількома нормативно-правовими актами. Наприклад, до них варто віднести Закон про електронний підпис, прийнятий у 2000 році [147, с. 87]. Його основне призначення – забезпечення правового режиму електронного підпису в комерційних відносинах. В Сполучених Штатах Америки прийнято надавати даному нормативному акту символу вступу людства у нову еру – еру електронної комерції. Сам же Закон є доволі стислим і закріплює незначну кількість понять та механізмів – у тому числі, компетенцію державних органів, відповідальних за функціонування усієї інфраструктури у даній сфері, взаємодію її елементів та органів державної влади тощо.

Як відзначає Н. В. Савчук, в країні давно переважає думка, що закон варто приймати лише у тому випадку, якщо усунення проблеми без цього є неможливим. Наприклад, 1 червня 1997 року президентом США була зроблена доповідь «Політика в галузі глобальної інформаційної комерції», у якій було сформульовано основні принципи політики держави у сфері надання Інтернет-послуг, один із яких: «уряд повинен встановлювати зрозумілі, мінімальні та прості правові норми лише там, де це потрібно» [149, с. 149]. Це означає, що активна боротьба із кіберзлочинністю у вигляді регламентації відповідних відносин здійснюється лише у тих сферах, де існують негативні тенденції до вчинення протиправних діянь, а інші характеризуються саморегуляцією та врегульовуються лише по мірі виникнення загроз. Такий досвід не є позитивним для переймання, проте як свідчить практика, Сполучені Штати Америки є однією з найзахищеніших

країн світу. Тому варто зробити висновок, що боротьба із кіберзлочинністю повинна мати комплексний характер, а відповідне галузеве законодавство є лише одним із елементів.

Найбільшу кількість нормативно-правових актів прийнято у сферах емісії цінних паперів, охорони інтелектуальної власності, захисту від несанкціонованого доступу до інформації, авторського права тощо [146, с. 25]. Загалом, до недавнього часу американські юристи підтримували точку зору, що для регулювання боротьби із кіберзлочинністю важливішими є міждержавні, а не національні нормативно-правові акти, оскільки введення певних обмежень одним суб'єктом може негативно вплинути на інтереси інших сторін [147, с. 87]. Проте, внаслідок терористичних актів 11 вересня 2001 року значним чином було посилено боротьбу із тероризмом, одним із різновидом якого є кібертероризм. В тому ж році урядом США було прийнято Закон «Про об'єднання та зміцнення США», згідно норм якого будь-яка дія, яка спричиняє порушення в роботі чи призводить до незаконного проникнення в комп'ютер, класифікується як тероризм. В свою чергу провайдер зобов'язаний надати всю відому йому інформацію про користувача на першу вимогу Федерального бюро розслідувань [150]. Таким чином, на сьогодні вектор правового регулювання боротьби із кіберзлочинністю пов'язується із протидією кібертероризму, як найнебезпечнішого вияву кіберзлочинності. Так, 17 листопада 2014 року було заявлено про ремонт системи електронної пошти Держдепартаменту США після можливої шкоди завданої ймовірною хакерською атакою [151, с. 71]. На сьогодні, Сполучені Штати Америки перебувають у стані постійної готовності до захисту своїх громадян від негативного впливу кіберзлочинців. Зважаючи на загальну кількість кібератак, важливими проблемами, які постають перед США, є проведення оперативно-розшукових заходів та покарання порушників закону. Одними із елементів таких процесів є збільшення міри відповідальності за вчинення комп'ютерних злочинів та захист прав й інтересів громадян у разі завдання шкоди.

Деструктивна діяльність в кіберпросторі США санкціонується значно жорсткіше, ніж у Європі. Так, у Сполучених Штатах визначено кримінальну відповідальність за неналежне зберігання та обробку персональної інформації чи її знищення у відмінний, від встановленого законом спосіб. Для порівняння, у країнах Європейського Союзу кримінальні справи можуть заводитися лише у випадку завдання шкоди державній безпеці та основним правам громадян [152, с. 126]. Це свідчить про те, що соціальним аспектом правового регулювання боротьби із кіберзлочинністю в Сполучених Штатах не знехтувано, оскільки величезне значення все ще має не лише захист державних інтересів, а й кожного окремого громадянина.

Тож, дослідження сучасного стану боротьби із кіберзлочинністю засвідчило, що даний напрям є одним із пріоритетних у державній політиці США. Позитивними тенденціями є активна боротьба із кібертероризмом та оперативність заходів по вирішенню існуючих проблем. До негативних віднесемо передусім реагування на загрози лише по мірі їх настання, проте в той же час Сполучені Штати Америки залишаються однією із найзахищеніших держав світу.

У контексті боротьби із кіберзлочинністю, важливим є аналіз нормативно-правових актів, у яких закріплено повноваження органів державної влади та правоохоронних органів щодо протистояння кіберзлочинам.

У 2009 році у Сенаті США зареєстровано законопроект «Акт про кібербезпеку 2009» (Cybersecurity Act of 2009) [153], розроблений Національною розвідкою Сполучених Штатів Америки, яким було запропоновано значним чином розширити повноваження федеральної влади у сфері забезпечення кібербезпеки та передбачити обов’язкову ідентифікацію користувачів кіберпростору в інтересах національної безпеки. Даний законопроект у разі прийняття значним чином міг би вплинути на суть сучасного Інтернету, адже з його допомогою планувалось встановити нові стандарти комп’ютерної безпеки, зокрема шляхом встановлення стандартів,

які би зобов'язали користувачів здійснювати обов'язкову ідентифікацію та дати згоду уряду на законних підставах перевіряти вміст електронних листів, переданих файлів, пошукових запитів користувачів кіберпростору тощо [153]. Проте, даний закон все ж не було прийнято і це є позитивним моментом в контексті захисту прав людини і громадянина. Прийняття такого нормативно-правового акту державою, що має вагомий вплив на усі глобальні процеси, безсумнівно мало б серйозний вплив на усю світову систему кібербезпеки і такий досвід поступово би переймався іншими країнами. На сьогодні в Україні ми все ж спостерігаємо спроби державної влади встановити контроль за користувачами Всесвітньої мережі та спрямовувати діяльність громадян у кіберпросторі у вигідному для держави напрямку, але масштаби наслідків нинішньої ситуації в Україні та перспектив для громадян США за умови прийняття Акту все ж відрізняються значним чином.

Продовжуючи аналіз нормативно-правової бази боротьби із кіберзлочинністю Сполучених Штатів Америки, відзначимо вагому роль законодавства у сфері захисту інформації. Як відзначає І. М. Сопілко, щодо захисту інформації уряд США керується принципом недопущення перехоплення іноземними державами конфіденційної державної і приватної інформації, а також відкритої інформації, що передається урядовими й комерційними телекокомунікаціями, що може завдати шкоди державі або ж її громадянам [151, с. 73]. Для забезпечення такого рівня захисту, в технічному аспекті було зроблені значні кроки для захисту ліній зв'язку й автоматизованих систем, а у нормативному – прийнято Закон «Про забезпечення безпеки ЕОМ» № HR – 145 [154]. Так, його нормами зокрема встановлено вимоги для державних організацій щодо забезпечення необхідного рівня захисту інформації. Наприклад, у частині 3 Закону зазначено, що «важливою є інформація, втрата, зміна або доступ до якої може призвести до небажаних наслідків для національних інтересів» [154]. Це свідчить про те, що на початкових етапах основна увага у правовому

регулюванні боротьбі із кіберзлочинністю все ж уділялась державним інтересам, а приватні були захищені у меншій мірі. Проте, останніми роками спостерігаються спроби посилити захист індивідуальних суб'єктів. США, як високотехнологічна держава, забезпечила захист стратегічних об'єктів на високому рівні, тому кіберзлочини, спрямовані проти держави у цілому, відбуваються набагато рідше і потребують серйозної підготовки і умінь у кіберзлочинців. Прості громадяни частіше постають у якості об'єктів кібератак на сьогодні, тому сучасна нормотворча діяльність у Сполучених Штатах Америки пов'язується із захистом прав та інтересів громадян.

І. М. Сопілко відзначає внесення законопроектів, які передбачають посилення відповідальності за порушення у сфері захисту індивідуальної інформації, у тому числі шляхом інсталяції програмного забезпечення для збору індивідуальної інформації, ідентифікації користувача, без його відома та згоди [151, с. 73]. Тому, можна зробити висновок, що правове регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки регламентується жорсткіше, ніж у Європі. Якщо у європейських державах основна увага приділяється завданні шкоди державним інтересам та основним правам громадян, то у США до кримінальних проступків високого рівня небезпечності зараховується і неналежне зберігання й обробка персональної інформації та її знищення не за законом.

Окрім того, привертає увагу і система органів, що здійснюють боротьбу із кіберзлочинністю: 1) Кібернетичне командування США (United States Cyber Command, USCYBERCOM) – підрозділ збройних сил США, основними завданнями якого є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж США; 2) Комп'ютерна команда екстреної готовності США (United States Computer Emergency Readiness Team, US – CERT) – частина Національного відділу кіберзахисту Міністерства внутрішньої безпеки США, яка випускає інформацію про поточні питання безпеки, вразливі до кібервпливу об'єкти і працює з постачальниками програмного забезпечення для створення

спеціальних програмних застосувань, які усувають прогалини в системах безпеки; 3) відділ комп'ютерної злочинності і інтелектуальної власності (Computer Crime and Intellectual Property Section, CCIPS) – відділ у карних справах Міністерства юстиції США з розслідування комп'ютерних злочинів і порушення прав інтелектуальної власності, який спеціалізується в зоні пошуку і захоплення цифрових доказів у комп'ютерах і мережах [155, с. 213-214]. Для порівняння, в Україні на сьогодні діє лише один такий орган - Департамент кіберполіції Національної поліції України, тобто боротьба із кіберзлочинністю здійснюється лише на правоохоронному рівні, чого є недостатньо в сьогоднішніх умовах. В США таких рівнів троє – військовий, правоохоронний та юстиційний, при чому кожен із них наділений особливими повноваженнями. Тому, відповідно і боротьба із кіберзлочинністю здійснюється значно ефективніше. Звернемо увагу на військовий напрям, який є актуальним для держави, що веде неоголошену війну. О. В. Орлов та Ю. М. Онищенко в даному контексті вживають термін «операції кібервійни» [155, с. 214]. Переносячи дане визначення у сучасні українські реалії, відзначаємо, що на сьогодні відбувається значний та деструктивний вплив на кібермережі вітчизняних органів державної влади та інших стратегічних для країни об'єктів. Більше того, значних масштабів набули інформаційні атаки у Інтернеті, передусім у соціальних мережах. Тому, такий досвід Сполучених Штатів міг би бути корисним у сучасних умовах.

Таким чином, виділимо основні характеристики правового регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки: 1) США вважають себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) дана держава має значний вплив на прийняття відповідного законодавства у країнах Європейського Союзу; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам.

Окремі із проаналізованих напрямів є безперечно доцільними для втілення в нашій державі. Тому, виділимо наступні шляхи запозичення позитивного досвіду Сполучених Штатів Америки в Україну:

1) посилення відповідальності за злочини у сфері захисту індивідуальної інформації.

Не зважаючи на те, що у цілому в Сполучених Штатах відповідальність за кіберзлочини є суворішою, ніж у європейських державах, сьогодні в США існує можливість встановлення санкцій за порушення у сфері захисту індивідуальної інформації у розмірі штрафу до 1 мільйона доларів або ув'язнення до 5 років [152, с. 73]. Вважаємо, що такий досвід варто перейняти і в українських реаліях. Тому, Розділ XVI Кримінального кодексу України [3] пропонуємо доповнити статтею:

- «Порушення у сфері захисту індивідуальної інформації. 1. Порушення у сфері захисту індивідуальної інформації суб'єктів, персональні дані яких обробляються у вигляді незаконних втручань та втрати даних у мережі Інтернет, - карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до п'яти років. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою групою осіб, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до шести років».

2) посилити захист від перехоплення іноземними державами конфіденційної державної і приватної інформації, а також відкритої інформації, що передається урядовими й комерційними телекомунікаціями, що може завдати шкоди державі або ж її громадянам.

Необхідність вдосконалення Закону України «Про основні засади забезпечення кібербезпеки України» має важливість у наступних положеннях: 1) зобов'язати державні організації забезпечити необхідний рівень захисту інформації від кібервпливу; 2) сформувати у суспільстві розуміння необхідності захисту інформації; 3) заповнити прогалини у вітчизняному законодавстві про інформацію.

Тому, в нормах даного нормативно-правового акту пропонується встановити захист ліній зв'язку й автоматизованих систем пріоритетним завданням компетентних державних органів. Також у Законі варто вирішити питання безпеки приватної та іншої інформації шляхом визначення вимог для державних організацій щодо забезпечення необхідного рівня захисту інформації.

3) розширити мережу органів, що здійснюють боротьбу із кіберзлочинністю.

Для виконання такого завдання необхідно: - визначитись, які саме органи необхідні для забезпечення кібербезпеки в Україні; - прийняти нормативно-правову основу їх діяльності. Використовуючи досвід США, найбільш доцільним напрямом буде створення підрозділу у рамках Збройних Сил України. Співвідносячи функції подібного підрозділу із повноваженнями Міністерства оборони України, варто відзначити, що згідно пункту 4 Положення про Міністерство оборони України, останнє здійснює моніторинг інформаційного середовища, виявляє потенційні та реальні інформаційні загрози в оборонній сфері, проводить попереджувальні інформаційні заходи [156]. Тобто, Міністерство здійснює переважно превентивну та організаційну діяльність. Водночас, необхідним є орган, до компетенції входитиме вчинення активних дій на кібернетичному фронті, у тому числі ведення операцій кібервійн та захисту військових комп'ютерних мереж України. У даному контексті даний орган значним чином відрізнятиметься від існуючого Департаменту кіберполіції, який здійснює попередження та протидію кіберзлочинам, виявляє та припиняє їх вчинення [9]. Пропонований підрозділ здійснюватиме функції, пов'язані із обороною України, захисту її суверенітету, територіальної цілісності та недоторканності під час ведення кібервійн. Звертаючись до досвіду Сполучених Штатів Америки, найбільш доцільною назвою для такого підрозділу буде Кібернетичне командування України. Тому, для регламентації діяльності потрібно: - по-перше, внести зміни до статті 3 Закону України «Про Збройні Сили України» від 06.12.1991

№ 1934-XII [157], та доповнити її наступним чином – «Збройні Сили України мають таку загальну структуру: … Кібернетичне командування України - підрозділ Збройних Сил України, основними завданнями якого є централізоване проведення операцій кібервійни, управління і захист військових комп'ютерних мереж України»; - по-друге, прийняти Положення про Кібернетичне командування України, яким регламентувати завдання та механізми їх реалізації.

До пріоритетних напрямків діяльності такого органу варто віднести протидію кібертероризму в умовах ведення військових дій, а також кіберзахист воєнних та інших стратегічних об'єктів. Тому в запропонованому Положенні варто визначити завдання такого органу, структуру, повноваження та механізми їх реалізації. Додаткові функції вбачаємо у впливі на кібермережі противників в умовах ведення війни. Тобто, даний орган покликаний в першу чергу стримувати і попереджувати агресію противника та брати участь у заходах, пов'язаних із боротьбою з кібертероризмом.

Таким чином, Сполучені Штати Америки як стратегічний партнер України та одна із найвпливовіших держав світу, постійно привертають увагу вітчизняних вчених-правовиків. Не зважаючи на те, що масив національного американського законодавства у даній сфері є незначним, усі правовідносини у сфері використання кібермереж є регламентованими належним чином. Тому, США є прекрасним прикладом для запозичення досвіду правового регулювання боротьби із кіберзлочинністю.

Окрім Сполучених Штатів Америки, належне усвідомлення загроз і небезпек, які містяться в безконтрольному використанні можливостей кіберпростору деструктивними способами, належить країнам Європейського Союзу, де вже досить давно практикується законодавче регулювання Інтернету. У контексті курсу України до євроінтеграції, корисним є встановлення як позитивного досвіду усієї організації, так і окремих держав, що входять до її складу.

Початок вирішення проблем нормативно-правового забезпечення боротьби із кіберзлочинністю у Європейському Союзі датовано початком XX століття, зокрема у 2001 році було представлено перший документ «Мережева та інформаційна безпека: європейський політичний підхід» (Network and Information Security: Proposal for A European Policy Approach), в якому окреслювався європейський підхід до проблеми інформаційної безпеки. Зокрема, під поняттям «мережева та інформаційна безпека» розуміється здатність мережі або інформаційної системи чинити опір випадковим подіям або зловмисним діям, які становлять загрозу доступності, аутентичності, цілісності та конфіденційності даних, що зберігаються або передаються, а також послуг, що надаються через ці мережі і системи [158; 159, с. 36]. Іншими словами, даним нормативно-правовим актом встановлювалось поняття та групування видів порушень безпеки кібермереж. Прийняття даного документу можна пов'язати із формуванням розуміння європейським співтовариством ролі мережевої безпеки у суспільних відносинах. Зазначення термінології «конфіденційність даних» свідчить про те, що розробниками нормативно-правового акту допускалась можливість атак на дані, що містять цінну інформацію, до якої доступ обмежено. У такий спосіб в Європейському Союзі розпочалась підготовку то захисту від збоїв систем комунікацій, та попередження можливості витоку конфіденційної інформації.

Важливими моментами даного документу було встановлення наступних напрямків європейської політики кібербезпеки: 1) освітній напрям, що полягав у підвищенні обізнаності споживачів кіберпослуг щодо загроз; 2) створення повноцінної системи попередження та інформування про нові загрози; 3) забезпечення належного технологічної підтримки; 4) стандартизація та сертифікація; 5) правове забезпечення; 6) зміцнення безпеки на державному рівні; 7) міжнародне співробітництво з питань інформаційної безпеки [160; 159, с. 36]. Варто зробити висновок, що більшість із цих напрямів є пріоритетними й на сьогодні. Більше того, окремі

з них є сучасними тенденціями розвитку правового регулювання боротьби із кіберзлочинністю й на сьогодні. Особливо звернемо увагу на напрям правового забезпечення. До моменту прийняття досліджуваного документу масив міжнародного законодавства у сфері кібербезпеки був не значним, проте у подальшому для вирішення проблеми кіберзлочинності, європейськими країнами прийнято низку нормативно-правових актів, серед яких особливе місце посідає Конвенція про кіберзлочинність [1], прийнята Комітетом міністрів Ради Європи в листопаді 2001 року та ратифікована Україною 7 вересня 2005 року [8]. Тобто, перші кроки для дотримання високих європейських стандартів уже здійснені нашою державою. Разом з тим, це не дає підстав стверджувати, що за рівнем правового регулювання боротьби із кіберзлочинністю Україна значним чином наблизилась до провідних європейських держав. У даному випадку доцільно зазначити, що навіть у межах Європейського Союзу кадрові та фінансові можливості країн відрізняються, а отже потенціал організацій, які здійснюють боротьбу із кіберзлочинцями не є однорідним.

Щодо подальшого врегулювання проблеми боротьби із кіберзлочинністю, у травні 2007 року Європейською Комісією було представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» (Towards a general policy on the fight against cyber crime), який є цікавим в першу чергу закріпленням терміну «кіберзлочинність» та висвітленням основних напрямів політики ЄС в сфері боротьби з кіберзлочинністю [159, с. 39]. Кіберзлочинність роз’яснюється як кримінальні дії, скоєні з використанням електронних комунікаційних мереж та інформаційних систем або проти таких мереж та систем. До даного поняття віднесено три категорії злочинів: 1) традиційні форми злочину (шахрайство та підробки в електронних комунікаційних мережах та інформаційних системах); 2) публікація протизаконного контенту в електронних медіа (дитяча порнографія, матеріали із закликами до расової ненависті і т.п.); 3) специфічні злочини в електронних мережах (атаки на

інформаційні системи, хакерство тощо) [160]. Із самою дефініцією погодимось, а також відмітимо доцільність розподілу кіберзлочинів на групи. Однією із проблем сучасного нормативно-правового регулювання боротьби із злочинністю є розмитість формулювань. Нами в межах даної роботи вже неодноразово було відмічено, що на даному етапі поняття кіберзлочинності суттєво розширилось і на сьогодні включає в себе види злочинів, які не є врегульованими належним чином. Формулювання, закріплене досліджуваним документом, демонструє яким чином могло б здійснюватись правове регулювання даного інституту у разі прийняття профільного нормативно-правового акту. В даній роботі нами запропоновано прийняття Закону України «Про боротьбу із кіберзлочинністю», який закріпить та узагальнить усі ключові поняття досліджуваного інституту, зокрема у одній із норм було би доцільно здійснити роз'яснення того, які ж саме групи злочинів віднесено до категорії кіберзлочинів.

Ураховуючи безмежні можливості Інтернету та переважне розслідування кіберзлочинів одразу декількома державами, особливого значення набувають міжнародні європейські організації. Зокрема, вітчизняними дослідниками відзначається роль наступних - Комп'ютерної групи швидкого реагування (CERT – Computer Emergency Response Team) у Брюселі та Європейського центру по боротьбі з кіберзлочинністю (European Cybercrime Centre) в Гаазі [155, с. 214-215], Європейської агенцію з питань мережевої та інформаційної безпеки (European Network and Information Security Agency - ENISA) [159, с. 38]. Комп'ютерна група швидкого реагування покликана боротись із новітніми комп'ютерними вірусами та виявляти слабкі місця в системі захисту інформації, здійснювати розробку інтернет-стратегії для Єврокомісії і проводити спільно із різними структурами ЄС семінари з кібербезпеки. Тобто, спектр діяльності даного органу є досить широким і включає в себе як активну теоретичну, дипломатичну, так і практичну діяльність. В свою чергу, Європейський центр по боротьбі з кіберзлочинністю функціонує на базі Європолу та покликаний

надавати інформаційну, оперативну і експертну підтримки розслідуванням на міжнародному і регіональному рівнях. Як відзначають О. В. Орлов, та Ю. М. Онищенко, дана організація сформована в рамках стратегії внутрішньої безпеки ЄС та укомплектована новітніми технологіями для проведення розслідувань, пов'язаних з кіберзлочинністю. До її складу входять найкращі фахівці Європолу у сфері боротьби із кіберзлочинністю та експерти безпеки з країн – учасниць Євросоюзу [155, с. 215]. Щодо завдань організації, ними є збір і обробка даних по кіберзлочинах, здійснених на території Європи, експертне оцінювання Інтернет-загроз, стимулюванням інформаційного обміну, розробка передових методів профілактики і розслідування кіберзлочинів, надання допомоги правоохоронним і судовим органам, і координування спільних дій зацікавлених сторін, які спрямовані на підвищення рівня безпеки в європейському кіберпросторі. Тобто, і у даному випадку має місце об'єднання в межах однієї організації як найкращих теоретиків, так і практиків у сфері боротьби із кіберзлочинністю. Діяльність Агенції спрямована на зміцнення можливостей європейської спільноти, країн-членів, а також ділових кіл в сфері попередження і реагування на проблеми, пов'язані з інформаційною безпекою. Даний орган виконує переважно дипломатичні функції, забезпечуючи співпрацю держав для вирішення проблем по мірі їх виникнення. Для України важливим є поширення діяльності таких організацій на її території, або ж по меншій мірі співпраця та обмін інформацією з ними.

Таким чином, правове регулювання боротьби із кіберзлочинністю у Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів,

розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

Отже, виділимо наступні шляхи запозичення позитивного досвіду Європейського Союзу в Україну:

1) еволюція вітчизняного законодавства згідно європейських стандартів.

Варто відзначити, що в даному випадку діяльність України є активною. Найголовніший нормативно-правовий акт у даній сфері, Конвенція про кіберзлочинність [1], ратифікований нашою державою, відбувається оперативне реагування на вказівки Ради Європи щодо еволюції вітчизняного законодавства в усіх сферах. Тож єдиним вірним напрямом щодо реалізації даного вектору запозичення досвіду є подальше втілення у вітчизняне законодавство європейських стандартів та імплементація європейських програм розвитку даного інституту у вітчизняні стратегії. Іншими словами, євроінтеграція України можлива лише за умови відповідності норм вітчизняного законодавства європейським стандартам. Втілення даного напряму є можливим в першу чергу шляхом ратифікації чи запозичення досвіду. В будь-якому випадку, вимоги ЄС мають виконуватись вітчизняним законодавцем, тому звернення до європейського законодавства є беззаперечною необхідністю.

2) поширення діяльності європейських міжнародних організацій по боротьбі із кіберзлочинністю на українську територію.

Пріоритетним напрямом реалізації даного вектору є продовження співпраці з Європейським Союзом і подальше входження до даної організації. Проте, такий шлях є ретроспективним і не в повній мірі залежить від України. Тому, на даному етапі більш важливим є укладення міжнародних двосторонніх чи багатосторонніх угод щодо співпраці із такими організаціями, як Комп'ютерна групи швидкого реагування (CERT – Computer Emergency Response Team), Європейський центр по боротьбі з кіберзлочинністю (European Cybercrime Centre) та Європейська агенція з

питань мережевої та інформаційної безпеки (European Network and Information Security Agency - ENISA), обміном інформацією та правовою допомогою, відомостями оперативно-розшукового характеру, прийняттям працівників правоохоронних органів іноземних держав в Україні тощо. Оскільки негайне входження до європейського співтовариства наразі є неможливим, доцільною є поступове підвищення участі та ролі нашої держави у міжнародних процесах по боротьбі із кіберзлочинністю.

3) запропоновано конкретизувати поняття «кіберзлочинності» ц вітчизняному законодавстві за допомогою норм європейського законодавства. Приймаючи Закон України «Про боротьбу із кіберзлочинністю», покликаного систематизувати усі ключові поняття досліджуваного інституту, варто здійснити роз’яснення того, які ж саме групи злочинів віднесено до категорії кіберзлочинів. Тож пропонується регламентувати норму в наступному вигляді – «Стаття 1. Визначення основних термінів. … традиційні форми кіберзлочинності - здійснювані у світовому чи регіональному масштабі кіберзлочинцями, суспільно небезпечні діяння, пов'язані з шахрайством та підробкою в електронних комунікаційних мережах та інформаційних системах; публікація протизаконного контенту в електронних медіа – здійснювані у кіберпросторі суспільно небезпечні діяння, пов'язані з поширенням дитячої порнографії, матеріалів із закликами до расової ненависті і т.п.; специфічні злочини в електронних мережах - здійснювані у світовому чи регіональному масштабі кіберзлочинцями чи їх угрупованнями, у тому числі за підтримки державних органів окремих держав, суспільно небезпечні діяння, пов'язані з атаками на інформаційні системи, хакерство тощо.

Отже, у контексті курсу України до євроінтеграції, дослідження особливостей правового регулювання боротьби із кіберзлочинністю у Європейському Союзі засвідчило необхідність постійної співпраці нашої держави з іншими країнами. Фундаментальне значення у протидії кіберзлочинам в європейських державах має єдність та взаємодія, що

відображається у залученні кращих фахівців кожної з країн-учасників до глобальних процесів. Тому, з метою участі, сприяння та обміну досвідом і знаннями для України є доцільним якнайшвидше залучення до таких процесів.

Окрім дослідження досвіду усієї європейської спільноти, доцільним є звернення до аналізу практики провідних держав Союзу. Розпочнемо із аналізу правового регулювання боротьби із кіберзлочинністю у Франції, оскільки дана держава одна із перших у Європі здійснила кроки до посилення ролі держави у регулюванні кіберпростору. Так, на сьогодні у даній державі виділено наступні форми кіберзлочинності: 1) суспільно небезпечні діяння, пов'язані з незаконним тиражуванням комп'ютерного програмного забезпечення, незаконним втручанням до автоматизованих систем обробки даних, вторгненням на сайти, створенням та розповсюдженням шкідливих програм тощо; 2) розповсюдження сайтів, пов'язаних з дитячою порнографією, збутом наркотиків, расистською, ксенофобною або антисемітською спрямованістю, терористичною спрямованістю, про замахи на приватне життя, з інструкціями по експлуатації вибухових речовин, реклами в шахрайських цілях тощо [161, с. 241]. Даний досвід є актуальним для втілення в України з огляду на недосконаліть розуміння та формулювання сутності поняття «кіберзлочинність» у нашій державі. Окрім того, важливим є чіткий розподіл проступків за мірою впливу на суспільні процеси у державі та негативними наслідками. Якщо регулювання першої форми кіберзлочинності за Французькою класифікацією здійснюється в Україні на достатньому рівні Розділом XVI Кримінального кодексу України [3], то досвід регулювання другої форми кіберзлочинів є доцільним для детального аналізу.

Вже сьогодні у Франції діють спеціальні закони, які забороняють публікацію матеріалів, які містять нацистську символіку чи підтримують ідеї нацизму [157, с. 88]. Дане питання є актуальним для Франції в силу багато національності даної держави, проте останнім часом в силу інформаційної

війни, спрямованої проти України, актуалізувалось і у наших умовах. Схожий нормативно-правовий акт було прийнято і в України, проте на 15 років пізніше. Так, 09.04.2015 року датовано прийняття Закону України «Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки» № 317-VIII [162]. Проте, відзначимо, що в нашій державі норми даного Закону не місять прямих вказівок на віднесення такої негативної діяльності до кіберзлочинів, обмежуючись формулюванням «поширення інформації», чого є недостатньо для формування розуміння пропаганди такої символіки у мережі Інтернет як кіберзлочину.

Також привертає увагу французький Закон про обов'язкову реєстрацію власників сайтів країни та про кримінальну відповідальність провайдерів за надання хостингу неідентифікованим користувачам. Ще одним цікавим моментом даного нормативно-правового акту є встановлення вимоги до провайдерів щодо надання відомостей про авторів сайтів будь-яким третім особам, за порушення якої передбачено кримінальну відповідальність. Також даний вид відповідальності передбачено за надання неповних чи недостовірних відомостей авторами французьких сайтів та за надання провайдерами місця на сервері неідентифікованим користувачам. При чому, за усі сайти, авторство яких не встановлено, відповідальність несе провайдер, а можливою мірою покарання є позбавлення волі строком на півроку [146, с. 26]. Будь-яка державна діяльність по встановленню контролю за громадянами апріорі є негативною, тому такий напрям розвитку вітчизняного законодавства по боротьбі із кіберзлочинами не вважаємо першочерговим. Проте, ураховуючи останні тенденції розвитку вітчизняного законодавства, питання встановлення відповідальності за порушення правил авторизації у кібермережах рано чи пізно опиниться на порядку денному вітчизняного законодавця. За таких умов доцільним буде аналіз досвіду більш розвинених держав і законодавство Франції є одним із першочергових для вивчення даному контексті.

У сфері активної боротьби із кіберзлочинністю 14 лютого 2008 року було прийнято французьку Стратегію з питань боротьби із кіберзлочинністю, метою якої є співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з обміну інформацією та питаннях щодо об'єднання зусиль у боротьбі з кіберзлочинністю. Цікавими моментами Стратегії є курс на встановлення співробітництва провайдерів і поліції й жандармерії, та створення національної комісії з професійної етики по зв'язках із громадськістю [161, с. 242]. Особливо доцільним вбачаємо останній напрям. Будь-яке обмеження прав і свобод громадян потребує належного роз'яснення та двостороннього конструктивного діалогу із громадянами. Для цього у Франції окрім намірів створити спеціальну комісію вчиняються й інші дії. Відмітимо відкриття сайту Хартії Інтернету (Charte de'Internet), на якому визначено принципи добровільних обов'язків користувачів та надавачів Інтернет-послуг. Ще одним подібним напрямом є створення Інтернет-ресурсу Mineurs.org, на якому викладена інформація про проекти у галузі безпечного користування кібермережами. Користувачі можуть отримувати консультації про протистояння кіберзагрозам та потенційно загрозливого змісту мережі [146, с. 26]. Такий досвід є безумовно позитивним, адже ознайомлюючись із правилами користування Інтернетом, суб'єкти суспільних відносин у даній сфері фактично надають згоду на дотримання цих правил. Окрім того, важливими є роз'яснення, що надаються з боку держави щодо обмеження прав громадян. Однією із проблем України у всіх сферах є фактична відсутність громадського діалогу із державною владою. Усі ключові рішення приймаються без урахування суспільної думки та належного подальшого роз'яснення прийнятих норм. Тож у даному контексті звернення до досвіду Франції було б доцільним.

Щодо напряму співробітництва із іншими державами, особливо відзначимо положення Закону про внутрішню безпеку 2003 року, який дозволяє проводити обшуки в інформаційній мережі, якщо інформаційні

системи розташовуються на території держави. Тобто, шляхом укладення міжнародних угод у Франції передбачено можливість надання дозволу проводити віддалений обшук інформаційних ресурсів, без одержання попереднього дозволу країни, де розміщений сервер [161, с. 242]. У даній роботі до перспектив розвитку правового регулювання боротьби з кіберзлочинністю нами було віднесено потенційну необхідність скасування державних кордонів у питаннях боротьби із кіберзлочинністю. Для втілення даного напряму в Україні доцільним є вивчення досвіду Франції, оскільки можливість такої «вільної» співпраці чинним законодавством України не передбачено.

Отже, особливостями правового регулювання боротьби із кіберзлочинністю у Франції є: 1) суттєва роль держави у регулюванні суспільних відносин в Інтернеті; 2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів; 3) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз; 4) існування двостороннього діалогу із громадянами та належне роз'яснення їх прав і обов'язків як користувачів Інтернету, надання інструкцій; 5) встановлення курсу на вільне співробітництво із іншими державами шляхом надання доступу до власних кібермереж у разі вчинення на території Франції кібезлочинів.

Практично кожна із обраних характеристик була б доцільною для втілення в сучасних українських реаліях. Тому, аналіз правового регулювання боротьби із кіберзлочинністю в Франції дозволяє виділити наступні шляхи запозичення позитивного досвіду в Україну:

1) встановлення вимоги авторизації авторів веб-сайтів.

Використовуючи досвід Франції, по-перше, доцільним було б прийняття Закону України «Про обов'язкову реєстрацію власників сайтів». В такому нормативно-правовому акті варто передбачити наступні положення: - створити єдиний загальнодержавний реєстр власників сайтів; - встановити обов'язок провайдерів реєструвати відомості про авторів сайтів; - надати

такій інформації статусу публічної; - передбачити обов'язок надання Інтернет-провайдерів інформації про авторів сайтів при надходження таких запитів. По-друге, варто доповнити Розділ XVI Кримінального кодексу України [3] наступними статтями:

- «Порушення у сфері надання Інтернет-провайдерами хостингу не ідентифікованим користувачам. 1. Надання Інтернет-провайдерами хостингу не ідентифікованим користувачам, - карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 6 місяців. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до одного року»;

- «Порушення у сфері ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит. 1. Ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит, що надійшов, - карається штрафом до п'ятисот неоподатковуваних мінімумів доходів… 3. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли значну шкоду, - караються штрафом до тисячі неоподатковуваних мінімумів доходів або позбавленням волі на строк до одного року»;

- «Надання неповних чи недостовірних відомостей авторами французьких сайтів, або надання провайдерами місця на сервері неідентифікованим користувачам. 1. Надання неповних чи недостовірних відомостей авторами французьких сайтів, або надання провайдерами місця на сервері неідентифікованим користувачам, - карається штрафом від п'ятисот до тисячі неоподатковуваних мінімумів доходів громадян або позбавленням волі на строк до 6 місяців. 2. Дії, передбачені частиною першою цієї статті, вчинені повторно або за попередньою змовою, або якщо вони заподіяли значну шкоду, - караються позбавленням волі на строк до одного року».

2) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз.

Для реалізації даного напряму варто по-перше, у запропонованому Законі України «Про обов'язкову реєстрацію власників сайтів» передбачити норму, що зобов'язуватиме Інтернет-провайдерів максимально оперативно надавати правоохоронним органам відповіді на запити щодо авторів сайтів та підозрюваних у вчиненні кіберзлочинів. По-друге, у Розділі XVI Кримінального кодексу України [3] запропоновану статтю «Порушення у сфері ненадання Інтернет-провайдерами відомостей про авторів сайтів у відповідь на запит» доцільно доповнити частиною 2: «2. Ненадання Інтернет-провайдерами відомостей у відповідь на запит правоохоронних органів, - карається позбавленням волі на строк до шести місяців».

3) налагодження двостороннього діалогу із громадянами.

Використовуючи досвід Франції запропоновано створити спеціальні Інтернет-ресурси, обов'язковими умовами яких будуть: - роз'яснення користувачам Інтернету їх прав та обов'язків; - тлумачення новоприйнятих норм законодавства та причин обмеження прав та свобод громадян; - надання консультацій за отриманими запитами; - вчасно інформувати громадян про проекти, розробка яких здійснюється.

4) встановлення курсу на вільне співробітництво з іншими державами.

У разі вчинення на території України кіберзлочинів, наслідки яких були негативними для інших держав, запропоновано надавати без запиту доступу до власних кібермереж державам, із якими в Україні підписано двосторонні договори про співробітництво у сфері боротьби із кіберзлочинністю. Для цього, по-перше, потрібно укласти відповідні угоди або внести зміни до вже укладених. По-друге, доповнити статтю 8 Закону України «Про основи національної безпеки України» від 19.06.2003 № 964-IV [47] наступним чином «Основними напрямами державної політики з питань національної безпеки України є: у зовнішньополітичній сфері - проведення активної міжнародної політики України з метою: … поглиблення співпраці із зарубіжними держава у сфері боротьби із кіберзлочинністю … ; у сфері

державної безпеки: … участь України в міжнародному співробітництві у сфері боротьби з кіберзлочинністю».

Таким чином, Франція є вдалим прикладом країни для запозичення позитивного досвіду в Україну. По-перше, дана держава у порівнянні з іншими країнами Європейського Союзу характеризується жорсткішими підходами до встановлення контролю у кіберпросторі. Тому, у контексті нещодавніх змін до вітчизняного законодавства, є доцільним звернення до досвіду країн, у яких подібні обмеження прав і свобод громадян були успішно реалізовані. По-друге, Франція являється взірцем щодо встановлень двосторонніх відносин на рівнях «держава - держава», «держава - громадянин», «держава – приватний сектор економіки». Враховуючи загальну незадоволеність громадян України реформами, що відбуваються в нашій державі та недостатність гласності у діях суб'єктів державної влади, досвід Франції є безумовно корисним для втілення у наших реаліях.

Останньою групою країн, на досвід яких варто звернути увагу, є сусідні держави, у першу чергу колишні учасники Союзу Радянських Соціалістичних Республік. Двадцять шість років тому кожною із держав було обрано самостійний вектор розвитку. Тому, не зважаючи на етнічну та історичну близькість, вже сьогодні ми можемо спостерігати відмінності у правовому регулюванні різноманітних суспільних інститутів. Розглянемо досвід Республіки Білорусь, як однієї з перших держав колишнього СРСР, якої було утворено спеціальний орган для боротьби із кіберзлочинністю - управління по розкриттю злочинів у сфері високих технологій Міністерства внутрішніх справ Республіки Білорусь. 27 лютого 2001 року у структурі кримінальної міліції МВС з'явилося управління оперативно-організаційної роботи, у складі якого до листопада 2002 року активно діяло спеціалізоване відділення по розкриттю злочинів у сфері високих технологій, а вже 28 листопада 2002 року на підставі наказу Міністра внутрішніх справ, з метою вдосконалення організації роботи названих підрозділів, в МВС було створено самостійне управління, що здійснює практичну діяльність по розкриттю

злочинів у сфері високих технологій [163]. Даний орган має статус самостійного оперативно-розшукового підрозділу Міністерства, яке здійснює координацію підрозділів головного управління кримінальної міліції МВС і органів внутрішніх справ при виявленні ними злочинів проти інформаційної безпеки Для здійснення взаємодії з іншими правоохоронними органами і організаціями застосовується умовне найменування Управління «К» МВС Республіки Білорусь [164, с. 42]. Даний орган складається з трьох відділів: 1) з розкриття злочинів проти інформаційної безпеки, який відповідає за розкриття і профілактику злочинів проти інформаційної безпеки; 2) з розкриття злочинів у сфері телекомунікацій; 3) комп'ютерно-технічного забезпечення - підтримує роботу комп'ютерної техніки. Оскільки вітчизняний Департамент кіберполіції Національної поліції України перебуває ще на початковому етапі свого розвитку, доцільним було б звернути увагу на структурування таких органів у сусідніх державах. Окрім того, на сьогодні завданнями вітчизняної кіберполіції визначено: 1) Участь у формуванні та забезпеченні реалізації державної політики щодо попередження та протидії кримінальним правопорушенням із використання комп'ютерів, систем та комп'ютерних мереж і мереж електрозв'язку; 2) Сприяння іншим підрозділам Національної поліції у попередженні, виявленні та припиненні кримінальних правопорушень [165]. Таких напрямків є об'єктивно недостатньо, тому досвід Білорусі може бути використано у даному контексті [166]. По-перше, судячи по зазначених формулюваннях, на сьогодні вітчизняний кіберпідрозділ поліції виконує швидше консультаційні функції, аніж правоохоронні [167, с. 22]. У процесі такої взаємодії може втрачатись час, якого при розслідуванні кіберзлочинів переважно небагато [168, с. 245]. Тому доцільним було б наділення Департаменту кіберполіції Національної поліції України функцією розкриття комп'ютерних злочинів. По-друге, важливим було б здійснення таким органом безпосередньої діяльності щодо комп'ютерно-технічного забезпечення діяльності органів державної влади.

Аналізуючи законодавчу базу боротьби із кіберзлочинності в Білорусі, вона представлена незначною кількістю норм та законів: Глава Кримінального кодексу Республіки Білорусь, Закон про електрозв'язок, Закон про інформацію, інформатизації і захист інформації, Конвенція про кіберзлочини, Додатковий протокол до Конвенції про кіберзлочини, Указ «Про заходи щодо вдосконалення використання національного сегменту мережі Інтернет», Указ «Про деякі питання розвитку інформаційного суспільства в Республіці Білорусь», Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність» [163, 169, 170]. У цілому відзначаємо тотожність законодавчої бази Республіки Білорусь та України, проте звернемо особливу увагу на Указ «Про затвердження Положення про порядок взаємодії операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність». Як і у випадку з дослідженням досвіду Франції, відзначаємо важливість налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз. Для посилення даної норми, пропонуємо на приклади Білоруси здійснити її підзаконну регламентацію.

Отже, основними характеристиками правового регулювання боротьби із кіберзлочинністю у Республіці Білорусь є: 1) наявність спеціального органу із значним досвідом протистояння кіберзлочинності; 2) перелік повноважень даного органу є значно ширшим, ніж у Департаменту кіберполіції Національної поліції України; 3) невелика кількість нормативно-правових актів у сфері правового регулювання боротьби із кіберзлочинністю; 4) встановлення співпраці операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність.

Шляхи запозичення позитивного досвіду Республіки Білорусь в Україну ми вбачаємо у наступних напрямах:

1) розширення структури Департаменту кіберполіції Національної поліції України.

В даному напрямку доцільним було б прийняття Закону України «Про кіберполіцію», яким належним чином регламентувати діяльність даного органу, його структуру, напрями діяльності кожного із структурних елементів. Крім того, доцільно розширити сферу діяльності кіберполіції на підтримання роботи комп'ютерної техніки у органах державної влади.

Запропоновано наділити Департамент кіберполіції Національної поліції України функціями розкриття комп'ютерних злочинів та комп'ютерно-технічного забезпечення діяльності органів державної влади.

2) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз.

Виконання даного напряму вбачаємо у прийнятті Положення про порядок взаємодії операторів електрозв'язку з правоохоронними органами, та за проаналізованим прикладом Франції встановити відповідальність за порушення у процесі такої взаємодії. Тобто, необхідним Законом України «Про обов'язкову реєстрацію власників сайтів» зобов'язати Інтернет-провайдерів надавати правоохоронним органам необхідну інформацію щодо запитів та передбачити відповідальність за її ненадання.

Таким чином, дослідження досвіду країн-колишніх учасників Союзу Радянських Соціалістичних Республік на прикладі Республіки Білорусь засвідчило, що у цілому при виборі моделей для перейняття досвіду більш доцільним є звернення уваги на концепції більш розвинених європейських держав чи Сполучених Штатів Америки. Не зважаючи на самостійний вибір шляхів розвитку, законодавство наших держав все ще є наближеним, а численні норми є похідними від радянського законодавства. Тож, робимо висновок, що використання досвіду Республіки Білорусь не вплине значним чином на вітчизняну систему правового регулювання боротьби з кіберзлочинністю, проте окремі елементи є все ж доступними для запозичення.

Підсумовуючи здійснене дослідження, варто зробити висновок, що втілення зарубіжного досвіду у будь-якому разі є тривалим та важким

процесом, який не завжди призводить до позитивних наслідків. Аналізуючи моделі правового регулювання боротьби із кіберзлочинністю, нами встановлено тенденцію до спроб встановлення контролю за Всесвітньою мережею, проте наявні заборони все ж не містять ознак суттєвого порушення прав та свобод людини і громадянина. У досліджуваних державах існує двосторонній діалог влади та громадян, завдяки якому у суспільстві формується вірне розуміння необхідності встановлення обмежень, заборон чи регламентів. В той же час, ми звернули увагу на незначну кількість нормативно-правових актів, які при цьому належним чином врегульовують даний інститут, тобто в них переважає саморегулювання сфери кібербезпеки. Також доцільно відзначити роль міжнародного законодавства та міждержавних угод, які значним чином мають вплив на суспільні відносини всередині держав. Очевидно, що їх роль у вітчизняному праві необхідно виводити на новий рівень.

Розглядаючи досвід держав колишнього Радянського Союзу, в тому числі і України, необхідно відзначити відмінність у формах контролю за кіберпростором. Контроль має більш декларативний характер і негативнішим чином впливає на права та свободи громадян. Проте, варто враховувати відносну молодість усіх інститутів, пов’язаних із кіберпростором, тому зробимо висновок про перебування таких держав на проміжному етапі розвитку правового регулювання боротьби із кіберзлочинністю.

Висновки до Розділу 3

1. Виділено три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні:

1) тенденція розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні;

2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні;

3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

2. Деталізовано перелік основних тенденцій розвитку правового регулювання боротьби з кіберзлочинністю в Україні підтенденціями, які розкривають їх зміст.

У рамках тенденції розвитку вітчизняної нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні запропоновано виділено наступні підтенденції: 1) розширення меж розуміння поняття кіберзлочинність; 2) посилення кримінальної відповідальності за вчинення кіберзлочинів; 3) термінологічне узгодження у нормах усіх нормативно-правових актах, що регламентують дане питання, єдиного термінологічного апарату.

3. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки є такі: 1) США вважають себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) дана держава має значний вплив на прийняття відповідного законодавства у країнах Європейського Союзу; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам.

4. Правове регулювання боротьби із кіберзлочинністю у Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинами здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

5. Особливостями правового регулювання боротьби із кіберзлочинністю у Франції є: 1) суттєва роль держави у регулюванні суспільних відносин в Інтернеті; 2) контроль за користувачами шляхом встановлення вимоги до авторизації авторів веб-сайтів; 3) налагодження співробітництва правоохоронних органів та Інтернет-провайдерів з метою оперативного реагування на виникнення загроз; 4) існування двостороннього діалогу із громадянами та належне роз'яснення їх прав і обов'язків як користувачів Інтернету, надання інструкцій; 5) встановлення курсу на вільне співробітництво із іншими державами шляхом надання доступу до власних кібермереж у разі вчинення на території Франції кібезлочинів.

6. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Республіці Білорусь є: 1) наявність спеціального органу із значним досвідом протистояння кіберзлочинності; 2) перелік повноважень даного органу є значно ширшим, ніж у Департаменту кіберполіції Національної поліції України; 3) невелика кількість нормативно-правових актів у сфері правового регулювання боротьби із кіберзлочинністю; 4) встановлення співпраці операторів електрозв'язку з органами, які проводять оперативно-розшукову діяльність.

ВИСНОВКИ

У дисертації наведено теоретичне узагальнення та нове вирішення наукового завдання, що полягає у визначенні теоретико-правових засад правового регулювання боротьби із кіберзлочинністю. Основними науковими та практичними результатами роботи є такі висновки й пропозиції:

1. Кіберзлочинами є найбільш небезпечні кіберправопорушення, вчинення яких на різних стадіях безпосередньо пов'язане із використанням комп'ютерної техніки через комп'ютерні системи, або із комп'ютерними системами, та за які чинним законодавством передбачено кримінальну відповідальність.

Систему ознак боротьби із кіберзлочинністю визначено дворівнево. До загальних, тобто характерних явищу боротьби із злочинністю загалом, віднесено такі: 1) активність; 2) цілеспрямованість; 3) збірність; 4) комплексність.

У якості спеціальних, а саме характерних виключно боротьбі із кіберзлочинністю, у процесі аналізу правової доктрини виділено: 1) ознака можливості зустрічної атаки зі сторони кіберзлочинців; 2) ознака здійснення виключно компетентними суб'єктами, володіючими спеціальними знаннями та необхідними ресурсами; 3) ознака міждержавності; 4) ознака згуртування держав.

2. У рамках генезису правового регулювання боротьби з кіберзлочинністю в Україні виділено наступні етапи: 1) початковий етап (1991 рік – 2000 рік) – не зважаючи на те, що у даний період було прийнято декілька нормативно-правових актів, спрямованих на врегулювання проблем кібербезпеки, питанню захисту від кіберзлочинів законодавцем увага не приділялась у належному обсязі, проте у 2000 році почали бути помітними тенденції до розвитку законодавства про кіберзлочини; 2) етап прийняття вітчизняного законодавства про боротьбу із кіберзлочинністю (2001 рік –

2005 рік) – його початок пов’язується із прийняттям Кримінального кодексу України, у нормах якого незаконна діяльність у кіберпросторі була вперше визнана злочином на рівні вітчизняного законодавства, а за кіберзлочини було встановлено конкретні санкції. Відповідно, закінчення етапу автор відносить до введення у правовий обіг понять «комп’ютерна злочинність» та «комп’ютерний тероризм»; 3) етап відповідності правового регулювання боротьби з кіберзлочинністю існуючим загрозам (2005 рік – до 27.06.2017 року) – не зважаючи на те, що на даному етапі зроблено небагато, курс України до євроінтеграції вимагає імплементації європейських правових норм у вітчизняне законодавство. Існуючі кіберзагрози були врегульовані належним чином. У цілому, зазначений період характеризується відсутністю вагомих подій у сфері боротьби із кіберзлочинністю; 4) новітній етап (від 27.06.2017 року) – вірус «Petya.A» продемонстрував неготовність України до боротьби із сучасними кіберзагрозами. Тому, щойно розпочатий етап автор пов’язує із подальшою розробкою інструментів для боротьби із кібертерроризмом.

3. Механізм правового регулювання боротьби з кіберзлочинністю – це чітко визначена й організована система юридичного інструментарію, яка забезпечує правовий вплив шляхом застосування нормативних приписів на суспільні відносини, які виникають, змінюються та припиняються у сфері протидії вчиненню інформаційних злочинів, що дозволяє впливати на бажану поведінку учасників таких відносин, з метою досягнення належної й ефективної боротьби з кіберзлочинністю.

4. Особливостями універсального міжнародно-правового регулювання боротьби з кіберзлочинністю є наступні: 1) відповідна діяльність акумулюється навколо ООН та її органів або створених за її підтримки суб’єктів; 2) на сьогодні наявні виключно програмні та інші стратегічні документи, які повинні закласти основи міжнародно-правового регулювання відповідного кола відносин; 3) основними напрямами діяльності має бути створення й розробка організаційних та законодавчих заходів протидії

кіберзлочинності, а також питання взаємодії у даній сфері діяльності; 4) наявна необхідність у створенні міжнародних спільних органів оперативно-розшукової діяльності для забезпечення фіксування слідів вчинених злочинів; 5) удосконалення взаємодії між компетентними органами різних держав; 6) існує нагальна потреба розробки й прийняття універсальних конвенцій з відповідних питань, які би забезпечили участь більшості держав у відповідних заходах проти кіберзлочинності.

Особливостями регіонального міжнародно-правового регулювання протидії кіберзлочинності є такі: 1) значна увага з боку різноманітних регіональних міжнародних організацій до питань протидії кіберзлочинам; 2) розробка численних регіональних угод про співробітництво у сфері протидії інформаційним злочинам; 3) відповідна діяльність перебуває на етапі свого зародження, оскільки більшість документів почали формуватися наприкінці 1990-х рр. – на початку 2000-х рр.; 4) така діяльність є складовою частиною як міжнародних інформаційних відносин, так і кримінального судочинства.

5. Особливостями нормативно-правової бази національного правового регулювання боротьби з кіберзлочинністю є наступні: 1) наявність системи національного правового регулювання боротьби з кіберзлочинністю, проте недостатній рівень єдності її елементів, що полягає у відмінностях в термінології, наявності розбіжностей у формулюваннях, прогалин та інших проблем; 2) комбінування у правовій системі норм вітчизняного законодавства та міжнародних правових актів, ратифікованих нашою державою; 3) наявність міжнародних договорів щодо двосторонньої співпраці у сфері правового регулювання боротьби з кіберзлочинністю; 4) існування Стратегії кібербезпеки України, що визначає подальший розвиток національного правового регулювання боротьби із кіберзлочинністю.

6. Виділено три основних тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні: 1) тенденція розвитку вітчизняної

нормативно-правової та термінологічної бази у сфері боротьби з кіберзлочинністю в Україні; 2) тенденція посилення міжнародного співробітництва у сфері боротьби з кіберзлочинністю в Україні; 3) тенденція збільшення рівня контролю за користувачами мережі Інтернет.

7. Основними характеристиками правового регулювання боротьби із кіберзлочинністю у Сполучених Штатах Америки є такі: 1) США вважають себе однією із держав, що несе відповідальність перед усім світом за регламентацію відносин у кібермережах; 2) дана держава має значний вплив на прийняття відповідного законодавства у країнах Європейського Союзу; 3) значна увага приділяється захисту інформації та протидії неправомірному доступу до неї; 4) у США діє розгалужена система органів протидії кіберзлочинам.

Правове регулювання боротьби із кіберзлочинністю у Європейському Союзі характеризується наступними ознаками: 1) наявність як національного, так і міжнародного законодавства про боротьбу із кіберзлочинністю; 2) діяльність по протидії кіберзлочинам здійснюється одночасно національними та міжнародними організаціями, сформованими із кращих спеціалістів країн-учасників; 3) важлива роль відводиться теоретичним питанням, таким як експертне оцінювання кіберзлочинів, розробка передових методів профілактики і розслідування тощо; 4) здійснення активного інформаційного обміну.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конвенція про кіберзлочинність: Міжнародний документ від 23.11.2001. Офіційний вісник України. 2007 р. № 65. стор. 107. стаття 2535. код акту 40846/2007.
2. Біленчук Д.П. Кібрешахраї – хто вони? Міліція України. 1999. № 7-8. С. 32-34.
3. Кримінальний кодекс України. Закон України від 05.04.2001 № 2341-III. Відомості Верховної Ради України (ВВР). 2001. № 25-26. ст.131.
4. Литвак О. М. Злочинність, її причини та профілактика. К. : Україна, 1997. 168 с
5. Іванченко О. Ю. Кримінологічна характеристика кіберзлочинності, запобігання кіберзлочинності на національному рівні. Актуальні проблеми вітчизняної юриспруденції. 2016. Вип. 3. С. 172-177.
6. Конституція України: Закон України від 28.06.1996 № 254к/96-ВР. Відомості Верховної Ради України. 1996. № 30. ст. 141.
7. Кримінальний процесуальний кодекс України. Закон України від 13.04.2012 № 4651-VI. Відомості Верховної Ради України (ВВР). 2013. № 9-10. № 11-12. № 13. ст.88.
8. Про ратифікацію Конвенції про кіберзлочинність: Закон України від 07.09.2005 № 2824-IV. Відомості Верховної Ради України (ВВР). 2006. № 5-6. ст.71.
9. Положення про Департамент кіберполіції Національної поліції України. Наказ Національної поліції України від 10.11.2015 № 85. URL https://www.npu.gov.ua/uk/publish/printable_article/1816252 (дата звернення: 12.10.2016)
10. Закалюк А. П. Курс сучасної української кримінології : в 3 кн. Кн. 1. Теоретичні засади та історія української кримінологічної науки. К. : Видав. дім «Ін Юре», 2007. 423 с

11. Великий тлумачний словник сучасної української мови : словник / Уклад. і голов. ред. В. Т. Бусел. К.; Ірпінь : ВТФ «Перун», 2002. 1440 с.
12. Бандурка О. М. Протидія злочинності та профілактика злочинів : моногр. Х. : ХНУВС, 2011. 308 с.
13. Погорецький М. Взаємовідносини держави, суспільства і злочинності: боротьба чи протидія? Вісник прокуратури. 2010. № 9 (111). С. 36–42.
14. Юридична енциклопедія : в 6 т. / НАНУ, Ін-т держави і права ім. В.М. Корецького НАН України ; [ред. Ю.С. Шемшученко та ін.]. Київ : Українська енциклопедія ім. М.П. Бажана. Т. 1 : А - Г. 1998. 672 с
15. Карпец И. И. Проблемы преступности. М. : Юрид. лит., 1969. 167 с.
16. Аванесов Г. А. Криминология : [учебник]. [2-е из- д., перераб. и доп. – М. : Акад. МВД СССР, 1984. 500 с.
17. Долгова А. И. Криминология [Текст] : Учебник для вузов. М. : Норма : Инфра-М, 1999. 272 с.
18. Орлов О. В., Онищенко Ю. М. Актуальні напрями державної політики України у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління. Вип. 3 (42). С. 1-6
19. Юридична енциклопедія : в 6 т. / НАНУ, Ін-т держави і права ім. В.М. Корецького НАН України ; [ред. Ю.С. Шемшученко та ін.]. Київ : Українська енциклопедія ім. М.П. Бажана. Т. 2 : Д-Й. 1999. 744 с.
20. Юридична енциклопедія : в 6 т. / НАНУ, Ін-т держави і права ім. В.М. Корецького НАН України ; [ред. Ю.С. Шемшученко та ін.]. Київ : Українська енциклопедія ім. М.П. Бажана. Т. 3 : К-М. 2001. 792 с.
21. Чернєй В. В. Роль відомчої освіти та науки в забезпеченні протидії кіберзлочинності в Україні. Науковий вісник Національної академії внутрішніх справ. 2014. № 3. С. 3-15.
22. В.М. Болгов, Н.М. Гадіон, О.З. Гладун. Організаційно-правове забезпечення протидії кримінальним правопорушенням, що вчиняються з використанням інформаційних технологій: наук.-практ. посіб. К.: Національна академія прокуратури України, 2015. 202 с.

23. Словник термінів з кібербезпеки. за заг. ред. О. Копатіна, Є. Скулишина. К.: Аванпост-Прим, 2012. 214 с.
24. Погорецький М. Кіберзлочини: до визначення поняття. Вісник прокуратури. 2012. № 8. С. 89–96.
25. Бурячок В. Л. Інформаційна та кібербезпека: соціотехнічний аспект: підручник. за заг. ред. д-ра техн. наук, професора В. Б. Толубка. К.: ДУТ, 2015. 288 с.
26. Перелік кібератак. Вікіпедія – вільна енциклопедія. URL : https://uk.wikipedia.org/wiki/Перелік_кібератак (дата звернення: 12.11.2016)
27. Заворуєв Р.С., Резніченко В.А. Протидія кіберзлочинності в Україні. Матеріали Всеукраїнської науково-практичної конференції 23-25 листопада 2016 р. м. Кропивницький. С. 49-50
28. Войціховський А. В. Міжнародне співробітництво в боротьбі з кіберзлочинністю. Право і Безпека. 2011. № 4. С. 107-112.
29. Дзюндзюк В. Б. Поява і розвиток кіберзлочинності. Державне будівництво. 2013. № 1. URL http://nbuv.gov.ua/UJRN/DeBu_2013_1_3 (дата звернення: 13.11.2016)
30. A Brief History of Computer Crime: An Introduction for Students. M. E. Kabay, PhD, CISSP-ISSMP Program Director, MSIA School of Graduate Studies Norwich University. URL http://www.mekabay.com/overviews/history.pdf (дата звернення: 22.11.2016)
31. Європіна І. В. Види протиправних діянь у сфері новітніх інформаційних технологій. Вісник Академії адвокатури України. 2010. Число 3. С. 129-136.
32. Пушкаренко, П. І. Кіберзлочинність як новітній феномен тіньової економіки [Текст]. Проблеми і перспективи розвитку банківської системи України : зб. наук. праць / Державний вищий навчальний заклад «Українська академія банківської справи Національного банку України». Суми, 2006. Т. 17. С. 75-82.

33. Літвінов М.Ю. Світова та українська практика боротьби з кіберзлочинністю. Право і безпека : науковий журнал. Харк. нац. ун-т внутрішніх справ. Харків, 2014. № 1 (52). С. 85-89.

34. Jarrett, H. Marshall; Bailie, Michael W. (2010). Office of Legal Education Executive Office for United States Attorneys. Retrieved June 3, 2013. 213 p. URL https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ccmanual.pdf (дата звернення: 07.12.2016)

35. Гринчак І.В. Кіберзлочинність як злочин міжнародного характеру. Науково-інформаційний вісник Івано-Франківського університету права імені Короля Данила Галицького : право, економіка / Івано-Франківський університет права імені Короля Данила Галицького. Івано-Франківськ, 2015. Вип. 12. С. 93-98.

36. Голубєв В.О. Інформаційна безпека: проблеми боротьби з кіберзлочинами : Монографія. Гуманітарний ун-т "Запорізький ін-т державного та муніципального управління". Запоріжжя : ЗІДМУ, 2003. 250 с.

37. Міщук Н. Кіберзлочинність як загроза інформаційному суспільству // Вісник Львівського університету : збірник наукових праць / Львівський національний університет ім. Івана Франка. – Львів, 2014. – (Серія економічна ; вип. 51). – С. 173-179.

38. Манжай О. В. Проблеми нормативно-правового забезпечення боротьби з кіберзлочинністю в Україні. Форум права. 2013. № 1. С. 646-650.

39. Computer-related crime. Recommendation no. R. (89) 9 on computer-related crime and final report of the European Committee on Crime Problems / Strasbourg. Council of Europe, Pub. and Documentation Service. Croton, N.Y. : Manhattan Pub. Co. [distributor], 1990. 114 p.

40. Конвенція Організації Об'єднаних Націй проти транснаціональної організованої злочинності. Міжнародний документ від 15.11.2000. Офіційний вісник України. 2006 р. № 14. стор. 340. стаття 1056. код акту 35837/2006.

41. Віденська декларація про злочинність та правосуддя: відповіді на виклики XXI століття. Міжнародний документ від 17.04.2000 року. URL http://zakon5.rada.gov.ua/laws/show/995_443 (дата звернення: 10.12.2016)
42. Конвенція про взаємодопомогу в кримінальних справах між державами-членами Європейського Союзу. Міжнародний документ від 29.05.2000 URL http://zakon3.rada.gov.ua/laws/show/994_238?test=Up9Mf3o6frtCt4d2ZiIViVNwHI4Uks80msh8Ie6 (дата звернення: 19.12.2016)
43. Додатковий протокол до Конвенції про кіберзлочинність, який стосується криміналізації дій расистського та ксенофобного характеру, вчинених через комп'ютерні системи. Міжнародний документ від 28.01.2003. Офіційний вісник України 2010 р. № 56, / № 31. 2006. ст. 2202 /. стор. 73. стаття 1920. код акту 52082/2010
44. Угода про співробітництво держав-учасниць Співдружності Незалежних Держав в боротьбі зі злочинами у сфері комп'ютерної інформації. Міжнародний документ від 01.06.2001. URL http://zakon4.rada.gov.ua/laws/show/997_353 (дата звернення: 25.12.2016)
45. Комп’ютерна злочинність. Навчальний посібник. Київ: Атіка, 2002. 232 с.
46. Про інформацію. Закон України від 02.10.1992 № 2657-XII. Відомості Верховної Ради України (ВВР). 1992. № 48. ст.650.
47. Про захист інформації в інформаційно-телекомунікаційних системах. Закон України від 05.07.1994 № 80/94-ВР. Відомості Верховної Ради України (ВВР). 1994. № 31. ст.286.
48. Про державну таємницю. Закон України від 21.01.1994 № 3855-XII. Відомості Верховної Ради України (ВВР). 1994. № 16. ст.93.
49. Про основи національної безпеки України. Закон України від 19.06.2003 № 964-IV. Відомості Верховної Ради України (ВВР). 2003. № 39. ст.351.
50. Програма інтеграції України до Європейського Союзу. Програма від 14.09.2000 URL http://zakon4.rada.gov.ua/laws/show/n0001100-00 (дата звернення: 12.01.2017)

51. Про заходи щодо зміцнення банківської системи України та підвищення її ролі у процесах економічних перетворень. Указ Президента України від 14.07.2000 № 891/2000. Урядовий кур'єр від 22.07.2000. URL zakon.rada.gov.ua (дата звернення: 17.01.2017)
52. Про заходи щодо розвитку національної складової глобальної інформаційної мережі Інтернет та забезпечення широкого доступу до цієї мережі в Україні // Урядовий кур'єр від 08.08.2000. URL zakon.rada.gov.ua (дата звернення: 23.01.2017)
53. Про деякі заходи щодо захисту державних інформаційних ресурсів у мережах передачі даних. Указ Президента України від 24.09.2001 № 891/2001 // Урядовий кур'єр від 03.10.2001. № 179. URL zakon.rada.gov.ua (дата звернення: 01.02.2017)
54. Вирус Petya.A: киберполиция изъяла сервера M.E.Doc. URL http://news.liga.net/news/politics/14781131-virus_petya_a_kiberpolitsiya_izyala_servera_m_e_doc.htm (дата звернення: 04.02.2017)
55. Вирок Стрийського міськрайонного суда Львівської області від 21 січня 2016 року по справі № 456/4615/15-к. URL Режим доступу: http://www.reyestr.court.gov.ua/Review/55146476 URL (дата звернення: 07.02.2017)
56. Вирок Першотравневого районного суда м. Чернівців від 22.05.2017 року по справі № 725/85/17. URL http://www.reyestr.court.gov.ua/Review/66614097 (дата звернення: 10.02.2017)
57. Вирок Ленінського райсуда м. Кіровограда від 24 лютого 2015 року по справі № 405/1660/14-к. URL http://www.reyestr.court.gov.ua/Review/42833218 (дата звернення: 19.01.2017)
58. Александров Н.Г. Право и законность в период развернутого строительства коммунизма. М.: Юридическая лит-ра. 1961. 271 с.
59. Алексеев С.С. Механизм правового регулирования в социалистическом государстве. М.: Юридическая лит-ра. 1966. 187 с.

60. Алексеев С.С. Право: азбука – теория – философия: Опыт комплексного исследования. М.: «Статут». 1999. 712 с.

61. Матузов Н.И., Малько А.В. Теория государства и права. Курс лекций. – М.: Юристъ. 1997. 672 с.

62. Загальна теорія держави і права: навчальний посібник. За ред. В.В. Копейчикова. К.: Юрінком. 1997. 320 с.

63. Хропанюк В.Н. Теория государства и права. Под ред. В.Г. Стрекозова. М.: Юрист. 2000. 366 с.

64. Скакун О.Ф. Теорія держави та права: підручник. перек. з рос. Харків: Консул. 2001. 656 с.

65. Нерсесянц В.С. Общая теория права и государства: учебник для юридических вузов и факультетов. М.: Норма-Инфра. 1999. 552 с.

66. Кривицький Ю.В. Спеціалізовані норми права в механізмі правового регулювання: дис. … канд. юрид. наук: спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень. К. 2010. 260 с.

67. Кархут О.Я. Механізм правового регулювання суспільних відносин у сфері освіти: теоретико-правовий аспект: автореф. дис. … канд. юрид. наук: спец. 12.00.01 «Теорія та історія держави і права; історія політичних і правових учень». К. 2014. 21 с.

68. Зусь Л.Б. Правовое регулирование в сфере уголовного судопроизводства. Владивосток: Из-во Дальневосточного у-та. 1984. 145 с.

69. Ступник Я.В. Поняття і структура механізму протидії наркозлочинності. Политика, государство и право. 2012. №2. URL http://politika.snauka.ru/2012/02/118 (дата звернення: 03.03.2017)

70. Якутова М.А. Механизм правового регулирования межбюджетных отношений: теория и практика. Законодательство и экономика. 2004. №8. С. 24-28.

71. О.В. Зайчук, Н.М. Оніщенко. Теорія держави і права. Академічний курс: підручник. К.: Юрінком Інтер. 2006. 685 с.

72. Козюбра М.І. Загальна теорія права : підручник. Київ : Ваіте, 2015. 391 с.

73. Куракін О.М. Структура механізму правового регулювання. Науковий вісник Ужгородського національного університету. Серія: Право. 2015. Вип. 35. Ч. 2. Т. 1. С. 41-44.

74. Колонтаевский Ф.Е. Курс административно-правового регулирования деятельности ОВД в системе управления знаний руководителей. Актуальные проблемы совершенствования организационных и правовых основ деятельности ОВД. Труды Академии управления (юбилейный выпуск). М. 1999. С. 15-20.

75. Коренев А.П. Нормы административного права и их применение. М.: Юрид. лит. 1978. 142 с.

76. Бобровник С.В. Загальна теорія держави і права (основні поняття, категорії, правові конструкції та наукові концепції): навч. посіб. К.: Юрінком Інтер. 2008. 400 с.

77. Мурашин О.Г. Акти прямого народовладдя у механізмі правового регулювання. Право України. 2000. №9. С. 18-20.

78. Бєляков Р.Г. Взаємодія управління боротьби з кіберзлочинністю МВС України з іншими правоохоронними органами: питання сьогодення. Право і безпека : науковий журнал. Харк. нац. ун-т внутрішніх справ. Харків, 2014. № 4 (55). С. 85-88.

79. Власова Г.П. Проблеми боротьби з кіберзлочинністю. Актуальні питання реформування правової системи України : зб. матеріалів XII Міжнар. наук.-практ. конф. (м. Луцьк, 26-27 черв. 2015 р.). Східноєвроп. нац. ун-т ім. Лесі Українки, Юрид. ф-т ; [уклад. Л.М. Джурак ; редкол.: Коцан І.Я. (голова) та ін.]. Луцьк : Вежа-Друк, 2015. С. 171-173.

80. Голубєва О.В. Жертви кіберзлочинів. Теорія і практика віктимології : матеріали Всеукр. конф. для студентів, аспірантів, ад"юнктів, здобувачів присвяч. 50-річчю з дня заснування каф. кримінології та кримінально-виконавчого права (Харків, 12 листоп. 2015 р.) / М-во освіти і науки України, Нац. юрид. ун-т ім. Ярослава Мудрого, Каф. кримінології та кримінал.-

виконав. права ; за ред. А.П. Гетьмана, Б.М. Головкіна ; [редкол.: Б.М. Головкін та ін.]. Харків : Право, 2015. С. 211-212

81. Горова С.В. Кіберпрофесіонали і кіберзлочинність // Боротьба з організованою злочинністю і корупцією (теорія і практика) : науково-практичний журнал. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ, 2014. № 2 (33), спецвипуск. С. 170-173.

82. Демедюк С.В. Міжнародний досвід протидії кіберзлочинності. Вісник Харківського національного університету внутрішніх справ : збірник наукових праць. Харківський національний університет внутрішніх справ. Харків, 2014. № 4 (67). С. 65-75.

83. Каланча С.Г. Кіберзлочинність: шляхи попередження та протидії. Наше право : науково-практичний журнал. Харк. нац. ун-т внутрішніх справ ;Кримінологічна асоціація України ; Київський міжнар ун-т; МАУП;Західно-регіональна асоціація клубів ЮНЕСКО. Дрогобич, 2012. № 3, ч.2. С. 213-217

84. Лук"янчук Р.В. Сучасний формат державного регулювання процесів забезпечення кібернетичної безпеки: досвід європейського союзу. Вісник Київського національного університету імені Тараса Шевченка. Київський національний університет імені Тараса Шевченка. Київ , 2016. (Державне управління ; вип. 2 (6)). С. 34-38.

85. Люта Н.В. Кіберзлочини як сучасна загроза фінансовій безпеці банків та їх клієнтів. Наука: теорія та практика : зб. тез доп. III Всеукр. наук.-практ. заоч. конф., 16-18 жовт. 2014 р. М-во освіти і науки України, Черкас. нац. ун-т ім. Богдана Хмельницького, Навч.-наук. ін-т економіки та права, Каф. менеджменту та екон. безпеки, Всеукр. спілка вчених-економістів ; [за заг. ред. проф. Мігус І.П.]. Черкаси : Чабаненко Ю.А., 2014. С. 247-252.

86. Марков В.В. Напрями діяльності НАТО у справі протидії кіберзлочинності. Право і безпека : науковий журнал / Харк. нац. ун-т внутрішніх справ. Харків, 2014. № 4 (55). С. 119-123.

87. Менджул М.В. Питання оптимізації зобов"язань, зумовлених ратифікацією Конвенції про кіберзлочинність. Бюлетень Міністерства юстиції України : загальнодержавне науково-практичне фахове видання. Міністерство юстиції України. Київ, 2012. № 3 (125). С. 70-74

88. Орлов Ю.Ю. Реалізація вимог міжнародної конвенції про кіберзлочинність у законодавстві України. Науковий вісник Національної академії внутрішніх справ : науково-теоретичний журнал. Національна академія внутрішніх справ. Київ, 2011. № 6 (79). С. 3-9

89. Рудой К.М. Протидія кіберзлочинності як напрям забезпечення міжнародної безпеки ОВС України. Публічне право : науково-практичний юридичний журнал. Всеукр. громадська організація "Майбутнє країни" ; Ужгород. нац. ун-т. Київ, 2015. № 3 (19). С. 144-149.

90. Савчук Н.В. Кіберзлочинність: зміст та методи боротьби. Теоретичні та прикладні питання економіки : збірник наукових праць. МОНУ; КНУ імені Тараса Шевченка; Ін-т конкурентного суспільства. Київ, 2009. Вип. 19. С. 338-342

91. Сироїд Т.Л. Діяльність Генеральної Асамблеї ООН у протидії кіберзлочинності. Справедливість у юриспруденції: теорія та практика : зб. матеріалів Міжнар. юрид. наук.-практ. конф. : тези наук. доповідей (23 лютого 2016 р.) : www.LegalActivity.com.ua / [відп. за вип. Н.І. Смеречинська]. Київ : МЮНІПК "Актуальна юриспруденція" ; АртЕк, 2017. (Міжнародні юридичні науково-практичні конференції "Актуальна юриспруденція"). С. 54-58.

92. Скулиш Є.Д. Посилення відповідальності в контексті підвищення ефективності боротьби із кіберзлочинністю. Правова інформатика : науковий фаховий журнал з питань інформатики, інформатизації, інформаційного права та інформаційної безпеки / Н.-д. ін-т інформатики і права Нац. акад. правових наук України ; Ін-т законодавства Верх. Ради України. Київ, 2013. № 4 (40). С. 90-97

93. Хахановський В.Г. Проблеми боротьби з організованою кіберзлочинністю в економічній сфері. Боротьба з організованою злочинністю і корупцією (теорія і практика) : науково-практичний журнал. Міжвідомчий науково-дослідний центр з проблем боротьби з організованою злочинністю. Київ, 2013. № 2 (30). С. 79-81.

94. Резолюція 45/113 Генеральної Асамблеї ООН від 14 грудня 1990 року. URL: http://zakon4.rada.gov.ua/laws/show/995_204 (дата звернення: 12.04.2017)

95. Goodman M.D., Brenner S.W. The Emerging Consensus on Criminal Conduct in Cyberspace. UCLA J.L. & Tech. 2002. № 3. URL http://www.lawtechjournal.com/articles/ 2002/03_020625_goodmanbrenner.php (дата звернення: 14.04.2017)

96. Курносов И.Н. Информационное общество и глобальные информационные сети: вопросы государственной политики. Информационное общество, 1998, вып. 6, С. 29 – 36. URL http://emag.iis.ru/arc/infosoc/emag.nsf/BPA/1dac741b1548a987c32569670032fc51 (дата звернення: 28.04.2017)

97. Грицун О.О. Регулювання питань міжнародної інформаційної безпеки в межах міжнародних організацій. Вісник Запорізького національного університету. Юридичні науки. 2014. №4(1). С. 172-180. URL http://nbuv.gov.ua/UJRN/Vznu_Jur_2014_4(1)__24. (дата звернення: 05.05.2017)

98. Computer-related crime. Recommendation No. R(89)9 on computer-related crime and final report of European committee on crime problems. Stasbourg. 1990. p. 60.

99. Европейская Конвенция по киберпреступлениям от 23 ноября 2001 года. URL: http://www.eos.ru/eos_delopr/eos_law/detail.php?ID=32003&SECTION_ID=671 (дата звернення: 09.05.2017)

100. Шепетько С. А. Міжнародний досвід протидії транснаціональній організованій злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2013. № 1. С. 298-306.

101. Угода між Кабінетом Міністрів України і Урядом Турецької Республіки про співробітництво правоохоронних органів. Міжнародний документ від 04.12.2009. Офіційний вісник України від 11.02.2011. 2011 р. № 8. стор. 226. стаття 408. код акту 54711/2011

102. Договір між Україною та Сполученими Штатами Америки про взаємну правову допомогу у кримінальних справах. Міжнародний документ від 22.07.1998. Офіційний вісник України від 16.08.2006. 2006 р. № 31. стор. 463. стаття 2280.

103. Угода про співробітництво між Генеральною прокуратурою України та Федеральною прокуратурою Королівства Бельгія у боротьбі з кіберзлочинністю, організованою злочинністю, корупцією і тероризмом. Міжнародний документ від 15.10.2015. Офіційний вісник України від 20.11.2015. 2015 р. № 90. стор. 443. стаття 3083. код акту 79308/2015.

104. Меморандум про співробітництво між Генеральною прокуратурою України та Національною прокуратурою Королівства Нідерланди у боротьбі з кіберзлочинністю, організованою злочинністю та відмиванням доходів, одержаних злочинним шляхом. Міжнародний документ від 09.09.2009. Офіційний вісник України від 12.10.2009. 2009 р. № 76. стор. 99. стаття 2601. код акту 48062/2009

105. Угода між урядами держав-членів ШОС про співробітництво в області забезпечення міжнародної інформаційної безпеки від 16 червня 2009 року URL http://base. spinform.ru/show_doc.fwx?rgn=28340 (дата звернення: 13.05.2017)

106. Хакерська атака в Україні: як працює вірус Petya.A і що робити? URL http://24tv.ua/hakerska_ataka_v_ukrayini_virus_petya_a_yak_pratsyuye_i_shho_robiti_n835033 (дата звернення: 18.05.2017)

107. Великий енциклопедичний юридичний словник. НАНУ; Ін-т держави і права ім. В.М. Корецького; Редкол.: Шемшученко Ю.С., Горбатенко В.П., Касяненко Ю.Я., Авер"янов В.Б. та ін. – Київ : Юридична думка, 2007. 992 с.

108. Цвік М.В. Загальна теорія держави і права : підручник для студ. юрид. спец. ВНЗ. М-во освіти і науки України, Нац. юрид. акад. України ім. Ярослава Мудрого. – Харків : Право, 2011. – 583 с.

109. Рассказов Л. П. Теория государства и права: Учебник для вузов. М.: РИОР, 2008. 463 с.

110. Луць Л.А. Загальна теорія держави та права : навч.-метод. посібник (за кредитно-модульної системою). Київ : Атіка, 2013. 411 с.

111. Луньова О. С. Окремі аспекти правового регулювання розслідування кіберзлочинів в Україні. Актуальні питання розслідування кіберзлочинів. Харків, 2013. С. 106-110

112. Орлов О. В. Міжнародна співпраця у сфері боротьби з кіберзлочинністю. Теорія та практика державного управління. 2013. Вип. 4. С. 17-23.

113. Луцький Р. П. Ієрархічність правових джерел (нормативних актів) як відображення буття позитивного права. Часопис Київського університету права. 2012. № 2. С. 18-21.

114. Про судову експертизу. Закон України від 25.02.1994 № 4038-XII // Відомості Верховної Ради України (ВВР). 1994. № 28. ст.232.

115. Про рішення Ради національної безпеки і оборони України від 31 жовтня 2001 року "Про заходи щодо вдосконалення державної інформаційної

політики та забезпечення інформаційної безпеки України». Указ президента України від 06.12.2001 № 1193/2001. Урядовий кур'єр від 18.12.2001. № 235

116. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України». Указ Президента України від 15.03.2016 № 96/2016. Урядовий кур'єр від 18.03.2016. № 52

117. Основні завдання Департаменту кіберполіції Національної поліції України. URL https://www.cybercrime.gov.ua/contacts (дата звернення: 02.06.2017)

118. Про Національну поліцію. Закон України від 02.07.2015 № 580-VIII. Відомості Верховної Ради (ВВР). 2015. № 40-41. ст.379.

119. Про Службу безпеки України. Закон України від 25.03.1992 № 2229-XII. Відомості Верховної Ради України (ВВР). 1992. № 27. ст.382.

120. Про Державну службу спеціального зв'язку та захисту інформації України. Закон України від 23.02.2006 № 3475-IV. Відомості Верховної Ради України (ВВР). 2006. № 30. ст.258.

121. Про Національний банк України. Закон України від 20.05.1999 № 679-XIV. Відомості Верховної Ради України (ВВР). 1999. № 29. ст.238.

122. Про утворення територіального органу Національної поліції. Постанова Кабінету Міністрів України від 13.10.2015 № 831. Урядовий кур'єр від 21.10.2015. № 195

123. Про затвердження Штату Департаменту кіберполіції Національної поліції України. Наказ Національної поліції України від 07.11.2015 № 10. URL https://www.npu.gov.ua/uk/publish/printable_article/1816252 (дата звернення: 03.06.2017)

124. Про ратифікацію Конвенції Організації Об'єднаних Націй проти транснаціональної організованої злочинності та протоколів, що її доповнюють (Протоколу про попередження і припинення торгівлі людьми, особливо жінками і дітьми, і покарання за неї і Протоколу проти незаконного ввозу мігрантів по суші, морю і повітрю). Закон України від 04.02.2004 № 1433-IV. Відомості Верховної Ради України (ВВР). 2004. № 19. ст.263.

125. Сорокин В. Д. Правовое регулирование: предмет, метод, процесс. Правоведение. 2000. №4 (231). С. 35-44.

126. Андрушко П. Використання модельних норм Конвенції Ради Європи "Про кіберзлочинність" та Додаткового протоколу до неї у нормотворчому процесі в Україні: теоретичні проблеми реалізації. Право України : юридичний журнал / Міністерство юстиції України; Конституційний Суд України та ін. Київ, 2007. № 12. С. 64-68.

127. Йона О.О. Світові тенденції боротьби з кіберзлочинністю. Вісник Східноукраїнського національного університету імені Володимира Даля. 2013. № 15(1). С. 59-61

128. Котух Є. Кіберзброя: проблеми та перспективи протидії кіберзлочинності. Зовнішні справи : суспільно-політичний журнал. М-во закордонних справ України ; Дипломатична акад. України при М-ві закордонних справ України ; Держ. п-во "Журн. М-ва закордонних справ України "Політика і час". Київ, 2012. № 4. С. 38-40

129. Сучасна правова енциклопедія. за ред. О.В. Зайчука ; Ін-т законодавства Верхов. Ради України. Київ : Юрінком Інтер, 2009. 382 с.

130. Пашковська Т. Кіберзлочинність в Україні: тенденції, статистика, протидії. Юридична газета. Київ, 2013. 12 лютого (№ 7). С. 10-13

131. Хлевицький В. Правові засади боротьби з кіберзлочинністю. Україна - НАТО : Інформаційно-аналітичний журнал Національного центру з питань євроатлантичної інтеграції України. Київ, 2006. № 4. С. 32-39

132. Маренич Д. Криміналістична характеристика кіберзлочинів. Вісник прокуратури : загальнодержавне фахове юридичне офіційне видання / Генеральна прокуратура України ; Нац. юрид. ун-т ім. Я. Мудрого ; Київ. нац. ун-т ім. Т. Шевченка. Київ, 2014. № 12 (162). С. 113-120

133. Цимбалюк В. Організація та координація боротьби з організованою транскордонною кіберзлочинністю. Право України : Юридичний журнал. Міністерство юстиції України; Конституційний Суд України та ін. Київ, 2003. № 2. С.26-30.

134. Хлевицький В. Основні напрямки вдосконалення нормативно-правового забезпечення боротьби правоохоронних органів України з кіберзлочинністю. Євроатлантикінформ : Науково-аналітичний бюлетень Нац центру з питань євроатлантичної інтеграції України. Київ, 2007. № 2/3. С. 51-53

135. Денькович О. Поняття кіберзлочину у зарубіжній кримінології. Проблеми державотворення і захисту прав людини в Україні : матеріали XXIII звіт. наук.-практ. конф., 7-8 лют. 2017 р. / Львів. нац. ун-т ім. Івана Франка, Юрид. ф-т ; [редкол.: В.М. Бурдін (голова) та ін.]. Львів : Львівський національний університет імені Івана Франка, 2017. Ч. 2. С. 130-133

136. Про внесення змін до Кримінального кодексу України щодо вдосконалення інституту спеціальної конфіскації з метою усунення корупційних ризиків при її застосуванні. Закон України від 10.11.2015 № 770-VIII. Відомості Верховної Ради (ВВР). 2015. № 49-50. ст.464.

137. Про внесення змін до деяких законодавчих актів України щодо припинення норм законів, схвалених 16 січня 2014 року. Закон України від 23.02.2014 № 767-VII. Відомості Верховної Ради (ВВР). 2014. № 17. ст.593.

138. Марков В. В. До питання щодо зарубіжного досвіду протидії кіберзлочинності. Право і Безпека. 2015. № 2. С. 107-113

139. Вінер О. В тенетах світової павутини: тенденції розвитку кібербезпеки у 2016 році. URL https://defence-ua.com/index.php/statti/562-v-tenetakh-svitovoyi-pavutyny-tendentsiyi-rozvytku-kiberbezpeky-u-2016-r (дата звернення: 14.06.2017)

140. Про боротьбу з тероризмом. Закон України від 20.03.2003 № 638-IV. Відомості Верховної Ради України (ВВР). 2003. № 25. ст.180.

141. Забара І.М. Міжнародно-правове регулювання співробітництва держав у боротьбі з інформаційною злочинністю. Часопис Академії адвокатури України. 2012 р. Т. 5. №4 (17). С. 1-6

142. Цивільний кодекс України. Закон України від 16.01.2003 № 435-IV // Відомості Верховної Ради України (ВВР). 2003. №№ 40-44. ст.356.

143. Селіванов В. Розмежування і взаємодія публічного і приватного права в системі права України. Право України. 1996. № 12. С. 30-37.

144. Про рішення Ради національної безпеки і оборони України від 28 квітня 2017 року "Про застосування персональних спеціальних економічних та інших обмежувальних заходів (санкцій)". Указ Президента України від 15.05.2017р. №133/2017. URL http://www.president.gov.ua/documents/1332017-21850 (дата звернення: 20.06.2017)

145. Савченко С. В. Співвідношення приватних і публічних інтересів: досвід України. Форум права. 2013. № 3. С. 520–528

146. Савчук Н. В. Світовий досвід державного регулювання ринку інтернет–послуг. Формування ринкових відносин в Україні. 2012. № 4. С. 24-28

147. Курицкий А.Ю. Интернет-экономика : закономерности формирования и функционирования. СПб. : Издательство С. Петербургского университета, 2000. 232 с.

148. National Security Strategy. The White House, February 2015. Washington D.C., 2015. 29 p. URL http://nssarchive.us/wp-content/uploads/2015/02/2015.pdf (дата звернення: 05.07.2017)

149. Винарик Л. С., Щедрин А. Н., Васильєва Н. Ф. Информационная экономика : становление, развитие, проблемы. НАН Украины ; Институт экономики промышленности. Донецк, 2002. 312 с.

150. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism : USA PATRIOT ACT (Act of 2001). Public Law 107–56—OCT. 26, 2001 URL https://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf (дата звернення: 08.07.2017)

151. Сопілко І. М. Міжнародно-правовий досвід захисту персональних даних: напрямки вдосконалення для України. Юридичний вісник. Повітряне і космічне право. 2014. № 4. С. 70-75.

152. Кравчук М. М. Міжнародний досвід правового регулювання захисту персональних даних в мережі Інтернет. Наукові записки Інституту законодавства Верховної Ради України. 2013. № 3. С. 123-126.

153. Cybersecurity Act of 2010. S. 773 (111th). April 1, 2009. URL https://www.govtrack.us/congress/bills/111/s773/text/is (дата звернення: 12.07.2017)

154. Computer Security Act Of 1987. June 11, 1987 № HR – 145. URL http://csrc.nist.gov/groups/SMA/ispab/documents/csa_87.txt (дата звернення: 20.07.2017)

155. Орлов О. В. Узагальнення міжнародного досвіду створення державної системи попередження та запобігання злочинам у мережі інтернет. Теорія та практика державного управління. 2014. Вип. 2. С. 212-219

156. Про Положення про Міністерство оборони України та Положення про Генеральний штаб Збройних Сил. Указ Президента України від 06.04.2011 № 406/2011. Офіційний вісник Президента України від 18.04.2011. 2011 р. № 10. стор. 39. стаття 559

157. Про Збройні Сили України. Закон України від 06.12.1991 № 1934-XII. Відомості Верховної Ради України (ВВР). 1992. № 9. ст.108.

158. Communication from the European Commission: "Network and Information Security: Proposal for a European Policy Approach" (COM (2001) 298 (June 6, 2001). URL http://ec.europa.eu/information_society/eeurope/2002/news_library/pdf_files/netsec_en.pdf (дата звернення: 14.06.2017)

159. Запорожець О.Ю. Політика Європейського Союзу в сфері інформаційної безпеки. Актуальні проблеми міжнародних відносин : зб. наук. пр. Київський нац. ун-т ім. Тараса Шевченка, Ін-т міжнар. відносин. К., 2009. Вип.87, ч.2. С.36-45.

160. Communication from the Commission: Towards a general policy on the fight against cyber crime. Brussels, 22.5.2007. COM(2007) 267 final. URL http://eur-lex.europa.eu/LexUriServ/site/en/com/2007/com2007_0267en01.pdf (дата звернення: 22.06.2017)

161. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. Боротьба з організованою злочинністю і корупцією (теорія і практика). 2008. Вип. 19. С. 240-246

162. Про засудження комуністичного та націонал-соціалістичного (нацистського) тоталітарних режимів в Україні та заборону пропаганди їхньої символіки. Закон України від 09.04.2015 № 317-VIII. Відомості Верховної Ради (ВВР). 2015. № 26. ст.219.

163. Управление по раскрытию преступлений в сфере высоких технологий (Управление «К»). История. URL http://mvd.gov.by/ru/main.aspx?guid=3291 .gov.by/ru/main.aspx?guid=1701 (дата звернення: 24.09.2017)

164. Буяджи С.А. Положительный опыт правового регулирования борьбы с киберпреступностью в странах ЕС. *Evropsky politicky a pravni diskurz, svazeky, 4 vydani 2017. European political and law discourse.* Volume 4. Issue 4. 2017. P. 41-46.

165. Войчишин В.Б. Актуалізація онто-гносеологічної моделі кібернетичного злочину. Науковий вісник Чернівецького університету : збірник наукових праць. Чернівецький національний університет. (Правознавство ; вип. 765). Чернівці, 2015. С. 11-17.

166. Амелін О. Кваліфікація кіберзлочинів та її вплив на компетенцію органів правопорядку. Вісник Національної академії прокуратури України / Національна академія прокуратури України. Київ, 2017. № 2 (48). С. 71-79.

167. Буяджи С.А. Тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія".* 2017. № 2. С. 21-32.

168. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. *Право України.* 2017. № 9. С. 245-251.

169. Бєляков Г Р. Принципи та правове регулювання діяльності управління боротьби з кіберзлочинністю МВС України // Вісник Харківського національного університету внутрішніх справ : збірник наукових праць / Харківський національний університет внутрішніх справ. Харків, 2014. № 4 (67). С. 17-25.

170. Рафал Канія Розвиток правової кібернетики у Польщі в XX-му сторіччі // Інформація і право : науковий журнал / Н.-д. ін-т інформатики і права Нац. акад. правових наук України ; Нац. б-ка України ім. В.І. Вернадського Нац. акад. наук України ; Відкритий міжнар. ун-т розвитку людини "Україна" ; голов. ред. Пилипчук В.Г. Київ, 2018. № 1 (24). С. 81-88.

ДОДАТКИ

СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Буяджи С.А. Генезис правового регулювання боротьби з кіберзлочинністю в світі. *Науковий вісник Ужгородського національного університету. Серія «Право».* 2014. № 29, ч. 2. Т. 4/2. С. 145-149.

2. Буяджи С.А. Поняття боротьби з кіберзлочинністю. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки».* 2015. № 3-2, Т. 4. С. 53-57.

3. Буяджи С.А. Перспективи правового регулювання боротьби з кіберзлочинністю в Україні. *Право України.* 2017. № 9. С. 245-251.

4. Буяджи С.А. Тенденції розвитку правового регулювання боротьби з кіберзлочинністю в Україні. *Вісник Чернівецького факультету Національного університету "Одеська юридична академія".* 2017. № 2. С. 21-32.

5. Буяджи С.А. Особливості правового регулювання боротьби із кіберзлочинністю у США. *Lex Portus: юридичний науковий журнал.* 2017. № 2 (4). С. 130-142.

6. Буяджи С.А. Положительный опыт правового регулирования борьбы с киберпреступностью в странах ЕС. *Evropsky politicky a pravni diskurz, svazeky, 4 vydani 2017. European political and law discourse.* Volume 4. Issue 4. 2017. P. 41-46.

7. Буяджи С.А. Теоретико-правова характеристика боротьби з кіберзлочинністю. *Актуальні проблеми сучасного правознавства: Матеріали міжнародної науково-практичної конференції (м. Київ, 28-29 січня 2016 р.).* К.: «Науково-дослідний інститут публічного права», 2016. С. 19-22.

8. Буяджи С.А. Структура механізму правового регулювання боротьби з кіберзлочинністю. *Реформування національного та міжнародного права:*

перспективи та пріоритети: матеріали міжнародної науково-практичної конференції (м. Одеса, 20-21 січня 2017 р.). Одеса: ГО «Причорноморська фундація права», 2017. С. 34-36.

9. Буяджи С.А. Національне правове регулювання боротьби з кіберзлочинністю. *Актуальні проблеми реформування системи законодавства України: матеріали міжнародної науково-практичної конференції (м. Запоріжжя, 27-28 січня 2017 р.).* Запоріжжя: Запорізька міська громадська організація «Істина», 2017. С. 29-31.