МІНІСТЕРСТВО ВНУТРІШНІХ СПРАВ УКРАЇНИ
НАЦІОНАЛЬНА АКАДЕМІЯ ВНУТРІШНІХ СПРАВ

Кваліфікаційна наукова праця
на правах рукопису

БІЛОБРОВ ТЕТЯНА ВІТАЛІЇВНА

УДК 342.951:[351.74:004](477)

АДМІНІСТРАТИВНО-ПРАВОВИЙ СТАТУС ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

12.00.07 – адміністративне право і процес;
фінансове право; інформаційне право

Подається на здобуття наукового ступеня кандидата юридичних наук

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

Науковий керівник **Басс Вікторія Олександрівна,** кандидат юридичних наук, доцент

Київ – 2020

АНОТАЦІЯ

Білобров Т. В. **Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України.** – *Кваліфікаційна наукова праця на правах рукопису.*

Дисертація на здобуття наукового ступеня кандидата юридичних наук за спеціальністю 12.00.07 – адміністративне право і процес; фінансове право; інформаційне право. – Національна академія внутрішніх справ, Київ, 2020.

У дисертаційному дослідженні наведено теоретичне узагальнення й нове вирішення наукового завдання щодо визначення сутності та особливостей адміністративно-правового статусу Департаменту кіберполіції Національної поліції України, а також шляхів його удосконалення. В результаті проведеного наукового дослідження сформульовано низку нових концептуальних положень, висновків та рекомендацій, спрямованих на досягнення поставленої у дисертації мети й вирішення завдань.

Надано теоретико-методологічну характеристику адміністративно-правового статусу Департаменту кіберполіції Національної поліції України, де визначено: поняття та окреслено сучасний стан кібербезпеки в Україні; виокремлено місце та роль органів Національної поліції України як суб'єкта забезпечення кібербезпеки в державі; охарактеризовані нормативні засади забезпечення кібербезпеки Національною поліцією України та визначено місце серед них адміністративно-правового регулювання; виокремлено поняття та елементи адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції.

Встановлено, що кібербезпека – це стан захищеності кіберпростору як від реальних так й потенційних кіберзагроз; охорони та захисту важливих інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища.

Обгрунтовано розмежування категорій національної системи кібербезпеки та системи забезпечення кібербезпеки, з яких першу запропоновано розуміти як сукупність всіх компонентів, за допомогою яких досягається кібербезпека: 1) суб'єктів та здійснюваних ними заходів (система забезпечення кібербезпеки), 2) об'єктів кібербезпеки та кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів, 3) норм права, що є основою для забезпечення кібербезпеки через встановлення зв'язків між суб'єктом та об'єктом: прямих та зворотних.

Під адміністративно-правовим статусом Департаменту кіберполіції Національної поліції України як міжрегіонального територіального органу поліції запропоновано розуміти характеристику правового положення відповідного суб'єкта забезпечення кібербезпеки та включає наступні елементи: 1) порядок утворення та припинення, найменування та місце в структурі апарату та механізмі держави; 2) правові норми, що встановлюють адміністративно-правовий статус Департаменту кіберполіції як міжрегіонального територіального органу поліції; 3) принципи служби в поліції; 4) цілі та завдання; 5) компетенцію (предмет відання та функції), 6) повноваження; 7) правові форми і методи їх реалізації; 8) юридичні гарантії діяльності; 9) правові обмеження.

Визначено роль і місце окремих елементів адміністративно-правового статусу Департаменту кіберполіції Національної поліції України, зокрема надано характеристику та визначені особливості таких його елементів як: завдання та функції; права й обов'язки; територіальна юрисдикція підрозділів Департаменту та юридичні гарантії підрозділів Департаменту кіберполіції Національної поліції України.

Аргументовано, що завдання та функції Департаменту кіберполіції Національної поліції України є важливою складовою визначення особливостей його діяльності та адміністративно-правового статусу, оскільки ефективне виконання Департаментом кіберполіції Національної поліції України своїх повноважень залежить від чіткого законодавчого розуміння

його завдань та функцій як базового елемента адміністративно-правового статусу будь-якого органу державної влади.

Виокремлено спеціальні завдання Департаменту кіберполіції Національної поліції України, зокрема наступні: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів.

З'ясовано, що за територіальною юрисдикцією управління кіберполіції Департаменту кіберполіції Національної поліції України поділяються на: Подільське управління кіберполіції Національної поліції України охоплює обслуговування Хмельницької, Вінницької та Тернопільської областей. Поліське управління кіберполіції Департаменту кіберполіції Національної поліції України, що охоплює обслуговування Волинської, Рівненської та Житомирської областей. Придніпровське управління кіберполіції Департаменту кіберполіції Національної поліції України – охоплює обслуговування Дніпропетровської, Кіровоградської та Запорізької областей. Донецьке управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Донецької та Луганської областей. Карпатське управління кіберполіції Департаменту кіберполіції Національної поліції України – зокрема обслуговування Львівської, Івано-Франківської, Чернівецької та Закарпатської областей. Київське управління кіберполіції Департаменту кіберполіції Національної поліції України обслуговує місто Київ, Київську, Черкаську та Чернігівську області. Причорноморське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Одеської, Миколаївської та Херсонської областей. Слобожанське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Сумської, Харківської та Полтавської областей.

Встановлено, що особливістю діяльності Департаменту кіберполіції Національної поліції України є визначення його територіальної юрисдикції, де остання визначена як передбачене нормативно-правовими актами коло повноважень кіберполіції залежно від території, на яку поширюється їх юрисдикція.

Під функціями Департаменту кіберполіції Національної поліції України запропоновано розуміти комплекс закріплених на нормативно-правовому рівні адміністративних, оперативно-розшукових, нормотворчих, кадрових, інформаційних і профілактичних напрямів його діяльності, виконання яких зумовлено завданнями у сфері протидії кіберзлочинності. До числа функцій Департаменту кіберполіції Національної поліції України віднесені: адміністративна, оперативно-розшукова, нормотворча, кадрова, інформаційного забезпечення, превентивна та профілактична.

Наголошено, що юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України – це відображені у нормативно-правових актах сукупність умов, способів та засобів, за допомогою яких визначаються умови і порядок реалізації, здійснення прав і свобод працівників, а також їх охорону, захист та відновлення у разі порушення. Аргументовано, що юридичним гарантіям Департаменту кіберполіції Національної поліції України притаманні ознаки, які мають важливе значення, адже вони відображають специфічні властивості, за допомогою яких можливо відокремити юридичні гарантії від інших видів гарантій. Визначено, що юридичні гарантії в сукупності з притаманними їм ознаками ефективніше діють та забезпечують реалізацію й захист прав, в іншому випадку можна поставити під сумнів їх фактичну реалізацію.

Встановлено, що до юридичних гарантій діяльності Департаменту кіберполіції Національної поліції України віднесені: 1) юридичні гарантії професійної діяльності Департаменту кіберполіції; 2) правові гарантії діяльності Департаменту кіберполіції; 3) організаційні гарантії діяльності Департаменту кіберполіції; 4) матеріально-технічні гарантії діяльності

Департаменту кіберполіції; 5) соціально-економічні гарантії діяльності Департаменту кіберполіції; 6) психологічні гарантії діяльності Департаменту кіберполіції.

Запропоновано шляхи удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України. Досліджено успішний (позитивний) зарубіжний досвід діяльності органів поліції у сфері протидії кіберзлочинам та виокремлені можливості його використання в Україні. Визначені шляхи удосконалення адміністративного законодавства, що регулює правовий статус Департаменту кіберполіції в Україні. Запропоновано удосконалити критерії оцінювання ефективності діяльності Департаменту кіберполіції в Україні, а також його організаційне забезпечення.

Визначено, що удосконалення адміністративно-правового забезпечення протидії кіберзлочинності в Україні має відбуватися з урахуванням національних культурно-історичних, соціально-економічних особливостей країни на підставі детального наукового аналізу міжнародного законодавства та досвіду інших країн у сфері боротьби з кіберзлочинністю з метою оптимального входження у європейське та світове правове поле.

Обгрунтовано доцільність затвердження концепції розвитку кіберполіції в Україні як арсеналу сучасних інструментів удосконалення роботи системи Національної поліції України взагалі. Наголошено, що розвиток кіберполіції передбачає таке реформування відповідних підрозділів Національної поліції України, що забезпечить підготовку та функціонування висококваліфікованих працівників в експертних, оперативних та слідчих підрозділах поліції, задіяних у протидії кіберзлочинності, та здатних застосовувати на високому професійному рівні новітні технології в оперативно-службовій діяльності.

Ключові слова: кібербезпека, суб’єкти забезпечення кібербезпеки, нормативні засади, адміністративно-правовий статус, завдання та функції, права й обов’язки, територіальна юрисдикція, юридичні гарантії, зарубіжний

досвід, удосконалення, Департамент кіберполіції Національної поліції України.

SUMMARY

Bilobrov T.V. The administrativeand legal status of the Cyberpolice Department of the National Police of Ukraine. – *Qualification scientific work on the rights of the manuscript.*

Thesis for a Candidate Degree in Law, specialty 12.00.07 – administrative Law and Process; finance law; Information Law. National Academy of Internal Affairs, Kyiv, 2020.

The dissertation research provides a theoretical generalization and a new solution to the scientific problem of determining the nature and features of the administrative and legal status of the Cyberpolice Department of the National Police of Ukraine, as well as ways to improve it. As a result of the conducted scientific research a number of new conceptual positions, conclusions and recommendations directed on achievement of the purpose set in the dissertation and the decision of problems is formulated.

Theoretical and methodological characteristics of the administrative and legal status of the Cyberpolice Department of the National Police of Ukraine are given, which defines: the concept and outlines the current state of cybersecurity in Ukraine; the place and role of the bodies of the National Police of Ukraine as a subject of cybersecurity in the state are highlighted; the normative bases of cybersecurity provision by the National Police of Ukraine are characterized and the place of administrative and legal regulation among them is determined; the concepts and elements of the administrative and legal status of the Cyberpolice Department of Ukraine as an interregional territorial police body are highlighted.

It is established that cybersecurity is a state of protection of cyberspace from both real and potential cyber threats; protection and defense of important interests of man and citizen, society and the state during its use as a condition for sustainable development of the information society and digital communication environment.

The distinction between the categories of the national cybersecurity system and the cybersecurity system is substantiated, the first of which is proposed to be understood as a set of all components through which cybersecurity is achieved: 1) subjects and measures (cybersecurity system), 2) cybersecurity and cybersecurity facilities as parts of the system that are influenced by the subjects, 3) the rules of law that are the basis for cybersecurity through the establishment of links between the subject and the object: direct and reverse.

Under the administrative and legal status of the Cyberpolice Department of the National Police of Ukraine as an interregional territorial police body, it is proposed to understand the characteristics of the legal status of the subject of cybersecurity and includes the following elements: 1) procedure for formation and termination; 2) legal norms establishing the administrative and legal status of the Cyberpolice Department as an interregional territorial police body; 3) principles of service in the police; 4) goals and objectives; 5) competence (subject of jurisdiction and functions), 6) authority; 7) legal forms and methods of their implementation; 8) legal guarantees of activity; 9) legal restrictions.

The role and place of certain elements of the administrative and legal status of the Cyberpolice Department of the National Police of Ukraine are determined, in particular, the characteristics and features of its elements such as: tasks and functions are given; rights and responsibilities; territorial jurisdiction of subdivisions of the Department and legal guarantees of subdivisions of the Cyberpolice Department of the National Police of Ukraine.

It is argued that the tasks and functions of the Cyberpolice Department of the National Police of Ukraine are an important component of determining the specifics of its activities and administrative status, as the effective implementation of the Cyberpolice Department of the National Police of Ukraine depends on a clear legislative understanding of its tasks and functions. any public authority.

Special tasks of the Cyber Police Department of the National Police of Ukraine are highlighted, in particular the following: implementation of state policy in the field of combating cybercrime; early informing the population about the

emergence of new cybercriminals; introduction of software for systematization of cyber incidents; responding to requests from foreign partners that will come through the channels of the National Round-the-clock network of contact points.

It was found that according to the territorial jurisdiction of the cyberpolice department of the Cyberpolice Department of the National Police of Ukraine are divided into: Podolsk cyberpolice department of the National Police of Ukraine covers services of Khmelnytsky, Vinnytsia and Ternopil regions. Polissya Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine, which covers the services of Volyn, Rivne and Zhytomyr regions. Prydniprovske Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine - covers the services of Dnipropetrovsk, Kirovohrad and Zaporizhia regions. Donetsk Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine covers services in Donetsk and Luhansk oblasts. Carpathian Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine - in particular service of Lviv, Ivano-Frankivsk, Chernivtsi and Zakarpattia regions. Kyiv Cyber Police Department The Cyber Police Department of the National Police of Ukraine serves the city of Kyiv, Kyiv, Cherkasy and Chernihiv regions. The Black Sea Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine covers the services of Odesa, Mykolaiv and Kherson oblasts. Slobozhansk Cyberpolice Department of the Cyberpolice Department of the National Police of Ukraine covers the services of Sumy, Kharkiv and Poltava regions.

It is established that the peculiarity of the Cyberpolice Department of the National Police of Ukraine is the definition of its territorial jurisdiction, where the latter is defined as provided by regulations of the powers of cyberpolice depending on the territory to which their jurisdiction extends.

The functions of the Cyber Police Department of the National Police of Ukraine are proposed to be understood as a set of administrative, operational and investigative, rule-making, personnel, information and preventive areas of its activity, which are conditioned by tasks in the field of combating cybercrime.

Among the functions of the Cyber Police Department of the National Police of Ukraine are: administrative, operational and investigative, rule-making, personnel, information support, preventive and preventive.

It is emphasized that the legal guarantees of the Cyberpolice Department of the National Police of Ukraine are a set of conditions, methods and means reflected in the regulations, which determine the conditions and procedure for exercising, exercising the rights and freedoms of employees, as well as their protection, protection and restoration. case of violation. It is argued that the legal guarantees of the Cyberpolice Department of the National Police of Ukraine are characterized by important features, as they reflect the specific properties by which it is possible to separate legal guarantees from other types of guarantees. It is determined that legal guarantees in combination with their inherent features are more effective and ensure the implementation and protection of rights, otherwise their actual implementation can be questioned.

It is established that the legal guarantees of the Cyberpolice Department of the National Police of Ukraine include: 1) legal guarantees of the professional activity of the Cyberpolice Department; 2) legal guarantees of the Cyberpolice Department; 3) organizational guarantees of the Cyberpolice Department; 4) material and technical guarantees of the Cyberpolice Department; 5) socio-economic guarantees of the Cyberpolice Department; 6) psychological guarantees of the Cyberpolice Department.

Ways to improve the administrative and legal status of the Cyber Police Department of the National Police of Ukraine are proposed. The successful (positive) foreign experience of police activity in the field of combating cybercrime is studied and the possibilities of its use in Ukraine are singled out. Ways to improve the administrative legislation governing the legal status of the Cyber Police Department in Ukraine have been identified. It is proposed to improve the criteria for evaluating the effectiveness of the Cyberpolice Department in Ukraine, as well as its organizational support.

It is determined that the improvement of administrative and legal support to combat cybercrime in Ukraine should take into account the national cultural, historical, socio-economic characteristics of the country on the basis of a detailed scientific analysis of international law and experience of other countries in combating cybercrime. rights field.

The expediency of approving the concept of cyberpolice development in Ukraine as an arsenal of modern tools for improving the work of the National Police of Ukraine in general is substantiated. It was stressed that the development of cyberpolice involves such a reform of the relevant units of the National Police of Ukraine, which will ensure the training and operation of highly qualified police, operational and investigative police units involved in combating cybercrime and able to apply the latest technologies in operational and service activities.

Key words: cybersecurity, subjects of cybersecurity, normative principles, administrative and legal status, tasks and functions, rights and responsibilities, territorial jurisdiction, legal guarantees, foreign experience, improvement, Cyberpolice Department of the National Police of Ukraine.

СПИСОК ПУБЛІКАЦІЙ ЗДОБУВАЧА ЗА ТЕМОЮ ДИСЕРТАЦІЇ

1. Ткач Т. В. Особливості територіальної юрисдикції підрозділів департаменту кіберполіції національної поліції України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2018. Випуск 50. Т. 4. С. 134–139.

2. Ткач Т. В. Понятие и структура административно-правового статуса Департамента киберполиции Национальной полиции Украины. *Право и политика*. 2019. № 1. С. 191–196. (Кыргызская Республика).

3. Ткач Т. В. Департамент киберполиции Национальной полиции Украины как субъект обеспечения кибербезопасности. *Право и Закон*. 2019. № 3. С. 184-189. (Кыргызская Республика).

4. Ткач Т. В. Юридичні гарантії діяльності департаменту кіберполіції національної поліції України. *Науковий вісник публічного та приватного права*. 2019. Випуск 6. С. 161–166.

5. Ткач Т. В. Органи національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень*. 2019. № 11. С. 113–117.

6. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96–102.

7. Білобров Т. В. Роль та місце департаменту кіберполіції національної поліції України у системі суб'єктів забезпечення кібербезпеки держави. *Правові новели*. 2020. № 11. С. 122–128.

8. Ткач Т. В. Забезпечення кібербезпеки як частина адміністративно-правового статусу Національної поліції. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи* : Міжнародна науково-практична конференція (м. Київ, 9–10 берез. 2018 р.). Київ : Центр правових наукових досліджень, 2018. С. 60–63.

9. Ткач Т. В. Завдання департаменту кіберполіції національної поліції України у сфері забезпечення кібербезпеки. *Актуальні проблеми реформування системи законодавства України* : матеріали міжнародної

науково-практичної конференції (м. Запоріжжя, 25-26 січ. 2019 р.). Запоріжжя : Запорізька міська громадська організація «Істина», 2019. С. 91–94.

10. Білобров Т. В. Сучасний стан та перспективи забезпечення кібербезпеки в Україні Національною поліцією. *Юридична наука України: історія, сучасність, майбутнє* : міжнародна науково-практична конференція (м. Харків, 1–2 листоп.а 2019 р.). Харків : Східноукраїнська наукова юридична організація, 2019. С. 78–80.

11. Білобров Т. В. Права та обов’язки департаменту кіберполіції національної поліції України як елемент адміністративно-правового статусу. *Право як ефективний суспільний регулятор* : матеріали міжнародної науково-практичної конференції (м. Львів, 14–15 лют. 2020 р.). Львів : Західноукраїнська організація «Центр правничих ініціатив», 2020. С. 45–47.

ЗМІСТ

ВСТУП..... 16

РОЗДІЛ 1. ТЕОРЕТИКО-МЕТОДОЛОГІЧНА ХАРАКТЕРИСТИКА ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ УКРАЇНИ..... 26

1.1. Поняття та сучасний стан кібербезпеки в Україні 26

1.2. Органи Національної поліції України як суб'єкт забезпечення кібербезпеки..... 37

1.3. Нормативні засади забезпечення кібербезпеки Національною поліцією України та місце серед них адміністративно-правового регулювання..... 48

1.4. Поняття та елементи адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції..... 57

Висновки до розділу 1 70

РОЗДІЛ 2. ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОКРЕМИХ ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ В УКРАЇНІ..... 73

2.1. Завдання та функції Департаменту кіберполіції в Україні..... 73

2.2. Права й обов'язки Департаменту кіберполіції в Україні..... 90

2.3. Територіальна юрисдикція підрозділів Департаменту кіберполіції в Україні 101

2.4. Юридичні гарантії підрозділів Департаменту кіберполіції в Україні 112

Висновки до розділу 2 125

РОЗДІЛ 3. УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ В УКРАЇНІ..... 130

3.1. Зарубіжний досвід діяльності органів поліції у сфері протидії кіберзлочинам та можливості його використання в Україні..... 130

3.2. Шляхи удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції в Україні..... 157

Висновки до розділу 3 163

ВИСНОВКИ 169

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 177

ДОДАТКИ..... 202

ВСТУП

Обгрунтування вибору теми дослідження. Сьогодні стан безпекового середовища в Україні є нижчим середніх показників стану захищеності життєво важливих інтересів як окремих громадян, так і держави в цілому. Безпековий простір в Україні кожного дня зазначає різних ударів, одним із яких є проведення Операції Об'єднаних Сил на Сході України, що здійснює дестабілізуючий вплив на стан правопорядку на тимчасово окупованих територіях України. Тим не менш, відповідними спеціалізованими органами (спеціальними підрозділами Національної поліції України) здійснюється ряд заходів щодо відновлення стану правопорядку тимчасово окупованих територіях України та підтримання миру та безпеки серед мирного населення.

В той же час, поряд із загрозами національній безпеці України, постало питання протидії кіберзагрозам у віртуальному середовищі, що непомітно пронизали сучасний Інтернет-простір. З урахуванням вітчизняних тенденцій розвитку кіберзагроз, що здійснюють свій систематичний руйнівний вплив на інформаційне та віртуальне середовище, актуальним є визначення основних напрямів трансформації державної політики забезпечення кібербезпеки в Україні та протидії кіберзлочинності. Відповідно чинне нормативно-правове регулювання сферою кібербезпеки сьогодні потребує свого удосконалення, а й відповідно – удосконалення діяльності суб'єктів уповноважених на протидію кіберзлочинності. Одним з таких суб'єктів є Департамент кіберполіції як головний суб'єкт реалізації державної політики в сфері протидії кіберзлочинності та захисту кіберпростору. Діяльність Департаменту кіберполіції сьогодні набуває особливо актуального значення у зв'язку з інтенсивним розвитком кіберзлочинності. Зокрема, поліцейськими Департаменту кіберполіції у поточному році було виявлено шість тисяч злочинів, вчинених у сфері використання високих інформаційних технологій.

У 2018 році працівники Департаменту кіберполіції викрили більше 800 осіб, які були причетні до вчинення злочинів у кіберпросторі. Згідно статистики, більша частина підозрюваних – чоловіки у віці від 25 до 40 років [137].

В умовах нових імпульсів кіберзагроз в Україні, держава потребує створення відповідної дієвої системи кіберзахисту та формування у відповідності з міжнародними нормами та стандартами нормативно-правової бази її регулювання. Вбачається доцільним провести комплексний аналіз кібербезпекової сфери держави та правового статусу Департаменту кіберполіції Національної поліції України.

Визначення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України є вельми актуальним та своєчасним, оскільки, практика функціонування зазначених органів свідчить про їх важливе призначення, що обумовлює потребу у чіткому визначенні їх завдань та функцій, кола повноважень, юридичної відповідальності та гарантій діяльності, тобто – їх адміністративно-правового статусу.

Загальнотеоретичні та галузеві питання адміністративно-правового статусу Національної поліції України та окремих її органів та підрозділів розробляли такі вчені-правознавці, як: В. Б. Авер'янов, С. М. Алфьоров, В. І. Андріяш, В. Г. Атаманчук, О. М. Бандурка, О. А. Баранов, В. Ю. Баскаков, В. О. Басс, Д. М. Бахрах, І. Л. Бачило, О. І. Безпалова, С. Г. Братель, К. І. Бєляков, В. В. Береза, В. М. Гаращук, О. П. Гетманець, Є. А. Гетьман, І. П. Голосніченко, С. М. Гусаров, С. Ф. Денисюк, В. Б. Дзюндзюк, О. Ю. Дрозд, В. А. Залізняк, Р. А. Калюжний, А. М. Клочко, Ю. В. Ковбасюк, Т. О. Коломоєць, В. К. Колпаков, А. Т. Комзюк, В. А. Копилов, Б. А. Кормич, К. М. Куркова, В. А. Ліпкан, О. В. Логінов, В. Я. Малиновський, Д. М. Мартинов, О. І. Миколенко, Л. В. Могілевський, О. М. Музичук, В. І. Олефір, М. Л. Пахнін, В. М. Плішкін, А. М. Подоляка, Г. Г. Почепцов, Т.О. Проценко, Р. А. Сербін, О. Ю. Салманова, О. Ю. Синявська, О. Ф. Скакун, В. В. Сокуренко, С. Г. Стеценко, В. В. Тертичка, В. С. Цимбалюк, В. В. Чумак, Д. В. Швець,

Ю. С. Шемшученко, І. М. Шопіна та інші. Проте, незважаючи на вагомий науковий доробок, присвячений різним аспектам діяльності щодо забезпечення кібербезпеки, у тому числі органами поліції, на сьогодні вченими питання адміністративно-правового статусу саме Департаменту кіберполіції Національної поліції України висвітлені фрагментарно, що й обумовлює актуальність даного наукового дослідження. Оскільки питання забезпечення кібербезпеки в державі останнім часом посідають чільне місце у системі реалізації державної політики захисту та забезпечення національної безпеки держави.

Необхідність підвищення реалізації державної політики у сфері забезпечення кібербезпеки держави, дотримання прав людини й громадянина у віртуальному просторі, забезпечення правопорядку в державі в цілому, недосконаліть адміністративно-правового регулювання діяльності Департаменту кіберполіції Національної поліції України, недостатність наукових розробок із зазначених питань обумовлюють актуальність комплексного дослідження сутності та особливостей адміністративно-правового статусу Департаменту кіберполіції Національної поліції України.

Зв'язок роботи з науковими програмами, планами, темами. Дисертація виконана відповідно до Закону України «Про основні засади забезпечення кібербезпеки України від 5 жовтня 2017 р. № 2163-VIII; Стратегії національної безпеки України, затвердженої Указом Президента України від 26 травня 2015 р. № 287/2015; Цілей сталого розвитку України на період до 2030 року, схвалених Указом Президента України від 30 вересня 2019 р. № 722/2019; Стратегії реформування державного управління України на період до 2021 року, схваленої розпорядженням Кабінету Міністрів України від 24 червня 2016 р. № 474-р; Стратегії розвитку системи Міністерства внутрішніх справ на період до 2020 року, схваленої розпорядженням Кабінету Міністрів України від 15 листопада 2017 р.; Пріоритетних напрямків наукового забезпечення діяльності органів внутрішніх справ України на період 2015–2019 років, затверджених наказом

МВС України від 16 березня 2015 р. № 275, а також, основним напрямам наукових досліджень Національної академії внутрішніх справ на 2018–2020 рр. та Плану науково-дослідних та дослідно-конструкторських робіт Національної академії внутрішніх справ на 2020 рік. Тему дисертації затверджено на засіданні Вченої ради Національної академії внутрішніх справ від 29 жовтня 2015 р. (протокол № 20).

Мета і завдання дослідження. *Мета* дослідження полягає в тому, щоб на основі аналізу чинного законодавства України та відповідних підзаконних нормативно-правових актів, узагальнення практики їхньої реалізації визначити сутність та особливості адміністративно-правового статусу Департаменту кіберполіції в Україні, а також шляхи його удосконалення.

Для досягнення поставленої мети в дисертації планується вирішити такі комплексні *завдання*:

– з’ясувати поняття та сучасний стан кібербезпеки в Україні; охарактеризувати органи Національної поліції України, як суб’єкт забезпечення кібербезпеки;

– встановити нормативні засади забезпечення кібербезпеки Національною поліцією України та з’ясувати місце серед них адміністративно-правового регулювання;

– визначити поняття та елементи адміністративно-правового статусу Департаменту кіберполіції в Україні, як міжрегіонального територіального органу поліції;

– систематизувати завдання та функції Департаменту кіберполіції в Україні;

– охарактеризувати права та обов’язки Департаменту кіберполіції в Україні;

– визначити територіальну юрисдикцію підрозділів Департаменту кіберполіції в Україні;

– розкрити сутність юридичних гарантій діяльності Департаменту кіберполіції в Україні;

– узагальнити зарубіжний досвід діяльності органів поліції у сфері протидії кіберзлочинам та можливості його використання в Україні;

– сформулювати пропозиції щодо удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції в Україні.

Об'єктом дослідження є правовідносини, що виникають під час реалізації адміністративно-правового статусу Департаменту кіберполіції Національної поліції України.

Предметом дослідження є адміністративно-правовий статус Департаменту кіберполіції Національної поліції України.

Методи дослідження. Методологічною основою дослідження є сучасні загальнонаукові та спеціальні методи пізнання. Їх застосування обумовлено системним підходом, що дозволило досліджувати проблеми в єдності їх соціального змісту та юридичної форми. За допомогою логіко-семантичного наукового методу поглиблено понятійний апарат (підрозділи 1.1, 1.4, розділ 2, 3.3, 3.4). Для аналізу змісту адміністративно-правового статусу Департаменту кіберполіції Національної поліції України використовувались методи аналізу та синтезу, класифікації (підрозділи 1.4, 2.1, 2.2, 2.3, 2.4, 3.2, 3.3). Функціональний підхід, документальний аналіз, статистичний та соціологічний методи застосовано для характеристики місця й ролі, а також нормативних засад діяльності Департаменту кіберполіції Національної поліції України, зарубіжного досвіду діяльності органів поліції у сфері протидії кіберзлочинам (підрозділи 1.3, 3.1, 3.2, 3.3). З використанням порівняльно-правового та діалектичного методів наукового пізнання встановлено напрями удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України (підрозділ 3.2, 3.3, 3.4). Структурно-логічний застосовано для аналізу функціонування органів Національної поліції України як суб'єкта забезпечення кібербезпеки (підрозділ 1.2).

Емпіричну базу дослідження становлять: 1) статистичні дані Міністерства внутрішніх справ України за 2018-2019 рр.; 2) статистичні дані Головного управління статистики у Київській області за 2019 рік; 3) звіт Голови Національної поліції України про результати роботи відомства у 2019 році; 4) дані OpenDataBot щодо кількості кіберзлочинів в Україні за 2017-2019 рр.; 5) узагальнення практичної діяльності Департаменту кіберполіції Національної поліції України за 2018 та 2019 роки.

Наукова новизна одержаних результатів полягає у тому, що дисертація є одним із перших комплексних наукових досліджень адміністративно-правового статусу Департаменту кіберполіції Національної поліції України. У результаті проведеного наукового дослідження сформульовано низку нових наукових положень, висновків та рекомендацій, запропонованих особисто здобувачем. Основні з них такі:

вперше:

– визначено сутність та зміст адміністративно-правового статусу Департаменту кіберполіції Національної поліції України як характеристику правового положення відповідного суб'єкту забезпечення кібербезпеки та включає наступні елементи: 1) порядок утворення та припинення, найменування та місце в структурі апарату та механізму держави; 2) правові норми, які встановлюють статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції; 3) принципи служби в поліції; 4) цілі та завдання; 5) компетенцію (предмет відання та функції), 6) повноваження; 7) правові форми і методи їх реалізації; 8) юридичні гарантії; 9) правові обмеження;

– сформульовано пропозиції щодо удосконалення організаційного забезпечення діяльності Департаменту кіберполіції Національної поліції України, зокрема: 1) закріпити на законодавчому рівні ключовий термін «кібербезпека»; 2) запровадити механізм взаємодії на внутрішньовідомчому рівні – з іншими оперативними підрозділами блоку кримінальної поліції, науково-дослідними експертно-криміналістичними центрами та слідчими

підрозділами; на внутрішньодержавному – з іншими правоохоронними органами України, трудовими колективами, громадськими організаціями й населенням; на міжнародному рівні – з правоохоронними органами інших країн; 3) запровадити системний підхід до реалізації міжнародних документів, що регламентують забезпечення кібербезпеки держави та протидії кіберзлочинності;

– запропоновано визначити нормативно-правову базу моніторингу кіберзагроз, кібератак та кіберінцедентів як основи для попередження кіберзлочинності, розробки методологічних рекомендацій по забезпеченню кібербезпеки, моделювання та прогнозування кібератак, виявлення та нейтралізації кіберзагроз;

удосконалено:

– поняття кібербезпеки, під яким визначено стан захищеності кіберпростору як від реальних так й потенційних кіберзагроз; охорони та захисту прав та інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища;

– підходи до розуміння поняття завдань та функцій діяльності Департаменту кіберполіції Національної поліції України, їх групування та характеристика, зокрема поділ функцій Департаменту кіберполіції здійснено на наступні види: адміністративна, оперативно-розшукова, нормотворча, кадрова, інформаційного забезпечення, превентивна та профілактична функції;

– характеристика прав й обов’язків Департаменту кіберполіції Національної поліції України, під якими розуміється система визначених на нормативно-правовому рівні юридичних прав (міри можливої поведінки) та юридичних обов’язків (міри необхідної поведінки), якими наділяється Департамент кіберполіції Національної поліції України з метою реалізації покладених на нього завдань та функцій;

– розуміння системи юридичних гарантій діяльності Департаменту кіберполіції Національної поліції України, до якої включені наступні: правові, матеріально-технічні та соціальні гарантії. Під юридичними гарантіями діяльності Департаменту кіберполіції Національної поліції України запропоновано розуміти відображені у нормативно-правових актах сукупність умов, способів та засобів, за допомогою яких визначаються умови і порядок реалізації, здійснення прав і свобод працівників, а також їх охорону, захист та відновлення у разі порушення;

дістало подальший розвиток:

– визначення особливостей територіальної юрисдикції управлінь кіберполіції Національної поліції України, де Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції України та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність;

– класифікація завдань Департаменту кіберполіції Національної поліції України, де останні запропоновано поділяти на: загальні та спеціальні, завдання, що не пов’язані із державною таємницею та такі, що пов’язані зі державною таємницею;

– розуміння національної системи кібербезпеки та системи забезпечення кібербезпеки, з яких до першої відносяться: 1) суб’єкти та здійснювані ними заходи (система забезпечення кібербезпеки), 2) об’єкти кібербезпеки та кіберзахисту як частини системи, що зазнають впливу з боку суб’єктів, 3) норми права, що є основою для забезпечення кібербезпеки через встановлення зв’язків між суб’єктом та об’єктом: прямих та зворотних;

– узагальнення успішного зарубіжного досвіду діяльності аналогічних органів поліції, за результатами якого максимально можливою визнається

імплементація канадської моделі розкриття комп'ютерних злочинів як найбільш привабливої для кібернетичної політики нашої держави.

Практичне значення отриманих результатів полягає в тому, що вони становлять як науково-теоретичний, так і практичний інтерес, зокрема висновки, пропозиції та рекомендації, сформульовані в дисертації, використовуються у:

– *науково-дослідній діяльності* – для подальшого дослідження актуальних питань адміністративно-правового статусу Департаменту кіберполіції Національної поліції України (акт впровадження у наукову діяльність Національної академії внутрішніх справ від 16.01.2020. року);

– *правотворчості* – під час розробки нових та удосконалення чинних нормативно-правових актів з питань функціонування та організації діяльності Департаменту кіберполіції Національної поліції України (акт впровадження Інституту законодавства Верховної Ради України від 18 січня 2019 р. № 22/771-1-15);

– *правозастосовній діяльності* – їх використання дозволить покращити практичну діяльність Департаменту кіберполіції Національної поліції України;

– *освітньому процесі* – при підготовці підручників та навчальних посібників, методичних розробок, а також при проведенні занять з навчальних дисциплін «Адміністративне право», «Актуальні проблеми адміністративного права та процесу», «Судові та правоохоронні органи в Україні», «Адміністративна діяльність поліції» (акт впровадження в освітній процес Національної академії внутрішніх справ від 17.01.2020. року).

Апробація результатів дисертації. Основні положення та висновки дисертації було оприлюднено на міжнародних, зокрема: «Сучасні правові системи світу в умовах глобалізації: реалії та перспективи» (м. Київ, 9–10 березня 2018 р.); «Актуальні проблеми реформування системи законодавства України» (25-26 січня 2019 р.); «Юридична наука України:

історія, сучасність, майбутнє» (м. Харків, 1–2 листопада 2019 р.), «Право як ефективний суспільний регулятор» (м. Львів, 14–15 лютого 2020 р.).

Публікації. Основні положення та результати дисертації відображено у 11 наукових статтях, 5 з яких опубліковано у наукових фахових виданнях України, 2 – в іноземному виданні (Киргизька Республіка), а також у чотирьох тезах, які оприлюднено на науково-практичних конференціях.

РОЗДІЛ 1
ТЕОРЕТИКО-МЕТОДОЛОГІЧНА ХАРАКТЕРИСТИКА ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ УКРАЇНИ

1.1. Поняття та сучасний стан кібербезпеки в Україні

Поняття кібербезпеки нещодавно було введено до законодавства України як відповідь на зміни відносин в аспекті комунікації суб'єктів поза фізичним простором. Як вказують М. М. Присяжнюк та Є. І Цифра, «стрімкий розвиток інформаційних технологій, інформатизація та комп'ютеризація, створення глобального інформаційного простору сформували принципово нові субстанції — інформаційне суспільство, інформаційний і кібернетичний простори, які мають невичерпний потенціал і відіграють головну роль в економічному та соціальному розвитку країн світу. Науково-технічна революція початку XXI ст. спричинила в усьому світі глибокі системні перетворення. Поєднання досягнень у сфері новітніх інформаційно-комунікаційних технологій та стрімкого розвитку інформаційно-телекомунікаційних систем викликало появу так званого віртуального простору, який ще отримав назву «кіберпростір» [142, с. 61] або інформаційний простір — глобальне інформаційне середовище, яке в реальному масштабі часу забезпечує комплексну обробку відомостей [78, с. 7]. Розвиток кіберпростору, вважає І. В. Діордіца, як окремого виду простору став закономірним наслідком взаємопроникнення суспільних та природничих наук, використання математичного апарату [72, с. 87]. І на сьогодні у всьому світі відбувається глобальне перенесення соціальної й економічної активності індивідів у кіберпростір, який стає невід'ємною складовою сучасного суспільства, частиною сучасного навколишнього середовища [63, с. 119] являючи собою нове середовище для встановлення зв'язків суб'єктів правовідносин, який відрізняється від фізичного рядом специфічних ознак.

Що найперше, його пропонується розглядати як середовище, що виникає в результаті функціонування на основі єдиних принципів і за загальними правилами інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем [11, с. 23]. Кіберпростір не має чітко визначених територіальних меж та кордонів, і взагалі не може вважатися територією. Завдяки цій властивості кіберпростір вважають глобальним середовищем для комунікації суб'єктів правовідносин. Кіберпростір не передбачає фізичного контакту суб'єктів правовідносин, які можуть бути і не ідентифікованими при здійсненні комунікації за допомогою цифровізації їх зв'язків. Такі зв'язки здійснюються через програмне забезпечення на основі спеціальних протоколів. Кіберпростір характеризують «неперевершені можливості зі створення незлічених зв'язків між окремими індивідами і соціальними групами та з надання різнопланових інформаційних послуг» [78, с. 9]. Як вважає В. В. Бухарєв, кіберпростір являє собою високорозвинену модель об'єктивної реальності, в якій відомості щодо осіб, предметів, фактів, подій, явищ і процесів подаються в математичному, символічному або в будь-якому іншому вигляді, розміщуються в пам'яті фізичних пристроїв, спеціально призначених для зберігання, обробки й передавання інформації [31, с. 31]. Всі виділені особливості кіберпростору як якісно нового середовища для реалізації та охорони правовідносин забезпечують суб'єктам правовідносин ряд переваг порівняно з комунікацією у просторі фізичному.

До таких переваг доцільно віднести і швидкість комунікації без затрат часу на фізичний контакт, і можливість з будь-якої точки планети стати учасником певних відносин, і оперативність вирішення питань тощо. Як обґрунтовано стверджують В. А. Ліпкан та І. В. Діордіца, відкритий та вільний кіберпростір розширює свободу і можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну та ефективну роботу влади й активне залучення громадян до управління державою та вирішення питань

місцевого значення, забезпечує публічність та прозорість влади, сприяє запобіганню корупції [109, с. 176]. Однак, при наявності ряду переваг, перенесення відносин у кіберпростір має і негативні наслідки.

Стрімкий розвиток віртуального середовища, новизна його властивостей є основою для порушення прав суб'єктів правовідносин, які з фізичного простору перенесли свої комунікації у простір віртуальний. На сьогодні, доходить висновку М. В. Камчатний, розвиток технологій досяг такого рівня, що замість первинної мети – полегшення комунікації, пришвидшення інформаційних та виробничих процесів – створюється нова загроза для користувачів таких технологій. Умовно, ще вчора протиправними діями із використанням Інтернету були крадіжки персональних даних, шахрайство, промисловий шпіонаж. На сьогодні ж можливості використання Мережі, як і масштаби її розповсюдження світом, значно підвищилися. Уже абсолютно реальними є такі поняття, як шпигунство із використанням Інтернету, кібернетичний тероризм і навіть кібервійна [79, с. 12]. М. М. Присяжнюк та Є. І. Цифра з цього приводу вказують, що відкритий кіберпростір розширює свободу та можливості людей, збагачує суспільство, створює новий глобальний інтерактивний ринок ідей, досліджень та інновацій, стимулює відповідальну й ефективну роботу влади і активне залучення громадян до управління державою та вирішення питань місцевого значення, забезпечує публічність і прозорість влади, сприяє запобіганню корупції. Водночас переваги сучасного кіберпростору обумовили виникнення нових загроз національній і міжнародній безпеці. Поряд з інцидентами природного (ненавмисного) походження зростає кількість і потужність кібератак, вмотивованих інтересами окремих держав, груп та осіб [142, с. 64].

Отже, не можна заперечувати, що через небачене досі поширення інформаційно-комунікаційних технологій та інформаційно-телекомунікаційних систем світова спільнота отримала не лише численні переваги, а й цілу низку проблем, зумовлених дедалі більшою вразливістю

інфосфери щодо стороннього кібернетичного впливу [78, с. 4] Як вважає А. В. Вінаков, вияви кіберзлочинності у вигляді хакерських атак на комп'ютерні системи банківських та інших фінансових установ, крадіжок електронних коштів, широкого використання мережі Інтернет для наркоторгівлі, торгівлі людьми, інших протиправних дій стають реальною загрозою національній безпеці [45, с. 34]. Від так поряд з поняттям кіберпростору з'являється поняття кібербезпеки, забезпечення якої на сьогодні є одним з пріоритетів як внутрішньої, так і зовнішньої політики не тільки України, але і всіх держав світу.

Дослідники В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа вважають, що цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи [78, с. 4]. Створення інформаційного суспільства, підсумовують автори М. М. Присяжнюк та Є. І Цифра, призвело до виникнення багатьох інформаційних загроз, а одним із головних завдань сучасної інформаційної епохи є забезпечення інформаційної та кібернетичної безпеки [142, с. 61]. На зв'язку таких категорій як «глобальне інформаційне суспільство» та «кібербезпека» наголошується ще в Окінавській хартії глобального інформаційного суспільства, де вперше з'являється поняття кіберпростору «безпечного» і «вільного від злочинності» як мети співпраці міжнародного співтовариства [127]. Дане завдання не втрачає актуальності й до сьогодні.

Автор В. А. Світличний стверджує, що на сучасному етапі розвитку науки і техніки кібербезпека перетворюється на одну з найактуальніших задач високотехнологічного суспільства. Внаслідок надзвичайно широкого використання сучасних інформаційних технологій в усіх сферах свого існування суспільство стало вразливим від незначних кібернетичних впливів, які все частіше стають ефективним інструментом на шляху досягнення мети щодо несилового контролю та управління як об'єктами критичної інфраструктури держави, підприємств, так і окремо взятими громадянами, їх об'єднаннями [163, с. 352]. Широких масштабів проблема кібербезпеки набула тоді, коли держави усвідомили усі можливі наслідки від реалізації загроз у сферах, де використовувались комп'ютерні системи. При незначному обсязі ресурсів для реалізації цих загроз досягаються значні результати, здатні паралізувати цілі компанії та держави [38, с. 118]. При цьому, як вказують В. А.Ліпкан та І. В. Діордіца, останнім часом проблема забезпечення національної безпеки зміщується у бік не стільки декларованої, скільки реально розглядуваної. Передусім, це обумовлено активізацією зовнішніх загроз безпечного розвитку України: посиленням мілітаризації держав у регіоні, використанням положення енергетичної та торговельно-економічної залежності нашої країни, посиленням економічного та інформаційного тиску на неї тощо. Разом із тим, зовнішні загрози посилюються наявністю внутрішніх викликів національній безпеці, зокрема, йдеться про розбалансованість та незавершеність системних реформ, зниження обороноздатності держави, боєздатності Збройних Сил України, незадовільний стан фінансування, складне економічне становище [109, с. 174].

Формуючи поняття кібербезпеки, В. А. Світличний доходить висновку про можливість трактування поняття одночасно у діяльнісному та статичному вимірах. Як вважає науковець, кібербезпека - це захищеність від наявних та потенційно небезпечних проявів інформаційного впливу, що створюють небезпеку для функціонування інформаційних ресурсів, систем,

мереж, програмних і апаратних засобів, а також свідомості, підсвідомості, морально-психологічного стану людини, соціальних груп та суспільства в цілому. З іншого, кібербезпека - це комплекс заходів та засобів, що спрямовані на захист комп'ютерів, цифрових даних і мереж їх передачі від несанкціонованого доступу та інших дій, пов'язаних з маніпулюваннями або крадіжкою, блокуванням, пошкодженням, руйнуванням та знищенням як випадкового, так і цілеспрямованого впливу. Тому об'єктом діяльності фахівця з кібербезпеки є процеси захисту інформації у всіх її видах [163, с. 352]. На наш погляд, більш точним є розмежування понять кібербезпеки як певного стану та поняття її забезпечення як діяльності.

Така позиція знаходить свої підтвердження в законодавстві України. Зокрема, в Законі України «Про основні засади забезпечення кібербезпеки України» [151] визначено не тільки поняття кібербезпеки, а й ряд інших понять, що мають провідне значення для забезпечення безпечних умов використання кіберпростору: кіберзагроза, кібератака, кіберінцедент, кіберзлочин, кіберзлочинність тощо.

Згідно ч. 5 ст. 1 вказаного Закону кібербезпека визначається як захищеність життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якої забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі [151]. Як бачимо, законодавець використовує статичний підхід до формування поняття кібербезпеки. А от поняття забезпечення кібербезпеки в законі відсутнє.

Виходячи з результатів комплексного аналізу статей вказаного закону можна запропонувати розуміти під забезпеченням безпеки комплекс взаємопов'язаних заходів політичного, науково-технічного, інформаційного, освітнього характеру, організаційних, правових, оперативно-розшукових, розвідувальних, контррозвідувальних, оборонних, інженерно-технічних заходів, а також заходів криптографічного і технічного захисту національних

інформаційних ресурсів, кіберзахисту об’єктів критичної інформаційної інфраструктури [151]. Близьке до наданого поняття кіберборотьби, під якою запропоновано розуміти 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 [78, с. 11].

Якщо конкретизувати дане визначення стосовно Національної поліції, то можна погодитись, що боротьба із кіберзлочинністю є процесом, який передбачає комплексне застосування заходів, а нормативно-правове регулювання забезпечує закріплення відповідних механізмів, як вважає С. А. Буяджи [32, с. 107]. Уточнення потребує лише обмеження заходів із забезпечення кібербезпеки боротьбою, поза увагою залишаючи попередження кіберзлочинів [129], інформування про кіберзлочинність та кіберзлочини та підвищення поінформованості громадян про безпеку в кіберпросторі.

Як вказує О. І. Гончаренко, питання протидії кіберзлочинам, їх виявлення та попередження у наш час набирає все більшої актуальності, через велику кількість атак, як на промислових гігантів, так і на рядових користувачів мережі Інтернет [54, с. 30, 31]. Україна поступово нагромаджує важливий досвід у захисті власної ІТ-інфраструктури від кіберзагроз сучасності та протидії проявам кібертероризму. Утім протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об’єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче [78, с. 5]. Нині для України питання кібербезпеки, нарощування потенціалу кібермогутності стоять на порядку денному [38, с. 119]. Вітчизняні реалії кібербезпекової сфери свідчать про низку важливих проблем, що заважають створити ефективну систему

протидії загрозам у кіберпросторі, доходить висновку С. Х. Барегамян [11, с. 24]. Питання їх вирішення тим більше актуалізується з початком російської гібридної війни, де кіберагресія є однією з її визначних складових. Не можна заперечувати, що за таких умов Україні необхідно самостійно шукати шляхи і механізми забезпечення кібербезпеки від сучасних загроз, які постають [38, с. 119]. А для цього критичній оцінці підлягає сучасний стан забезпечення кібербезпеки з виділенням проблем, вирішення яких сприятиме досягненню стану кібербезпеки.

Актуальним для України питанням на сьогодні є відсутність чи не конкурентоспроможність вітчизняних програмних продуктів та використання закордонної бази. Як вказують з цього приводу М. М. Присяжнюк та Є. І. Цифра, Україна все ще залишається вразливою (особливо її телекомунікаційна складова), не в останню чергу через надмірно широке впровадження західних програмних продуктів і використання матеріально-технічної бази іноземного виробництва. Необхідним є створення національної операційної системи (принаймні для використання у системі органів державної влади, хоча для такого переходу до програмного забезпечення з відкритим кодом є і суттєві зауваження з боку ключових вітчизняних безпекових організацій), відновлення вітчизняних потужностей з виробництва матеріально-технічної телекомунікаційної бази (особливо для потреб закритих відомчих інформаційних систем), стимулювання з боку держави створення національного антивірусу [142, с. 66]. Підтримуючи позицію науковців, зауважимо, що для вирішення вказаної проблеми необхідним є вирішення питання оплати праці фахівців сфери у державному секторі та її конкурентоздатності з приватним, що сприятиме вирішенню проблеми кваліфікованих кадрів.

Це означає, що значна вразливість інфосфери України через надмірну присутність у ній західних програмних продуктів (зокрема, фірми Microsoft) та використання матеріально-технічних засобів іноземного виробництва обтяжується деградацією науково-технічного потенціалу України,

нерозвиненістю національної інноваційної системи в інфосфері та низьким рівнем конкурентоспроможності в ній [78, с. 23]. Наразі найбільш кваліфіковані спеціалісти з досвідом роботи приймають пропозиції переїзду за кордон через більш сприятливі умови праці та вищу оплату, що беззаперечно відзначається не тільки на якості та кількості вітчизняних продуктів, але і на ефективності функціонування національної системи кібербезпеки.

Аналізуючи дану проблему фахівці доходять висновку, що протистояти фізичному руйнуванню технічних засобів, дезорганізації роботи інформаційних систем і мереж, порушенню функціонування об'єктів нападу, а також протиправній діяльності соціальних інженерів в умовах інтенсифікації кібервтручань з дня на день стає все важче. Одна з головних причин цих негараздів полягає у відчутній нестачі професіоналів з інформаційної та кібербезпеки, здатних: 1) відшукувати, збирати або добувати інформацію про ІТ-системи й мережі протиборчих сторін, а також про технології та засоби їхнього впливу на власну інфосферу; 2) виявляти ознаки стороннього кібервпливу й моделювати можливі ситуації такого впливу, прогнозуючи відповідні наслідки; 3) протидіяти несанкціонованому проникненню протиборчих сторін у власні ІТ-системи й мережі, забезпечуючи стійкість їхньої роботи, а також відновлення нормального функціонування після здійснення кібернападів тощо [78, с. 5]. При цьому складнощами з кадровим наповненням [11, с. 24] не вичерпуються проблеми організації і діяльності системи кібербезпеки України. До вад її функціонування відносять відсутність загальнонаціональних міжвідомчих координаційних структур, що могли б узгоджувати та координувати діяльність різних силових відомств під час розслідування злочинів у кіберпросторі (співпраця реально існує не на чітко визначеному, а швидше, міжособистісному рівні, а отже, є уразливою) [11, с. 24]; дефіцит щодо методичного забезпечення та кадрового наповнення відповідних структурних підрозділів, відсутність чіткого усвідомлення ролі та значення

кібербезпекової складової в системі забезпечення національної безпеки держави [78, с. 16]. До названого переліку доцільно додати і недосконаліть нормативно-правового забезпечення.

Враховуючи сучасний стан та проблеми кібербезпеки в Україні до пріоритетів України у забезпеченні кібербезпеки пропонують відносити: розвиток інформаційної інфраструктури держави; розвиток мережі реагування на комп'ютерні надзвичайні події (CERT – Computer Emergency Response Team - команда реагування на комп'ютерні надзвичайні події), розвиток спроможностей правоохоронних органів щодо розслідування кіберзлочинів, забезпечення захищеності об'єктів критичної інфраструктури, державних інформаційних ресурсів від кібератак, створення системи підготовки кадрів у сфері кібербезпеки для потреб органів сектору безпеки і оборони, розвиток міжнародного співробітництва у сфері забезпечення кібербезпеки, інтенсифікацію співпраці України та НАТО, зокрема в межах Трастового фонду НАТО для посилення спроможностей України у сфері кібербезпеки [51, с. 249-250]. Також для попередження кіберзлочинів, слід погодитись, необхідно постійно проводити моніторинг інформаційних загроз, ґрунтовні дослідження функціонування та розвитку кіберзлочинності. Не останнє місце також повинно займати спеціалізоване правове виховання суб'єктів інформаційного обороту та користувачів комп'ютерної техніки [54, с. 30, 31]. Окрім названих напрямків окремим аспектом доцільно визначати формування культури та проведення інформаційно-пропагандистської кампанії про значущість проблематики кібербезпеки держави за допомогою: 1) активного інформування про кібернетичні втручання і загрози, про потенційні уразливості ІТ-систем і мереж, а також способи їх компенсації; 2) розширення співпраці державних органів з ІТ-компаніями, некомерційними організаціями з метою популяризації та впровадження на практиці безпечної поведінки в кіберпросторі; 3) стимулювання заходів боротьби з кіберзлочинністю і кібертероризмом, кібершпіонажем і кіберактивізмом; 4) підвищення рівня безпеки електронних

послуг, що надаються державою власному населенню; 5) організації профілактичної роботи з потенційними жертвами кіберзлочинів, керівниками малого і середнього бізнесу [78, с. 19].

Враховуючи вищевикладене, доходимо висновку, що кіберпростір як цілком відмінне від фізичного простору середовище має специфіку при реалізації в ньому суспільних відносин. Віртуалізація зв'язків та комунікацій суб'єктів права має ряд позитивних наслідків (швидкість зв'язку, можлива відсутність фізичного контакту, глобальність мережі Інтернет, зв'язок з будь-якої точки світу тощо), але при цьому є передумовою для виникнення нових складів правопорушень, які будуються на специфічних ознаках кіберпростору. А тому з використанням кіберпростору постало питання кібербезпеки як певного стану його захищеності від реальних і потенційних загроз; охорони та захисту важливих інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища.

Цей стан досягається через діяльність по забезпеченню кібербезпеки, яка має вигляд заходів різнорідного характеру суб'єктів національної системи кібербезпеки, та суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки. Практика забезпечення ними кібербезпеки в Україні викриває ряд проблем, які за напрямками вирішення можна згрупувати у наступні групи: 1) підвищення рівня оплати праці як передумова вирішення кадрового питання сфери; 2) розробка вітчизняного програмного та матеріально-технічного забезпечення; 3) інформування про стан кібербезпеки, кіберзлочинність всіх зацікавлених суб'єктів; 4) налагодження координації та взаємодії суб'єктів забезпечення кібербезпеки на партнерських засадах як на національному. Так і на міжнародному рівнях; 5) моніторинг кіберзагроз, кібератак та кіберінцедентів як основи для попередження правопорушень, розробки методологічних рекомендацій по забезпеченню кібербезпеки, моделювання та прогнозування кібератак, виявлення та нейтралізації кіберзагроз;

6) удосконалення нормативно-правового регулювання питань забезпечення кібербезпеки.

1.2. Органи Національної поліції України як суб'єкт забезпечення кібербезпеки

Органи національної поліції України згідно норм Закону України «Про основні засади забезпечення кібербезпеки України» [151] входять до основних елементів національної системи кібербезпеки, яку Україна наразі активно формує відповідно світовим тенденціям організації кіберзахисту. Як вказує С. В. Демедюк, ураховуючи сучасні тенденції у сфері адміністративно-правового та організаційного забезпечення кібербезпеки на міжнародній арені протидії загрозам у кіберпросторі та зміни внутрішньої кібернетичної політики національної безпеки провідних держав світу, а також посилення механізмів і компонентів кібербезпеки, більшість країн світу активно модернізують власні сектори безпеки відповідно до викликів сучасності, особливо зважаючи на потенціал використання кіберпростору в злочинних намірах [64, с. 144]. Адже на сьогоднішній день провідні держави світу та суспільство в цілому все більшою мірою покладаються і, відповідно, залежать від безперешкодного функціонування кіберпростору. Для цього модернізація відбувається паралельно з активним реформуванням управлінських структур, впорядкуванням нормативного поля, що має забезпечити цілісність державної політики в даній сфері, активною роз'яснювальною роботою серед населення щодо небезпек кіберзагроз, збільшенням чисельності підрозділів, зайнятих у системі кіберзахисту, розробленням кіберзброї та проведенням пробних військово-розвідувальних акцій у кіберпросторі, посиленням контролю за національним інформаційним простором (способами доступу, контентом тощо) [11, с. 23]. Водночас, формування системи кібербезпеки для використання кіберпростору в інтересах людини, держави, суспільства є вирішальним фактором.

Від її визначення до втілення на практиці її функціонування система кібербезпеки є тим вирішальним фактором, діяльність якого є передумовою досягнення стану захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору. Як вказують М. М. Присяжнюк та Є. І. Цифра, Україна потребує створення адекватної системи безпеки у світі, де виклики національній безпеці все частіше набувають рис, що відмінні від традиційних загроз. Активність з боку провідних держав світу в кіберпросторі, глибинні зміни відношення до внутрішньої інформаційної політики та формування потужних транснаціональних злочинних груп, що спеціалізуються на злочинах в кіберпросторі, обумовлюють необхідність вироблення рекомендацій щодо коротко- та довгострокових пріоритетів трансформації вітчизняного безпекового сектора [142, с. 65]. Не можна заперечувати, що цілком природно постала необхідність контролю та подальшого врегулювання відповідних взаємовідносин, а отже, і невідкладного створення надійної системи кібернетичної безпеки. Натомість відсутність такої системи може призвести до втрати політичної незалежності будь-якої держави світу, бо йтиметься про фактичний програш нею змагання невійськовими засобами та підпорядкування її національних інтересів інтересам протиборчої сторони. Оскільки саме ці обставини відіграють останнім часом важливу роль у геополітичній конкуренції більшості країн світу, то забезпечення кібербезпеки та злагоди в кіберпросторі стає головним завданням нашої інформаційної епохи [78, с. 4] як частини національної безпеки.

Враховуючи той факт, що система національної безпеки є багатокомпонентною, В. А. Ліпкан та І. В. Діордіца вбачають необхідність в існуванні спеціальної підсистеми, мета функціонування якої полягала б у забезпеченні функціонування та розвитку цієї системи, тобто у забезпеченні життєздатності її системоутворюючих елементів, зокрема національних інтересів людини, суспільства, держави. Науковці ведуть мову про систему забезпечення національної безпеки та національну систему кібербезпеки

[109, с. 174]. І одразу звертаємо увагу на розбіжність підходів до формування категорій.

Система забезпечення національної безпеки ставиться поряд з національною системою кібербезпеки, під якою законодавець розуміє сукупність суб'єктів забезпечення кібербезпеки та взаємопов'язаних заходів різної спрямованості щодо регулювання кіберпростору (ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» від [151]). Однак, аналіз останнього визначення з точки зору тих складових, які визначаються структурними елементами національної системи кібербезпеки, вказує на доцільність використання конструкції «національна система забезпечення кібербезпеки» для позначення тієї структури, яка наведені у вказані статті. Певні суб'єкти та здійснювані ними заходи характеризують діяльнісний підхід до формування поняття, а тому доцільно використовувати і дефініцію (конструкцію), яка б позначала певні дії з боку визначеної системи. Такі дії, як свідчить міжнародний досвід, можуть охоплювати реалізацію конструктивних заходів щодо формування виваженої державної інформаційної політики, створення надійного захисту об'єктів критичної інформаційної інфраструктури та вітчизняного сегмента кіберпростору, інтеграцію до світових систем колективної безпеки [110, с. 51].

Якщо змінити підхід до поняття, закріпленого у ч. 1 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [151], то постає питання категорії національної системи кібербезпеки. Відповідне визначення можливо надавати, виходячи з поняття системи управління, де суб'єкт управляння пов'язується зв'язками впливу на об'єкт управління, отримуючи від останнього зворотній зв'язок. Суб'єкт державного управління не може існувати без відповідних керованих об'єктів, і тільки разом вони утворюють систему управління, доводить І. П. Ковалевич. Така система, як вважає науковець, повинна охоплювати: організацію і функціонування керуючої системи; зв'язки керуючої системи з керованими об'єктами;

структуру керованої системи і безпосередньо сприймають державно-управлінський вплив або беруть участь у його формуванні [91].

Таким чином, національну систему кібербезпеки, як нам видається, доцільно розуміти як сукупність всіх компонентів, за допомогою яких досягається стан захищеності життєво важливих інтересів людини і громадянина, суспільства та держави під час використання кіберпростору, за якого забезпечуються сталий розвиток інформаційного суспільства та цифрового комунікативного середовища, своєчасне виявлення, запобігання і нейтралізація реальних і потенційних загроз національній безпеці України у кіберпросторі – тобто кібербезпека (п. 5 ч. 1 ст. 1 Закону України «Про основні засади забезпечення кібербезпеки України» [151]).

До таких компонентів доцільно, на наш погляд, віднести: 1) суб'єктів та здійснювані ними заходи (система забезпечення кібербезпеки), 2) об'єкти кібербезпеки та кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів, 3) норми права, що є основою для забезпечення кібербезпеки через встановлення зв'язків між суб'єктом та об'єктом: прямих та зворотних.

Зв'язки у кожній країні між суб'єктами та об'єктами відрізняються залежно від тих цінностей, які проголошені в конкретній державі в якості принципів її функціонування. М. В. Гребенюк вказує, що кожна країна світу вибирає власну модель розбудови національної системи кібербезпеки. Наприклад, у міжнародному форматі науковець виділяє три основні моделі правового врегулювання поширення інформації в мережі Інтернет. 1. Тотальний, жорсткий контроль держави над мережею Інтернет (наприклад, КНР). 2. Відповідальність провайдера за будь-які дії користувача (наприклад, у Франції провайдери зобов'язані надавати відомості про авторів сайтів на вимогу третіх осіб; ще з 1978 року існує спеціальний орган (Національна комісія інформатики і свобод), який зобов'язаний контролювати, щоб інформація в мережі не порушувала права і свободи людини). 3. Звільнення провайдера від відповідальності в тому разі, якщо він виконує певні умови, пов'язані з характером надання послуг і взаємодії із суб'єктами

інформаційного обміну. Так, у Німеччині відповідальність провайдерів за розміщення нелегального контенту на Інтернет-ресурсах, що знаходяться в їх мережі, настає лише в разі, якщо вони самі є власником інформації або свідомо поширювали її з посиланням на інші джерела. Така модель також активно використовується в Японії [55, с. 203-204].

Повертаючись до складових національної системи кібербезпеки України, які на сьогодні визначені в Законі України «Про основні засади забезпечення кібербезпеки України», звертаємо увагу на належність всіх перерахованих в якості основних суб'єктів до числа органів держави: Державна служба спеціального зв'язку та захисту інформації України, Національна поліція України, Служба безпеки України, Міністерство оборони України та Генеральний штаб Збройних Сил України, розвідувальні органи, Національний банк України [151]. І при цьому відведення ролі координатора дій національної системи кібербезпеки з усіма суб'єктами, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки (ч. 4 ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» [151]), Раді національної безпеки і оборони України, що також є органом держави при цьому при Президентові України (ч. 1 ст. 1 Закону України «Про Раду національної безпеки і оборони України» [152]). Така позиція законодавця не в повній мірі відповідає викликам та загрозам, які на сьогодні постають перед системою забезпечення кібербезпеки; не в повні мірі враховує потреби всіх учасників відносин у кіберпросторі; не забезпечує ефективну взаємодію та співпрацю законодавчо виділених основних суб'єктів забезпечення кібербезпеки (які у підсумку представляють державу) з іншими суб'єктами забезпечення кібербезпеки, до числа яких входять чисельні громадські структури, що основною метою діяльності мають забезпечення кібербезпеки, та ті суб'єкти, що через здійснювану ними діяльність забезпечують кібербезпеку, хоча проголошують інші основні завдання та мету свого утворення (наприклад, отримання прибутку, надання адміністративних послуг тощо).

І от роль вказаних суб'єктів у забезпеченні кібербезпеки зростає, а про ефективність взаємодіє наразі не йдеться. Здійснивши ґрунтовне дослідження адміністративно-правового регулювання кібербезпеки України І. В. Діордіца обґрунтовує, що кібернетична функція держави через власну іманентну організаційну природу має реалізовуватися в рамках сформованої та ефективно функціонуючою національної системи кібербезпеки із залученням всіх центральних органів виконавчої влади, недержавних, в тому числі волонтерських, організацій кожного окремого суб'єкта кібербезпекових правовідносин [71, с. 11]. Одним із ключових питань організації ефективної роботи національних систем кібербезпеки науковець визначає налагодження взаємодії між компетентними державними органами, які є суб'єктами кібернетичної безпеки, та здійснення координації з такої діяльності [109, с. 178-179]. Для цього одним із принципів забезпечення кіберб.езпеки в Україні підп. 4 ч. 1 ст 7 Закону України «Про основні засади забезпечення кібербезпеки України» визначено державно-приватну взаємодію, широку співпрацю з громадянським суспільством у сфері кібербезпеки та кіберзахисту, зокрема шляхом обміну інформацією про інциденти кібербезпеки, реалізації спільних наукових та дослідницьких проектів, навчання та підвищення кваліфікації кадрів у цій сфері [151].

Як вказує І. О. Валюшко, наявність ефективної мережі громадських структур стає за сучасних умов однією з умов забезпечення національної безпеки. Однак наука в Україні до цього часу комплексно не досліджувала недержавну систему безпеки як громадський механізм, а громадські об'єднання - як суб'єкти забезпечення національної безпеки держави. Сама державна система та бюрократія не дозволяють державним структурам бути настільки мобільними, оперативними та використовувати соціальні мережі як патріотичні хакерські організації. У сучасних умовах громадські об'єднання, як невід'ємний елемент громадянського суспільства, є повноцінним учасником процесу забезпечення інформаційної безпеки України. Взаємодія

між громадським сектором та державними інститутами є важливим аспектом безпекової політики [38, с. 118, 123].

Однак, закріплення певного принципу ще не означає його реалізації. І на сьогодні до числа головних проблем забезпечення кібернетичної безпеки в Україні науковці відносять відсутності належної координації діяльності відповідних відомств, а отже, і неузгодженості дій зі створення окремих елементів системи кібербезпеки, відсутність загальнонаціонального координаційного центру, здатного узгоджувати й координувати діяльність правоохоронних органів, силових структур і відомств щодо протидії реальним загрозам інформаційному і кіберпростору України та керувати проведенням комплексних навчань із забезпечення кібернетичної безпеки держави в інфосфері на кшталт навчань «Cyber Storm», які проводяться в США, і/або «Cyber Europe», що проводяться в ЄС» [78, с. 23]. Отже, необхідним є забезпечення належної координації дій усіх заінтересованих суб'єктів під час запровадження інструментів забезпечення та організації кібербезпеки; удосконалення інституціонального механізму формування, координації та здійснення контролю за виконанням завдань розбудови кібернетичного суспільства [63, с. 122]. В цьому аспекті цілком справедливо до числа напрямків розвитку кібербезпеки відносять реалізацію механізмів партнерства держави, бізнесу й громадян у сфері кібербезпеки за рахунок: 1) упровадження механізмів обміну інформацією державних ситуаційних центрів і центрів реагування на прояви стороннього кібервпливу з представниками бізнесу та громадського суспільства; 2) підвищення ефективності взаємодії провайдерів інтернет-послуг та користувачів в аспекті інформування про кібервтручання і загрози, потенційні уразливості ІТ-систем і мереж; 3) організації співпраці державних і бізнесових інституцій, а також окремих громадян у питаннях розроблення сучасних програмно-апаратних засобів забезпечення кібербезпеки [78, с. 20-21]. І для виконання вказаного доцільним для організації є центр взаємодії та координації, що об'єднував би всіх вказаних суб'єктів.

Враховуючи викладене, як поняття національної системи кібербезпеки з точки зору закріпленого у законодавстві підходу до його формування потребує критичної оцінки, так і підхід до обмеження основних суб'єктів забезпечення кібербезпеки та суб'єкту координації виключно інституціями держави доцільний для перегляду з точки зору необхідності врахування потреб всіх суб'єктів забезпечення кібербезпеки в Україні (згідно ст. 5 Закону України «Про основні засади забезпечення кібербезпеки України» – це міністерства та інші центральні органи виконавчої влади; місцеві державні адміністрації; органи місцевого самоврядування; правоохоронні, розвідувальні і контррозвідувальні органи, суб'єкти оперативно-розшукової діяльності; Збройні Сили України, інші військові формування, утворені відповідно до закону; Національний банк України; підприємства, установи та організації, віднесені до об'єктів критичної інфраструктури; суб'єкти господарювання, громадяни України та об'єднання громадян, інші особи, які провадять діяльність та/або надають послуги, пов'язані з національними інформаційними ресурсами, інформаційними електронними послугами, здійсненням електронних правочинів, електронними комунікаціями, захистом інформації та кіберзахистом [151]). У сучасному варіанті організації структури системи існує проблема ефективності координації та взаємодії не тільки щодо основних суб'єктів забезпечення кібербезпеки національної системи кібербезпеки з іншими суб'єктами, які реалізують відносини у кіберпросторі, але і між собою.

Як вважає І. В. Діордіца, розв'язання основних завдань кібербезпеки неможливе без створення міжвідомчого структурного органу, який на постійній основі забезпечував би координацію діяльності певних відомств, правоохоронних і силових структур України з питань забезпечення кібернетичної безпеки. Кібератака 27 червня 2017 року на Україну довела неефективність діяльності Національного координаційного центру кібербезпеки, поставила питання не про демагогічні та популістські формування недієздатних центрів / органів, а про формування відповідно до

національних інтересів національної системи кібербезпеки, власне, як на те вказується безпосередньо в Стратегії кібербезпеки України [70, с. 111]. Додаємо, що забезпечення координації на постійній сонові потребують не тільки вказані науковцем органи. Питання забезпечення безпеки знаходить прояв у діяльності як державних структур, так і недержавного сектору.

Отже, вирішенням проблеми може стати, з одного боку, центр координації та взаємодії національного рівня, що охоплював би представників всіх зацікавлених сторін (включаючи «недержавних» суб'єктів), з іншого, створення на рівні кожного суб'єкта забезпечення кібербезпеки одиниці, відповідної за координацію та взаємодію.

Запропоновані напрямки досліджень задля здійснення подальшого розвитку національної системи кібербезпеки України не впливають на вже на сьогодні визначене місце Національній поліції України в якості основного суб'єкту забезпечення кібербезпеки залишить незмінним. Вони розроблені в якості перспектив підвищення ефективності діяльності кожного суб'єкта забезпечення кібербезпеки окремо та при цьому у взаємодії між собою як єдиної системи, мета якої у вигляді кібербезпеки в Україні та за її межами. І останнє уточнення має важливе значення для розуміння ролі Національної поліції для забезпечення кібербезпеки в якості одного з основних елементів національної системи кібербезпеки. Адже адміністративно-правовий статус вказаного суб'єкту забезпечення кібербезпеки пов'язується з поняттям кіберзлочинності.

Як вказує Г. В. Шевчук, заходи боротьби з кіберзлочинністю повинні мати сьогодні комплексний характер та бути спрямованими на мінімізацію ризиків віртуальних загроз та на підвищення засобів і способів захисту у віртуальному просторі. У вказаних процесах кіберполіція стає центральним суб'єктом боротьби з кіберзлочинністю [215, с. 249]. Значення Національної поліції у цьому аспекті полягає у створенні умов розвитку безпечного середовища життєдіяльності, як основи безпеки на території України [14], шляхом захисту прав і свобод людини і громадянина, інтересів суспільства і

держави від злочинних посягань у кіберпросторі. Це означає, що метою створення кіберполіції є організація ефективної протидії проявам кіберзлочинності та забезпечення дієвого впливу на оперативну обстановку в зазначеній сфері [65, с. 89].

Як пояснюють С. В. Демедюк та В. В. Марков, кіберзлочинність є новітнім соціальним явищем, що активно поширюється по всьому світу [65, с. 88]. Кіберзлочинність не є традиційним злочином, а відносно молодим явищем, яке пов'язується із появою та поширенням глобальної мережі Інтернет, - доходить висновку С. А. Буяджи. 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 [32, с. 13]. Під кіберзлочинністю розуміються кримінальні правопорушення, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, а також інші кримінальні правопорушення, учинені з їх використанням [65, с. 88].

Дослідник С. В. Демедюк зазначає, що за своєю сутністю кіберзлочини є транскордонними, і тому міжнародні організації закликають держави до співпраці з іншими зацікавленими сторонами розробляти дієві механізми адміністративно-правового регулювання у сфері кібербезпеки, що передбачає не лише розроблення та прийняття необхідного законодавства, а й проведення спільних розслідувань зазначених діянь з використанням існуючого міжнародного права [64, с. 144]. Вказана мета обумовлює завдання всіх структурних елементів національної системи кібербезпеки, серед яких до числа основних віднесено Національну поліцію.

Для протидії кіберзлочинності та виконання інших функцій на вирішення поставлених завдань Національну поліцію уповноважено на здійснення заходів із запобігання, виявлення, припинення та розкриття

кіберзлочинів, підвищення поінформованості громадян про безпеку в кіберпросторі (під. 2 ч. 2 ст. 8 Закону України «Про основні засади забезпечення кібербезпеки України» [151]).

Реалізацію означених функцій покладено, в першу чергу, на спеціально створений з огляду на динаміку поширення комп'ютерних інцидентів теренами України структурний підрозділ. Зокрема, в липні 2010 року у структурі МВС України на базі Департаменту боротьби зі злочинами, пов'язаними з торгівлею людьми, утворено новий структурний підрозділ — Департамент боротьби з кіберзлочинністю та торгівлею людьми [78, с. 4] як структурний міжрегіональний територіальний орган поліції із широкими аналітичними та оперативно-тактичними повноваженнями, котрий спеціалізується на попередженні, виявленні, припиненні та розкритті кримінальних правопорушень, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), телекомунікаційних систем, комп'ютерних мереж і мереж електрозв'язку, а також інших кримінальних правопорушень, учинених з їх використанням [65, с. 89].

Враховуючи вищевикладене, доходимо висновку, що органи Національної поліції – це один з основних суб'єктів національної системи кібербезпеки, яку на сьогодні визначено як сукупність заходів та їх здійснювачів. І дане визначення потребує удосконалення в аспекті розмежування поняття системи кібербезпеки як системи управління та системи забезпечення кібербезпеки, структури яких відрізняються.

Роль Національної поліції у забезпеченні кібербезпеки визначається поняттям кіберзлочинності, що є новим видом правопорушень, виявлення, запобігання, припинення, протидія та розкриття яких визначає адміністративно-правовий статусу Національної поліції як суб'єкту забезпечення кібербезпеки. Однак не обмежує, оскільки провідне значення має уповноваження на інформування громадян про безпеку в кіберпросторі.

1.3. Нормативні засади забезпечення кібербезпеки Національною поліцією України та місце серед них адміністративно-правового регулювання

Нормативні засади забезпечення кібербезпеки Національною поліцією України формуються і змінюються в контексті розвитку нормативно-правового регулювання забезпечення кібербезпеки в цілому в державі. І цей процес на сьогодні активно відбувається під впливом зовнішніх та внутрішніх чинників. Як пояснює С. Х. Барегамян, Україна інтегрована у світовий кіберпростір і, відповідно, зазнає різних загроз і негативних впливів, пов'язаних з його розвитком (зокрема від наслідків суперництва США і ЄС з РФ та КНР), що гостро актуалізує проблеми кібербезпеки на загальнодержавному рівні. Це призводить до необхідності концептуального розуміння нової кібербезпекової реальності, впорядкування внутрішнього нормативно-правового поля, визначення повноважень відомств та організацій, задіяних у забезпеченні кібербезпеки держави і вирішення комплексу проблем, пов'язаних із розбудовою національної системи кібербезпеки [11, с. 23-24]. Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю [78, с. 4] серед яких першочергове значення надається розвитку нормативної бази.

До останнього часу про її існування можна було стверджувати лише з великою обережністю. Адже забезпечення кібербезпеки відбувалося на основі фрагментарно розміщених у різних актах нормах, якими було охоплено окремі аспекти організації забезпечення кібербезпеки, статусів суб'єктів, державної політики в цій сфері тощо.

Для Національної поліції в аспекті забезпечення кібербезпеки і на сьогодні мають значення Кримінальний кодекс України, Закони України «Про основи національної безпеки України», «Про інформацію», «Про державну таємницю», «Про захист інформації в інформаційно-

телекомунікаційних системах», «Про боротьбу з тероризмом», та інші. Однак, окремо акцентуємо увагу на прийнятті спеціального закону для кіберпростору. Зокрема, у 2017 році прийнято базовий Закон України «Про основні засади забезпечення кібербезпеки України» [151] на основі попередньо прийнятої Стратегії кібербезпеки України [153] як програмно-цільового акту, метою якого було визначено створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави.

Протягом останніх років Україна, як і більшість інших країн світу, робить впевнені кроки в напрямку розбудови інформаційного суспільства, забезпечення кібербезпеки та боротьби з кіберзлочинністю [78, с. 4]. Аналізуючи розвиток нормативних засад забезпечення кібербезпеки в Україні, І. О. Валюшко підсумовує, що законодавство у сфері кібербезпеки України в останні роки було переглянуто і трансформовано відповідно до нових викликів та загроз. Разом з тим науковець акцентує увагу, що побудова законодавства у такій важливій сфері, як кібербезпека, відбувається за принципом надолуження згаяного [38, с. 122-123], що впливає на ефективність роботи системи кібербезпеки, кібератаки якої в Україні мають прилади завершених дій з завданням збитків.

Дослідження генезису правового регулювання боротьби з кіберзлочинністю в Україні дозволило виділити С. А. Буяджи його наступні етапи: 1. Початковий етап (1991 рік – 2000 рік) – 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. 3. Етап відповідності правового регулювання боротьби з

кіберзлочинністю існуючим загрозам (2005 рік – до 27.06.2017 року) 4. Новітній етап (від 27.06.2017 року) – вірус «Petya.A» продемонстрував неготовність України до боротьби із сучасними кіберзагрозами. Тому, розпочатий етап науковець пов’язує із подальшою розробкою інструментів для боротьби із кібертерроризмом [32, с. 13]. І на цьому етапі не втрачає актуальності необхідність якісного оновлення та уточнення адміністративно-правового статусу такого елементу механізму адміністративно-правового регулювання забезпечення кібербезпеки в Україні, як правові засади регулювання відносини у сфері кібербезпеки, про що стверджує В. Ю. Степанов. Причинами для цього є дисбаланс між розвитком суспільних відносин у зазначеній сфері та розвитком права, з яких перші випереджають розвиток другого й виявляються тенденції формування так би мовити подвійного стандарту, коли закону необхідно дотримуватися, але тільки не в мережі [178, с. 138]. З цією позицією неможливо не погодитись.

Тим більше, що описана проблема стосується не тільки України. На сьогоднішній день кіберпростір, через певну новизну, все ще не повністю нормативно врегульований і на міжнародному рівні [142, с. 65] При цьому міжнародні організації визнають небезпеку кіберзлочинності та її трансграничний характер, обмеженість одностороннього підходу до вирішення цієї проблеми й необхідність міжнародної співпраці як у вжитті необхідних технічних заходів, так і у виробленні міжнародного законодавства [64, с. 144], яке б доповнювало вже напрацьовані нормативні засади.

Серед останніх для забезпечення кібербезпеки Національною поліцією України провідне значення мають такі міжнародно-правові угоди та договори, учасницею яких є Україна (Конвенція Ради Європи про кіберзлочинність від 23 листопада 2001 р., ратифікована 2005 р.; Міжнародна конвенція про боротьбу з фінансуванням тероризму від 9 грудня 1999 р., ратифікована 2002 р.; Конвенція про відмивання, пошук, арешт та конфіскацію доходів, одержаних злочинним шляхом від 8 листопада 1990 р.,

ратифікована 1997 р.; Конвенція ООН про боротьбу проти незаконного обігу наркотичних засобів і психотропних речовин від 20 грудня 1988 р., ратифікована 1991 р.; Резолюція Генеральної асамблеї ООН 57/239 “Елементи для створення глобальної культури кібербезпеки” від 20 грудня 2002 р. та ін. [63, с. 120]). Кожна з цих конвенцій має свій об’єкт регулювання, які в сукупності формують підґрунтя для боротьби з кіберзлочинністю, попередження кібератак та кіберінцедентів, визначення статусу суб’єктів забезпечення кібербезпеки на національному рівні та вирішення інших питань функціонування кіберпростору.

Зрозуміло, що всі вказані та інші міжнародні норми у сфері забезпечення кібербезпеки, згода на які надана Верховною радою України, а також всі норми щодо регулювання кіберпростору входять до нормативних засад забезпечення кібербезпеки Національною поліцією України. При цьому без норм, якими визначено правовий статус вказаного суб’єкта забезпечення кібербезпеки; стратегію створення умов для безпечного функціонування кіберпростору, його використання в інтересах особи, суспільства і держави; реформи державного управління характеристика засад не може вважатися повною.

І одразу зауважимо, що з числа перерахованих питань програмно-цільові норми, адміністративно-правовий статус, адміністративна відповідальність, норми щодо розвитку державного управління в Україні мають адміністративно-правову природу І від цього доцільно відштовхуватися при усвідомленні ролі адміністративного права серед нормативних засад забезпечення кібербезпеки Національною поліцією України.

Щодо програмно-цільових норм, то провідне значення у досліджуваній сфері має названа Стратегія кібербезпеки України [153], якою не тільки проголошено намір створення умов для безпечного функціонування кіберпростору, але і визначені основні терміни, поняття, напрямки розвитку. М. В. Гребенюк акцентує увагу на тому, що в кожній країні існує власне

національне тлумачення поняття «кібербезпека». Як наслідок, відрізняються і підходи до формування стратегій кібербезпеки. Проте керівні документи, що охоплюють питання кібербезпеки, як правило, передбачають: побудову державної системи управління у сфері забезпечення кібербезпеки; визначення відповідного механізму (в основному суспільно-державного партнерства), що дає змогу приватним і державним зацікавленим сторонам обговорювати проблеми забезпечення безпеки національних інформаційних інфраструктур; регламентацію стратегічних засад політики безпеки та регулюючих механізмів, чіткий розподіл завдань, прав і відповідаль ності для приватного і державного секторів (наприклад, обов'язкове інформування про кіберінциденти, оцінка загроз, розробка критеріїв віднесення об'єктів до критичної інформаційної інфраструктури тощо) [55, с. 203-204].

Адміністративно-правове регулювання забезпечення кібербезпеки Національною поліцією України включає Указ Президента України «Про виклики та загрози національній безпеці України у 2011 році», яким оформлення рішення про початок організації Єдиної загальнодержавної системи протидії кіберзлочинності [143].

Основу адміністративно-правового статусу Національної поліції в аспекті забезпечення кібербезпеки на сьогодні складають вищеназваний Закон України «Про основні засади забезпечення кібербезпеки України» [151] та Закон України «Про національну поліцію». Однак вказаними законами не обмежено кількість норм, на основі яких визначається адміністративно-правовий статусу суб'єктів забезпечення кібербезпеки, їх місце та роль у державному управлінні. Вказані питання визначаються Конституцією України, законами України та іншими підзаконними нормативно-правовими актами [217, с. 98], що описують коло повноважень, які обумовлені метою, завданнями, функціями конкретного суб'єкта, та забезпечені на реалізацію визначеними формами та методами діяльності на основі певних принципів.

Автор С. А. Буяджи підсумовує, що 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 [32, с. 107]. З уточненням, що в Конституції України однією з найважливіших функцій держави та справою всього Українського народу визначене забезпечення інформаційної безпеки, підтримуємо описану концепцію нормативних засад забезпечення кібербезпеки кіберполіцією України.

Аналізуючи нормативні засади забезпечення кібербезпеки Національною поліцією Г. В. Шевчук підсумовує, що практика реалізації її завдань та функцій показує неефективність деяких законодавчих норм. Спостерігаються прогалини у праві, що мають своїм наслідком неспроможність кіберполіції якісно та ефективно виконувати покладені на неї законом повноваження [215, с. 249]. Дослідник О. І. Гончаренко обґрунтовує, що в чинному законодавстві України існують прогалини щодо регулювання питань відносно протидії кіберзлочинності. Враховуючи викладене, автор пропонує створити умови для забезпечення постійного розвитку внутрішньодержавної правової бази у сфері обігу комп'ютерної інформації, яка повинна відповідати вимогам сьогодення та нормам міжнародного права. Особливої уваги О. І. Гончаренко вважає за доцільне приділяти удосконаленню та узгодженню кримінального та кримінально-процесуального законодавства, пов'язаного з кваліфікацією, виявленням та розслідуванням кіберзлочинів. Слід також вирішити правові питання з приводу розголошення провайдерами інформації про користувачів на запит

правоохоронних органів та можливості використання такої інформації у якості доказу [54, с. 31; 52, с. 348].

А от Г. В. Шевчук головним завданням визначає розробку та затвердження основного закону, який би регулював діяльність кіберполіції в Україні – Закону України «Про кіберполіцію України» [215, с. 249]. Не можна заперечувати, що 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 [32, с. 13]. В свою чергу, недосконаліть національного законодавства у сфері адміністративно-правового забезпечення та організації кібербезпеки України значно підвищує ймовірність реалізації кіберзагроз, що негативно впливає на загальний рівень національної безпеки України [63, с. 122].

Запропонований для прийняття нормативно-правовий акт з питань регулювання статусу кіберполції повинен, як вважає Г. В. Шевчук, відображати основні положення органу поліції та висвітлювати його особливості: 1) основні завдання кіберполіції України, серед яких можна виділити захист прав, свобод та законних інтересів осіб, протидію кіберзлочинності, а також подолання негативних тенденцій віртуального простору; 2) функції кіберполіції, які умовно можна було б поділити на зовнішні та внутрішні, оскільки кіберзлочинність не обмежуються територіальними межами країни, адже вона займає дещо іншу площину; 3) правову основу діяльності, 4) принципи, 5) повноваження, 6) компетенцію, 7) особливості моніторингу кіберзагроз, 8) механізми взаємодії з приватним сектором у створенні автоматизованих інформаційних систем та масивів даних для потреб оперативного реагування та розслідування кіберзлочинів [215, с. 249]. Аналізуючи дану пропозицію доцільно погодитись з науковцем

щодо необхідності чіткого окреслення виділених ним питань з уточненням про доцільність врегулювання також і питання виконання поліцією завдання підвищення поінформованості громадян про безпеку в кіберпросторі.

З цього приводу О. О. Грицун наголошує, що засоби протидії, санкції і навіть правоохоронні органи не можуть замінити засоби системної безпеки. Важливим кроком у підтримці ефективного кіберзахисту є застосування передового досвіду та навчання кожного, хто законно користується мережею, а також кібернетична профілактика. У цьому відношенні краще провести аналогію із зупиненням пандемії, ніж із злочином чи війною [56, с. 201]. А для України рівень усвідомлення загрози кіберзлочинів та їх небезпечності у суспільстві все ще є невисоким [32, с. 13-14].

Як ми зауважували вище, регулюванням адміністративно-правового статусу роль адміністративно-правового регулювання забезпечення кібербезпеки Національною поліцією не вичерпується. При розробці нових норм щодо адміністративно-правового статусу кіберполіції, рівно як і стосовно інших питань управління кіберпростором, необхідними для врахування здійснюваного у країні реформування системи державного управління, що відбувається в рамках поглиблення європейської інтеграції з метою набуття Україною членства в ЄС.

На сьогодні питання та поняття державного управління зазнає змін у світлі виведення на перший план сервісної функції держави, перехід від концепції управління людьми до обслуговування громадянського суспільства, від традицій «владного розпорядництва» до «надання послуг» громадянам та інших приватних осіб [16, с. 510]. Відповідна реформа має багатоетапний характер і до сьогоднішнього дня ще не завершена, охоплюючи забезпечення функціональної типологізації центральних органів виконавчої влади, виключення функцій надлишкового державного регулювання, усунення дублювання функцій і повноважень органів виконавчої влади, організаційне розмежування регулятивних, правозастосовних, контрольно-наглядових функцій і функцій з управління

об’єктами державної власності, проведення оптимальної деконцентрації та децентралізації владних повноважень органів виконавчої влади в різних сферах і галузях господарства країни, а також законодавче забезпеченням функціонування цих органів [21, с. 10]. І ці зміни не можуть бути не враховані при розвитку нормативних засад забезпечення кібербезпеки Національною поліцією, що є органом виконавчої влади, органом публічної влади, правоохоронним органом.

Як найперше в цьому аспекті доцільним є прийняття закону про публічну службу як поняття об’єднуючого службу в органах держави та службу в органах місцевого самоврядування. Ми навмисне уникаємо поняття державної служби, оскільки його зміст хоч і визначено на законодавчому рівні, але закріплення вузького обсягу (обмеження органами виконавчої влади, апаратами органів влади) як в Законі 1993 року [145] так і у прийнятому у 2015 році [144] гостро дискутується представниками науки адміністративного права [12, с. 10]. Тим більше, що у п. 17 ч. 2 ст. 3 Закону України «Про державну службу», чітко зазначено, що зі сфери його дії виключено осіб рядового і начальницького складу правоохоронних органів та працівників інших органів, яким присвоюються спеціальні звання, якщо інше не передбачено законом [144].

Не використовуємо ми і поняття органів влади, оскільки конституційний поділ її на гілки передбачає виділення законодавчої, виконавчої та судової, що ставить питання місця в механізмі держави органів з контрольними функціями на повноваженнями, які недостатньо підстав відносити до вказаних гілок.

Від так доцільним вважаємо об'єднання під одним терміном «публічна служба» муніципальної служби та служби в органах держави [175, с. 630], що повинно знайти втілення у прийнятті відповідного закону «Про публічну службу». В цьому законі повинні бути встановлені принципи, мета, завдання, обмеження та інші єдині питання організації та діяльності органів публічної влади, до числа яких повинна бути віднесена і Національна поліція.

Враховуючи викладене, доходимо висновку, що на сьогодні нормативні засади забезпечення кібербезпеки Національною поліцією України розвиваються у контексті формування кібербезпекового законодавства, законодавства про публічну та державну службу в рамках реформування державного управління та формування категорії публічного адміністрування.

Доцільним для прийняття є спеціальний нормативно-правовий акт про кіберполіцію, яким би було докладно врегульовано статус відповідного міжрегіонального територіального органу поліції, включаючи принципи організації та діяльності, мету, завдання, повноваження, компетенцію, особливості умов та підстав прийняття на службу, відповідальність та інші питання адміністративно-правового статусу органу та його службовців.

1.4. Поняття та елементи адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції

Питання адміністративно-правового статусу суб'єктів права вже неодноразово ставало предметом ґрунтованих досліджень, що втім не вирішило однозначно ані проблему його поняття, ані структуру його складових. Хоча дані питання є базовими в теорії адміністративного права, а від їх вирішення залежать подальші напрямки досліджень, досконаліть правового регулювання організації та діяльності суб'єктів адміністративного права, а отже, ефективність виконання ними своїх повноважень як частини правового статусу конкретних осіб.-*

Термін правовий статус застосовується доволі широко, але при цьому, як вказує В.В. Макарчук, не має однозначного застосування в юридичній літературі, законотворчій та правозастосовчій практиці, тому трактується по-різному. Визначення «статус» використовується в різних словосполученнях: «юридичний статус», «правовий статус», «соціальний або фактичний статус». По-перше, категорія «правовий статус» нерозривно пов'язана з доктриною природного права; по-друге, постійно розвиваються уявлення

наукової спільноти про зміст основних прав і свобод особи; по-третє, права і свободи особи вийшли за межі внутрішньої компетенції держави, стали предметом міжнародного захисту. В нормативних актах, теоретичній та галузевій літературі, юридичних словниках широке застосування і визнання набув термін «правовий статус», що відповідає загальним вимогам, які встановлені правилами юридичної техніки (терміни повинні бути загальновизнаними, мати стійким характером, мати широке застосування) [111, с. 20]. В цілому категорія правового статусу складна і збірна, яку використовують для розкриття всього комплексу зв'язків суб'єкта права [41, с. 115] та нормативного закріплення основних принципів взаємодії особи та держави. Він є системою еталонів, зразків поведінки суб'єктів, які, з одного боку, захищаються державою, а, з іншого – схвалюються суспільством [185, с. 78].

Адміністративно-правовий статус відноситься до числа спеціальних. У попередньому підрозділі ми встановили, що норми адміністративного права відіграють провідну роль для організації діяльності Департаменту кіберполіції України як суб'єкта адміністративного права, наділеного владними повноваженнями. Принципи організації і діяльності, мета та завдання кіберполіції, компетенція, повноваження, форми і методи їх здійснення, відповідальність – це ті питання, які врегульовано нормами адміністративного права.

А тому постає декілька питань: які з названих категорій як визначених нормами адміністративного права входять до числа складових адміністративно-правового статусу Департаменту кіберполіції України? Яким чином статус органу держави, окремого службовця вказаного підрозділу відрізняється від адміністративно-правового статусу громадянина Україна? Адже кожна особа у суспільстві виконує багато ролей, кожна з яких пов'язується з певним колом прав та обов'язків, які перетинаються і доповнюють один одного в рамках конкретних індивідуальних статусів.

Поняття «правовий статус» – явище об'єктивної дійсності, що аж ніяк не характеризує суб'єкта права як учасника правовідносин, а скоріше, є середовищем, у якому суб'єкти права набувають ознак і стають суб'єктами правовідносин. Правовий статус особи існує безвідносно до конкретної особи. Людина ще не народилася але правовий статус громадянина об'єктивно вже існує [197, с. 68-69]. Аналізуючи різноманіття статусів І. Г. Орловська доходить висновку, що кожен громадянин наділений не тільки загальним правовим статусом, але також має можливість стати носієм комплексу спеціальних прав та обов’язків (правовий модус особи), що передбачає набуття громадянином спеціального адміністративно-правового статусу. Загальний адміністративно-правовий статус громадян доповнюється, залежно від соціальної ролі індивідуального суб’єкта, спеціальними адміністративно-правовими статусами [130, с. 205-206]. Якщо проаналізувати викладені положення щодо видів статусів, то вчена виділяє загальний правовий статус, відносить адміністративно-правовий статусу до числа спеціальних, але при цьому розрізняє загальний і спеціальний адміністративно-правовий статуси.

І така концепція має підстави для існування, оскільки адміністративно-правовими нормами визначаються права та обов’язки, і окрім цього – ряд повноважень як частина компетенції певних органів держави чи місцевого самоврядування. Таким чином, виділяються притаманні всім суб’єктам адміністративного права обов’язки та права, та поряд з цим – обумовлені зайняттям певної посади повноваження, належність яких конкретній особі може впливати і на її загальний правовий статус і на загальний адміністративно-правовий в аспекті обмежень та заборон, обумовлених специфікою виконуваної службової діяльності.

В цілому обмеження чи заборона означає відсутність можливості реалізувати певне право суб’єктом у зв’язку зі зміною його статусу [183, с. 639], через введення певних виключень, додаткових обов’язків, покарань, призупинення засобів захисту і подібних вимог, які спрямовують поведінку

суб'єкта у певному напрямі [116, с. 4]. В цьому аспекті доречною є позиція, що діяльність поліції із забезпечення верховенства права повинна включати в себе два різні, але взаємопов'язані обов'язки: забезпечувати дотримання офіційних законів, належним чином прийнятих державою, що включає забезпечення загального стану публічного спокою, та пов'язаний із цим обов'язок суворо обмежуватися власними визначеними повноваженнями, утримуючись від будь-яких свавільних дій і дотримуючись особистих прав і свобод представників громадськості. Верховенство права передбачає не тільки, що робиться, але і те, як це робиться. Виконуючи свої обов'язки, поліція повинна дотримуватись індивідуальних прав громадян, включаючи права людини і свободи людини, і не вчиняти свавільних або протиправних дій. Це є основоположним для розуміння верховенства права і, отже, для значущості і для мети діяльності поліції в демократичній державі [176, с. 25].

Для забезпечення вказаного статус ряду посад правоохоронних, органів виконавчої влади, місцевого самоврядування та інших уповноважених на виконання функцій органів місцевого самоврядування чи держави органів в структурі статусу окрім повноважень в якості окремих елементів включає обмеження та заборони, які є частиною статусу і спрямовані на попередження використання службових повноважень або становища та пов'язаних з цим можливостей з метою одержання неправомірної вигоди для себе чи інших осіб (ст. 22 Закону України «Про запобігання корупції» [146]) службовцями, які обіймають відповідні посади. Не можна заперечувати, що правові обмеження встановлюються для правового стримування протизаконного діяння як умови для задоволення інтересів контрсуб'єкта і громадських інтересів в охороні і захисті [183, с. 639]. Для цього правові обмеження можуть мати вигляд заборони реалізації (мають абсолютний характер) чи обмеження реалізації конкретних прав, являючи можливість їх реалізації з дотриманням визначених умов, що встановлюються з метою попередження правопорушень, які пов'язані з виконанням службових завдань. Правові обмеження виникають одночасно із вступом посадової

особи у службово-правові відносини та діють до моменту їх припинення [226, с. 13-14].

Отже, основою адміністративно-правового статусу Департаменту кіберполіції України є його повноваження як частина компетенції, доповнені обмеженнями та заборонами задля вирішення питання законного використання владних повноважень, посадового становища та інших особливостей статусу, обумовлених виконанням функцій держави. Повноваження, як нам видається, доцільно пов'язувати з поняттям спеціального адміністративно-правового статусу Департаменту кіберполіції України.

В цьому аспекті можливо розмежувати повноваження як частину спеціального адміністративно-правового статусу та права і обов'язки як частину загального адміністративно-правового статусу. Н. В. Загородня під адміністративно-правовим статусом громадянина України пропонує розуміти комплекс прав і обов'язків, передбачених нормами адміністративного права. Вчена уточнює, що не всі права, які регламентовано законодавством, характеризують адміністративно-правовий статус; до них відносяться ті, що передбачені нормами адміністративного права та реалізуються у взаємовідносинах з органами публічної влади. До обов'язків, які характеризують адміністративно-правовий статус, відносять тільки ті, що обумовлюються виникненням взаємовідносин з органами публічної влади [75, с. 77]. Хоча при цьому доцільно враховувати, що поняття повноважень формується через категорії прав та обов'язків.

Так, за визначенням В. В.Березі, Департамент кіберполіції Національної поліції України задля виконання поставлених перед ним завдань реалізує комплекс визначених на нормативно-правовому рівні функцій. Разом із тим задля того, аби реалізувати ту чи іншу функцію, Департамент кіберполіції повинен бути наділений відповідним обсягом повноважень. При цьому, розкриваючи сутність повноважень Департаменту кіберполіції як суб'єкта протидії кіберзлочинам, В. В. Береза не може

оминути увагою такі поняття, як «право» та «обов'язок». Право як одна зі складових частин повноважень Департаменту кіберполіції – це закріплена на нормативно-правовому рівні, забезпечувана й гарантована державою міра можливої поведінки даного органу, яку він використовує з метою протидії кіберзлочинності. Обов'язок науковець пропонує розуміти як встановлену на нормативно-правовому рівні міру необхідної поведінки, якої має дотримуватися Департамент кіберполіції в процесі протидії кіберзлочинності [13, с. 30, 33, 34] Водночас, різниця понять повноваження та право, і обов'язки дозволяє не тільки виділяти загальний та спеціальних адміністративно-правовий статус, але і розділити статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції, статус посади та статут службовця, який обіймає конкретну посаду в Департаменті.

Тепер переходимо до визначення складових адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції.

Якщо до основних елементів адміністративно-правового статусу громадянина України відносять правосуб'єктність (правоздатність, дієздатність, деліктоздатність), права, обов'язки та юридичну відповідальність [75, с. 77], то для характеристики структури адміністративно-правового статусу органу держави доцільно, по-перше, використовувати іншу термінологію, по-друге, кількість складових адміністративно-правового статусу – збільшити.

Щодо термінології, то до числа складових адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції відносимо замість прав та обов'язків повноваження, відмежовуючи дане поняття від категорії компетенції.

Повноваження та компетенція – це: 1) поняття не є тотожними чи взаємозамінними; 2) вони повинні використовуватися в теорії кримінального процесу (як і в практиці законотворення) суворо згідно з їхнім призначенням;

3) ці поняття необхідно чітко розмежовувати за змістом, значенням, структурою логічно пов'язаних їхніх внутрішніх елементів та за функціональним призначенням [132, с. 289]. Повноваження як соціальне явище – це володіння правами і обов'язками членів (члена) суспільства, переданих суб'єкту відносин в порядку та у спосіб, визначений соціальними правилами і нормами з метою реалізації в особистих або спільних інтересах особи делегувальника і можуть включати в себе право розпорядження її цінностями, право на загальнообов'язковій основі залучати до виконання суспільних доручень, та застосовувати у випадках, передбачених правилами суспільного життя, заходи примусу [53, с. 148]. Повноваження закріплюються нормами права та зумовлені предметом відання конкретного суб'єкта права, являючи в кінцевому підсумку коло прав та обов'язків (правообов'язків), встановлене для виконання конкретних дій та прийняття відповідних рішень, обумовлених функціями та випливаючих із завдань, що стоять перед ним. Вони випливають із нормативно визначених цілей діяльності суб'єкта та визначають його правове положення, статус в системі органів державної влади, будучи критерієм розмежування повноважень цих органів [132, с. 289]. Отже, повноваження – це основа адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції.

Звертаємо увагу, що у ст. 18 Закону України «Про Національну поліцію» [149], встановлено основні обов'язки поліцейського, а у ст. 23 цього ж Закону визначені основні повноваження поліції.

Встановлюючи компетенцію кожної інституції держава здійснює поділ владних повноважень [24, с. 21], що разом і відповідальністю та предметом відання (функціональне призначення) пропонують визначати складовими структури категорії компетенції [105, с. 14]. Повноваження, як вважають Д. І. Голосніченко та І. П. Голосніченко, має системні та функціональні зв'язки з органами держави, через них здійснюється делегування виборцями

права на управління державою справами суспільства, ці елементи системи є невід'ємною складовою компетенції органів виконавчої влади [53, с. 148].

При цьому, слід погодитись, що у понятті компетенції державної інституції виявляється спеціальна правосуб'єктність державної інституції як колективного суб'єкта правовідносин [24, с. 21], яку доцільно додати до числа елементів адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції. При цьому слід розуміти, що правосуб'єктність державних органів є спеціальною і залежить виключно від тих повноважень та функцій, які для них визначив законодавець, обмежується тими цілями і завданнями, заради яких вони створюються, а самі державні органи зобов'язані діяти в її межах [224, с. 81].

Щодо інших складових статусу, то загалом кількість його елементів відрізняється у трактуванні різних науковців. Як пояснюють О. М. Гумін та Є. В. Пряхін, не дивлячись на численні наукові дослідження із питань адміністративно-правового статусу, єдиного розуміння цього поняття не сформовано. Однак це має важливе науково-практичне значення, особливо з огляду на реформаційні процеси, що зараз відбуваються в Україні [59, с. 32]. Слід розуміти, що кількість складових адміністративно-правового статусу залежить від пов'язаної категорії: це статус індивіда, статус посади, органу держави тощо.

Як вказує В. В. Макарчук, спочатку термін «правовий статус» розроблявся теоретиками права стосовно питання про права і свободи особи, потім він став використовуватися щодо юридичних осіб, публічно-правових утворень, включаючи державу, інших галузях [111, с. 20] Адміністративно-правовий статус індивіда включає позицію обмеження його елементів правами, свободами та обов'язками [75, с. 77]. Наприклад, правовий статус індивіда, який відображає особливості соціальної структури суспільства, рівень демократії та стан законності, як вважають О. В. Зайчук та Н. М. Оніщенко, виражається у юридичній формі – у формі прав, свобод та

обов'язків. З цієї позиці правовий статус як юридична категорія не лише визначає стандарти можливої та необхідної поведінки, що забезпечують нормальну життєдіяльність соціального середовища, а й характеризують реальну взаємодію держави та особи [185, с. 78]. Аналогічну позицію щодо складових категорії правового статусу виказують і стосовно службовців.

Наприклад, О. В. Литвин пропонує адміністративно-правовий статус державного службовця розуміти як визначений чинним законодавством перелік суб'єктивних прав, юридичних обов'язків, гарантій їх реалізації, а також обмежень, котрі у своїй сукупності забезпечують реалізацію державним службовцем повноважень у рамках функцій та завдань державної служби [108, с. 10]. Однак, коли мова іде про адміністративно-правовий статус органу, то даних складових навряд буде достатньо для здійснення повної характеристики та формування цілісного уявлення про його правове положення.

А тому доцільними для розгляду є пропозиції в структуру правового статусу включати такі елементи як: правові норми, які встановлюють даний статус, правосуб'єктність, громадянство, правові принципи, юридичні гарантії (в тому числі і юридичну відповідальність) [197, с. 46-47; 41, с. 115], вимоги, що висуваються до кандидатів на службу [100, с. 54], порядок формування та припинення діяльності; компетенцію (функції та повноваження); принципи організації та діяльності [224, с. 80], найменування посадової особи, її місце в ієрархії посад; ранги і спеціальні звання; умови прийому на службу та порядок її проходження; посадові права й обов'язки; функції і повноваження, правові форми і методи їх реалізації; службову дисципліну; заохочення і відповідальність; умови служби; пільги, гарантії і компенсації [162, с. 84-86], завдання, які вирішуються згідно з посадою; порядок взаємовідносин за посадою [97, с. 21] тощо.

Щодо правових норм, які встановлюють певний статус, то їх віднесення до структури статусу має підстави з огляду на поняття правового

статусу як категорії, яка описує правове становище особи на підставі норм права.

Щодо громадянства та вимог, які висувають для кандидатів на посади в Департамент кіберполіції України**,** то дані фактори є передумовою набуття статусу, якщо мова іде про службовців. Якщо розглядати категорії в якості ймовірних складових адміністративно-правового статусу Департаменту кіберполіції України, то поняття громадянства як зв'язок індивіда з певною державою не доцільно розглядати в якості складових статусу юридичної особи**.**

Щодо спеціальних вимог до кандидатів на службу в поліції, то такі вимоги можуть бути висунуті до конкретних посад (наприклад, ч. 7 ст. 15 ,ч. 5 ст. 21 Закону України «Про Національну поліцію» [149]) чи мати вигляд загальних умов вступу на службу в поліцію (ст. 49 цього ж Закону). Їх дотримання є юридичним фатом, без якого розгляд кандидатур на службу в поліції не розглядається. Однак, слід звернути увагу,що законодавець вживає категорію «умови вступу на службу», що вказує на передування певних фактів набуттю статусу за посадою, чи статусу поліцейського. А тому вказані категорії доцільно визначати передумовами набуття статусу, не включаючи їх до його структури.

Якщо дану концепцію перевести у площину юридичної особи, то питання стосуються порядку утворення та припинення юридичної особи як елементів правового статусу. Коли мова іде про індивідів, то для них вимоги на службу можливо залишити поза межами правого статусу службовців. Але коли мова іде про статуси посад та юридичних осіб, то питання доцільно досліджувати окремо.

Досліджуючи питання правового статусу суду О. М. Юхимюк доходить висновку, що його ключовими структурними є: правові принципи організації та діяльності судів; правосуб'єктність судів; форми та методи їх діяльності; гарантії діяльності судів; порядок їх утворення та припинення діяльності [224, с. 80]. Хоча дослідження здійснене стосовно іншого органу держави,

загальну концепцію елементів правового статусу можливо використати в якості прикладу.

Отже, утворення Департаменту кіберполіції України є тим юридичним фактом, що є підставою набуття статусу. І здійснення відповідної процедури обов'язково має наслідком отримання мети та завдань, набуття ним повноважень тощо. Рівно як і припинення юридичної особи характеризує процедуру позбавлення певної юридичної особи повноважень. Від так принципи служби в поліції, порядок формування та припинення Департаменту кіберполіції України як міжрегіонального територіального органу поліції доцільно включити в число елементів його адміністративно-правового статусу.

Юридичні гарантії в якості елементу статусу будемо розглядати окремо від відповідальності, оскільки перші, як ми вважаємо, є елементами структури адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції. Доцільно лише погодитись з уточненням, що будучи переведеними у сферу права, гарантії набувають форми відповідних суб'єктивних прав того суб'єкта – функціонування, якого вони забезпечують. Отже, з формально-юридичної точки зору, юридичні гарантії нічим не відрізняються від суб'єктивних прав суб'єкта права, реалізацію яких вони покликані забезпечити. Більш того, провести чітку межу між власне суб'єктивними правами та суб'єктивними правами-гарантіями досить часто дуже складно, тому що одні і ті ж суб'єктивні права в одній сфері суспільних відносин, будучи гарантованими правами, в іншій сфері самі є гарантіями [141, с. 91-92]. Таким чином, гарантії у структурі статусу мають вигляд певних прав, а тому їх можна не виносити в якості окремого елементу загального адміністративно-правового статусу індивіда. Водночас, якщо до структури спеціального адміністративно-правового статусу включено поняття повноважень в якості його основи, то гарантії, пільги, компенсації та правові обмеження доцільно розглядати в якості окремих елементів.

Аналіз Закону України «Про Національну поліцію» [149] дозволяє встановити, що законодавець закріплює обов'язки поліцейських та повноваження Національної поліції. З цього приводу наведемо позицію О. В. Литвина, який виділяє особливості та характерні відмінності адміністративно-правового статусу службовців правоохоронних органів**,** до яких віднесено: переважаючий характер обов'язків у порівнянні з їх правами; права державних службовців правоохоронних органів є засобом реалізації покладених на них обов'язків; можливість легального застосування адміністративного примусу до особи; наявність атестованих та вільнонайманих посад усередині правоохоронних органів; наявність певного переліку так званих «компенсуючих прав» переважно соціального характеру; в основному імперативний характер суспільних відносин всередині системи [108, с. 10]. Враховуючи викладене, гарантії та правові обмеження включаємо до елементів адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції.

А от щодо відповідальності, то дану категорію вважаємо доцільним залишити поза межами категорії правового статусу, виходячи з розуміння відповідальності продуктом прояву статусу та його наслідком у вигляді політичної та юридичної відповідальність службовців [108, с. 14].

Компетенцію доцільно віднести до структури правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції в якості функцій та предмету відання, відмежовуючи від поняття повноважень, про що ми зазначили вище. Компетенцію доцільно розуміти як предмет відання та функції. В свою чергу, функції – це основні напрями діяльності державних інституцій, спрямовані на виконання державою свого соціального призначення та реалізуються у безпосередній діяльності державних службовців [108, с. 14]. Функції, які здійснюються органами державної влади, є визначальними правовими категоріями у правозастосовній чи правоохоронній діяльності будь-якого державного органу. Здебільшого у науково-правових колах «функції» розглядають як

напрями діяльності, що визначені завданнями та цілями відповідного суб'єкта правовідносин, в яких відображено його сутність і призначення в державі та суспільстві загалом. Функції Департаменту кіберполіції – це визначені на нормативно-правовому рівні напрями діяльності, що зумовлені метою та завданнями в процесі здійснення своєї правоохоронної діяльності» [15, с. 66-67]. Поняття функцій потребує розгляду категорій форм і методів діяльності.

Правові форми і методи їх реалізації доцільно визначати частиною адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції, оскільки дані категорії характеризують зовнішній прояв функцій, являючи способи, засоби та прийми (методи) у сталих поєднаннях (форми) впливу суб'єктів на об'єкти управління, для досягнення цілей розвитку держави. Одним з ключових термінів даного визначення М. Н. Курко визначає «цілі» Тобто форми і методи виявляються обумовленими загальною системою відносин держави і суспільства в залежності від цілей держави. Методи проявляються та реалізується у відповідних формах, які, в свою чергу, обумовлюють вибір методів, через які реалізуються цілі держави. Цілі державної влади завжди є специфічними і здебільшого встановлюються самою державною владою, тоді як функції держави становлять універсальну систему, яка реалізується в діяльності будь-якої держави незалежно від форми політичного режиму чи форми правління [103, с. 39]. Отже, цілі та завдання Департаменту кіберполіції України як міжрегіонального територіального органу поліції також доцільно віднести до елементів його адміністративно-правового статусу.

Найменування є тією базовою категорією, яка ідентифікує юридичну особу та дозволяє зв'язати всі елементи статусу з конкретним суб'єктом права. Разом з місцем в структурі апарату та механізму держави найменування доцільне для включення до структури адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального

територіального органу поліції.

Враховуючи вище викладене, до структури адміністративно-правового статусу Департаменту кіберполіції України як міжрегіонального територіального органу поліції включаємо: порядок його утворення та припинення, найменування та місце в структурі апарату та механізму держави**;** правові норми, які встановлюють статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції; принципи служби в поліції; цілі та завдання; компетенцію (предмет відання та функції), повноваження; правові форми і методи їх реалізації; гарантії та правові обмеження.

Висновки до розділу 1

1. Кіберпростір – це нове середовище для встановлення зв'язків суб'єктів правовідносин, який відрізняється від фізичного рядом специфічних ознак: 1) виникає в результаті функціонування інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем ; 2) не має чітко визначених територіальних меж та кордонів (не може вважатися територією); 3) глобальність; 4) не передбачає фізичного контакту суб'єктів правовідносин, які можуть бути і не ідентифікованими; 5) комунікація за допомогою цифровізації зв'язків шляхом використання програмного та апаратного забезпечення на основі спеціальних протоколів.

2. Кібербезпека – це стан захищеності кіберпростору від реальних і потенційних загроз; охорони та захисту важливих інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища. Цей стан досягається через діяльність по забезпеченню кібербезпеки, яка має вигляд заходів різнорідного характеру суб'єктів національної системи кібербезпеки, та суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

3. Напрямками вирішення проблем забезпечення кібербезпеки Національною поліцією України доцільно визначити: 1) підвищення рівня оплати праці; 2) вирішення кадрового питання; 2) розробку вітчизняного програмного та матеріально-технічного забезпечення; 3) систематичне інформування про стан кібербезпеки, кіберзлочинність всіх зацікавлених суб'єктів; 4) налагодження координації та взаємодії суб'єктів забезпечення кібербезпеки на партнерських засадах як на національному, так і на міжнародному рівнях; 5) моніторинг кіберзагроз, кібератак та кіберінцедентів як основа для попередження кіберзлочинності, розробки методологічних рекомендацій по забезпеченню кібербезпеки, моделювання та прогнозування кібератак, виявлення та нейтралізації кіберзагроз; 6) удосконалення нормативно-правового регулювання забезпечення кібербезпеки, в тому числі доцільним для прийняття є спеціальний нормативно-правовий акт про кіберполіцію, яким би було докладно врегульовано статус відповідного міжрегіонального територіального органу поліції, включаючи принципи організації та діяльності, мету, завдання, повноваження, компетенцію, особливості умов та підстав прийняття на службу, відповідальність та інші питання адміністративно-правового статусу органу та його службовців; 7) подальший розвиток міжнародного співробітництва у сфері забезпеченні кібербезпеки, включаючи співпрацю України та НАТО.

4. Доцільними для розмежування є категорії національної системи кібербезпеки та системи забезпечення кібербезпеки, з яких першу доцільно розуміти як сукупність всіх компонентів, за допомогою яких досягається кібербезпека: 1) суб'єктів та здійснюваних ними заходів (система забезпечення кібербезпеки), 2) об'єктів кібербезпеки та кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів, 3) норм права, що є основою для забезпечення кібербезпеки через встановлення зв'язків між суб'єктом та об'єктом: прямих та зворотних.

5. Підхід до обмеження основних суб’єктів національної системи кібербезпеки та суб’єкту їх координації виключно інституціями держави доцільний для перегляду з точки зору необхідності врахування потреб всіх суб’єктів забезпечення кібербезпеки в Україні. Доцільним для організації є центр взаємодії та координації, що об’єднував би всіх суб’єктів забезпечення кібербезпеки на засадах партнерства.

6. Адміністративно-правовий статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції являє собою характеристику правового положення відповідного суб’єкту забезпечення кібербезпеки та включає наступні елементи: 1) порядок утворення та припинення, найменування та місце в структурі апарату та механізму держави; 2) правові норми, які встановлюють статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції; 3) принципи служби в поліції; 4) цілі та завдання; 5) компетенцію (предмет відання та функції), 6) повноваження; 7) правові форми і методи їх реалізації; 8) гарантії; 9) правові обмеження.

РОЗДІЛ 2
ЗАГАЛЬНА ХАРАКТЕРИСТИКА ОКРЕМИХ ЕЛЕМЕНТІВ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ В УКРАЇНІ

2.1. Завдання та функції Департаменту кіберполіції в Україні

В сучасних умовах розвитку інформаційних технологій, злочинність дедалі частіше набуває різних форм та використовує різні методи злочинної діяльності, саме тому протидія злочинам, що націлені на електронне управління, електронне банківське обслуговування, електронну комерційну діяльність тощо, є одним із чинників розбудови України як демократичної, правової держави з пануванням принципів законності та верхавенства права, а також дотримання прав людини й громадянина [14, с. 45].

Сучасні виклики і загрози, перш за все гібридні, обумовлені впливом комплексу соціально-демографічних, економічних, політичних, правових, психологічних і технологічних чинників, вимагають системного реагування, адекватної трансформації органів публічної влади, зокрема правоохоронних органів, серед яких чільне місце відводиться Національній поліції України. Роль останньої полягає у створенні умов розвитку безпечного середовища життєдіяльності, як основи безпеки на території України. Станом на сьогодні основні сподівання щодо забезпечення безпеки сучасного кіберпростору покладається на Департамент кіберполіції Національної поліції України як міжрегіональний територіальний орган зі статусом юридичної особи публічного права [14, с. 44; 179].

Зазначимо, що науково-теоретичне підґрунтя дослідження завдань та функції поліції як правоохоронного сервісного органу, в тому числі Департаменту кіберполіції України склали праці таких провідних вчених та науковців як: В. Б. Авер’янов, М. І. Ануфрієв, О. М. Бандурка, О. В. Батраченко, Д. В. Бахрах, О. К. Безсмертний, Ю. П. Битяк,

С. М. Бортник, В. М. Бурденюк, В. М. Гаращук, І. П. Голосніченко, В. Л. Грохольський, С. М. Гусаров, Д. С. Денисюк, О. І. Довгань, Є. В. Додін, І. В. Зозуля, С. В. Ківалов, О. М. Клюєв, В. К. Колпаков, А. Т. Комзюк, А. Є. Крищенко, А. М. Куліш, В. В. Маліков, Р. С. Мельник, Л. В. Могілевський, О. М. Музичук, Д. С. Припутень, О. С. Проневич, О. П. Рябченко, О. Ю. Салманова, О. Ю. Синявська, В. В. Сокуренко, В. А. Троян, В. В. Чумак, Д. В. Швець, В. І. Шамрай та інші.

Визначення завдань та функцій Департаменту кіберполіції Національної поліції України є важливою складовою визначення особливостей його діяльності та адміністративно-правового статусу. Адже успішне та ефективне виконання Департаментом кіберполіції Національної поліції України своїх повноважень залежить від чіткого законодавчого розуміння його завдань та функцій як базового елемента адміністративно-правового статусу будь-якого органу державної влади.

Слід зазначити, що поряд із значним використанням категорій «завдання» та «функції» у національному законодавстві, серед науковців наразі немає одностайного розуміння щодо визначення сутності вищевказаних категорій. Тому дослідження пропонуємо розпочати із визначення сутності та взаємозв’язку понять «завдання» та «функції».

Першочерговим слід наголосити, що у філософському значенні завдання – це не просто завдання, а «соціальне завдання», і воно витлумачується у цьому сенсі «як необхідність для суб’єкта (суспільства, соціальної спільноти, особи) здійснити у майбутньому визначену діяльність», а мета – як «ідеальний, насамперед, визначений результат людської діяльності, спрямований на перетворення дійсності відповідно до усвідомленої людиною потреби. Мета є безпосереднім внутрішнім спонукальним мотивом людської діяльності» [121, с. 51; 66, с. 100].

Зміст категорії «завдання» із тлумачної точки зору розглядається у кількох значеннях: 1) як наперед визначений, запланований для виконання обсяг роботи, справа; 2) настанова, розпорядження виконати певне

доручення; 3) мета, якої прагнуть досягти; 4) те, що хочуть здійснити [40, с. 378]. Загальнотеоретичне розуміння поняття «завдання» тлумачиться як питання, що потребує вирішення на підставі певних знань та роздумів [203, с. 328].

Досліджуючи сутність категорії «завдання» деякі дослідники (В. О. Климков, В. І. Щербина) визначають її як мету. Так, В. О. Климков стверджує, що завдання – це мета, досягнення якої є бажаним до відповідного моменту в межах періоду, на який розраховано управлінське рішення. Автор наголошує, що завдання вказують на мету організації, що піддається кількісній характеристиці [90, с. 99]. У свою чергу В. І. Щербина вказує, що завдання – це активізована, конкретизована та сформульована перед кимось або чимось мета (ціль) [219, с. 57].

На наш погляд ототожнення понять «завдання» та «мета» є помилковим, оскільки не дає повною мірою розкрити сутність та значення окреслених категорій. В даному контексті заслуговує на увагу позиція В. Б. Авер'янова, який наголошує, що цілі та завдання можна розглядати як уявлення про напрями й очікуванні результати управлінської діяльності. Відмінність між зазначеними поняттями полягає у ступені узагальнення результатів, що мають бути досягнуті в процесі управлінської діяльності – в цілях відтворюються більш триваліші та значущі, ніж у завданнях показники [3, с. 260].

Зазначимо, що завдання більшою мірою характеризують соціальне покликання, призначення того або іншого суб'єкта, вони ближче стоять до мети його утворення, одночасно є визначальними для функцій, тобто функції, які, безумовно, також свідчать про призначення суб'єкта, деталізують і конкретизують завдання, передбачають напрямки діяльності суб'єкта, в яких ці завдання виконуються [169, с. 169–170; 210, с. 224]. У зв'язку з цим варто погодитися з думкою Л. В. Коваля про те, що природним посередником між завданнями й очікуваним результатом (метою) управління

виступає управлінська функція як практична діяльність на шляху реалізації цих завдань [92, с. 22; 196, с. 13]

Досліджуючи феномен категорії «завдання» органу державної влади О. Г. Комісаров стверджує, що цілі можуть бути недосяжними на конкретний (запланований) момент, але наближення до них за цей час повинно відбуватися постійно. Проте завдання, на відміну від цілей, повинні бути здійсненними, хоча не завжди можливо вимагати їх здійснення. Поряд з цим розглядається ціль, якої ніколи не можна досягти, але до якої треба постійно наближатися, що отримала назву – ідеал [96, с. 90].

Завдання – це конкретизація шляхів, що є необхідними та достатніми для досягнення кінцевої мети утворення органу державної влади. Тобто завдання завжди виходять із мети та є своєрідним засобом її реалізації. У процесі постановки завдань в ціле зводяться бажане (чого хочемо досягти) і можливе (що для цього є). Тому для того щоб завдання мали сенс, вони повинні бути досяжними, але в той же час вимагають від органу максимальних зусиль. Завдання повинні бути зорієнтовані як на сьогодення, так і на майбутнє, оскільки вона задають орієнтири планованого періоду, а також пропонують стандарти, за якими в кінці певного періоду оцінюватимуться результати [198]. Завдання на думку Д. В. Мандичева, передбачають сталість змісту, незмінність [118, с. 118].

Відповідно до Закону України «Про Національну поліцію», до числа завдань поліції віднесені наступні:

1) забезпечення публічної безпеки і порядку;

2) охорони прав і свобод людини, а також інтересів суспільства і держави;

3) протидії злочинності;

4) надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги [149].

У свою чергу, враховуючи специфіку діяльності Департаменту кіберполіції Національної поліції України відповідно до положення «Про Департамент кіберполіції Національної поліції України», затвердженого наказом Національної поліції України, до числа завдань Департаменту кіберполіції Національної поліції України належать:

1) забезпечення реалізації державної політики у галузі протидії кіберзлочинності;

2) здійснення інформаційно-аналітичного забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до його компетенції;

3) формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп'ютерів), систем та комп'ютерних мереж і мереж електрозв'язку [147].

Враховуючи викладене, пропонуємо надати авторське визначення поняття «завдання Департаменту кіберполіції Національної поліції України», де останні являють собою визначені на нормативно-правовому рівні шляхи досягнення конкретної мети діяльності, а саме – реалізація державної політики у галузі протидії кіберзлочинності, інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до компетенції кіберполіції.

З урахуванням специфіки діяльності Департаменту кіберполіції Національної поліції України доцільним вбачаємо визначити власну класифікацію завдань кіберполіції на: загальні та спеціальні, та на завдання, що не пов'язані із державною таємницею та такі, що пов'язані зі державною таємницею. В той же час, слід визначити класифікації завдань поліції, що вже запропоновані представниками науки адміністративного права. Зокрема, В. В. Чумак виокремлює наступну класифікацію завдань поліції:

- загальні (стратегічні) завдання поліції: «підтримання безпеки, спокою, миру та порядку в суспільстві» (Данія); «забезпечення і зміцнення порядку та спокою в країні» (Мальта); «забезпечення миру в країні» (Кіпр); «підтримання миру й порядку та забезпечення безпечного соціального розвитку громадян, включаючи виконання загальних поліцейських обов'язків та забезпечення безпеки на дорогах» (Греція); «захист прав і свобод людини» (Литва);

- завдання у сфері забезпечення особистої та майнової безпеки: «захист власності, життя і особистої гідності громадян» (Словенія); «забезпечення особистої безпеки громадян, захист їх прав і свобод, законних інтересів» (Україна), «особистої та майнової безпеки громадян» (Білорусь), «гарантій особистої та громадської безпеки» (Латвія), «безпеки Папи Римського як у межах держави під час папських церемоній і прийомів, так і під час подорожей Італією та іншими країнами» (Ватикан);

- завдання у сфері захисту суспільства і держави від злочинних та інших посягань: «запобігання правопорушенням та їх припинення» і «виявлення і розкриття злочинів, розшук осіб, які їх вчинили» (Україна); «попередження і розкриття злочинів, затримання правопорушників» (Кіпр); «профілактика кримінальних злочинів та інших правопорушень» і «розслідування кримінальних злочинів і кримінальний розшук» (Латвія);

- завдання у сфері охорони публічного порядку: «охорона і забезпечення громадського порядку» (Україна), «охорона громадського порядку» (Білорусь), «забезпечення громадського порядку та безпеки» (Литва), «забезпечення громадського порядку, безпеки особистості та суспільства» (Киргизстан), «профілактика злочинів і захист держави та демократичного уряду в рамках конституційного поля, включаючи реалізацію політики у сфері громадської та державної безпеки» (Греція), «дотримання законності і підтримання громадського порядку» (Кіпр);

- завдання соціального (гуманітарного) характеру: участь у наданні соціальної та правової допомоги фізичним і юридичним особам (Україна,

Білорусь), надання допомоги у надзвичайних ситуаціях, зокрема якщо особа постраждала від протиправних діянь чи природних катаклізмів або перебуває у безпорадному стані (Литва);

- завдання особливого характеру: виконання завдань військового характеру під час проведення миротворчих операцій за кордоном (карабінери Італії); забезпечення безпеки кордону, повітряного простору, міжнародних аеропортів і залізниці, охорона офіційних осіб, федеральних будівель і дипломатичних місій (федеральна поліція Німеччини) тощо [210, с. 225-226; 157, с. 194].

Враховуючи викладене, до загальних завдань Департаменту кіберполіції Національної поліції України ми відносимо: забезпечення публічної безпеки та публічного порядку; охорона основоположних прав і свобод людини, а також інтересів суспільства і держави; протидія кіберзлочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

У свою чергу, до спеціальних завдань Департаменту кіберполіції Національної поліції України ми відносимо: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів [88].

До завдань, що не пов’язані із державною таємницею належать: формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Слід також, окремо визначити завдання Департаменту кіберполіції у сфері протидії злочинності та зокрема визначити на законодавчому рівні підслідність кіберзлочинів, вчинених у сфері використання комп’ютерів, систем та комп’ютерних мереж, мереж електрозв’язку, державних інформаційних ресурсів і об’єктів критичної інформаційної інфраструктури та суттєво підвищити відповідальність за втручання в їхню роботу за кіберполіцією України. На підставі викладеного пропонуємо наступну класифікацію завдань у сфері протидії злочинності у відповідності до кіберзлочинів, а саме: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); 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 (ст. 361-2); 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 (ст. 362); 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 (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) та деякі інші [98].

Зазначена класифікація завдань Департаменту кіберполіції Національної поліції України визначена на законодавчому сприятиме більш чіткій та послідовній їх реалізації та сприятиме визначенню нових функцій та

відповідно кола повноважень з метою забезпечення безпеки кіберпростору та прав громадян.

Таким чином, реалізація завдань Національної поліції в Україні означає, що поліцейська діяльність відбувається на основі закріплених у чинному законодавстві принципів з урахуванням сучасних тенденцій європейської інтеграції. Принципи як керівні ідеї, що покладені в основу функціонування кожного органу та підрозділу поліції, покликані сприяти подальшій розбудові поліції як інституту європейського зразка. Своєю чергою завдання поліції визначають засоби здійснення поліцейської діяльності, що базуються на відповідних принципах [216, с. 123].

У свою чергу, завдання тісно переплітаються із напрямками діяльності, його мають назву «функції».

Поняття функція з латинської мови «functio» означає «виконання» [201, с. 498]. Семантичне розуміння поняття «функція» передбачає наступні значення: 1) специфічна діяльність організму людини, тварин, рослин, їхній органів, тканин і клітин; 2) відправлення членами тіла своїх дій; 3) величина, що змінюється зі зміною незалежної змінної величини (аргументу); 4) позначення дій над кількістю [61, с. 824]; 5) явище, що залежить від іншого явища, є формою його виявлення та змінюється відповідно до його змін; 6) робота, кого-, чого-небудь, обов'язок, коло діяльності когось, чогось; 7) призначення, роль чого-небудь [40, с. 1552].

Визначаючи взаємозв'язок функцій та завдань державного органу Н. В. Лебідь зазначає, що функціям властиві безперервність і постійність, не обумовленість конкретними подіями і діями. У свою чергу завдання – мають тимчасовий характер і в процесі їх досягнення вони будуть або зняті, або змінені на нові. Тому в статусі державного органу чітке закріплення і розмежування функцій можливе і доцільне шляхом вказівки на завдання, поставлені перед ними. При цьому автор визначає функції як основні взаємопов'язані напрямки діяльності, що реалізуються як державним органом, так і його структурними підрозділами, посадовими особами і

службовцями задля досягнення загальної мети [107, с. 39]. У свою чергу дослідник Л. В. Коваль під функціями органу державної влади вбачає розуміти складові частини змісту його діяльності, що відображені у поставлених перед органом державної влади завданнях із забезпечення життєво важливих потреб керованого об'єкта і здійснюється шляхом реалізації покладених на нього повноважень [93].

Автор О. В. Пономарьов у своєму науковому дослідженні, що присвячене адміністративно-правовому статусу податкової міліції України надає наступне визначення функціям податкової міліції України – це основні напрями її діяльності, що спрямовані на вирішення поставлених перед нею завдань. Саме функції розкривають призначення і основний зміст діяльності податкової міліції України [140, с. 58]. Д. В. Мандичев визначає функції як основні взаємопов'язані напрямки діяльності, що реалізуються органом державної влади чи його посадовими особами для реалізації поставленої мети [117, с. 113]. В. В. Чумак зазначає, що відповідно до законодавства Республіки Естонії, функції Департаменту муніципальної поліції покликані підтримувати правопорядок та забезпечувати законність у місті та поліпшити службу загальної поліції [207, с. 140]. Функції, як вказує А. Є. Крищенко, охоплюють комплекс способів, методів, прийомів і дій, які забезпечують виконання певних завдань і досягнення цілі. Функції поліції реалізують уповноважені суб'єкти (посадові особи), які несуть юридичну відповідальність за обґрунтованість і законність конкретних дій [99, с. 125]. В. А. Троян під функціями Національної поліції України розуміє основні напрямки її діяльності, в яких відображено її сутність і призначення в державі та суспільстві в цілому [196, с. 16]. Л. В. Могілевський наголошуючи на значенні визначення функцій трудового права вказує, що якщо функції правових норм полягають у забезпеченні конкретизованого й деталізованого закріплення загальних масштабів (етапів) поведінки учасників трудових і тісно пов'язаних із ними відносин, їх прав, обов'язків та гарантій, то на інших, більш високих рівнях системи трудового права здійснюються функції,

які забезпечують юридичну узгодженість правового впливу, цілісне, єдине регулювання суспільно-трудових відносин [124, с. 90].

Слід окремо зазначити, що деякі науковці, зокрема Б. М. Лазарєв наголошують на розмежуванні функцій державного органу та функцій управління. Так, автор вказує, що між функціями управління в цілому та функціями, покладеними на конкретний орган існує зв'язок. Функції, що покладаються на конкретний орган є похідними від перших і закріплюються за ними владним, вольовим шляхом, причому завжди із вказівкою об'єкта, на який кожна функція спрямована. При визначенні компетенції органів управління необхідно, по-перше, своєчасно виявити об'єктивну потребу в тій чи іншій управлінській функції щодо застосування до тих чи інших об'єктів, а ще краще – передбачити виникнення таких потреб у майбутньому; по-друге, знаходити найкращі у конкретних умовах варіанти розподілу функцій між різноманітними органами; по-третє, закріплювати вказані варіанти шляхом видання відповідних правових актів, в результаті чого в державного органу виникає право та обов'язок виконувати ті чи інші управлінські функції стосовно відповідних об'єктів управління [104, с. 31]. Дослідник В. Я. Малиновський поняття «функція державного управління» розкриває як складові змісту управлінської діяльності, що характеризуються певною самостійністю, однорідністю, складністю та стабільністю владно-організуючого впливу суб'єкта управління, спрямованого на забезпечення життєво значущих потреб об'єкта управління. До числа ознак функцій державного управління автор відносить: обумовленість цілями управління; реалізація в процесі державно-управлінських відносин)взаємодія суб'єкта та об'єкта); об'єктивний характер; відносна самостійність та однорідність; безпосередня вираженість владно-організуючої сутності виконавчої влади; спрямованість на забезпечення життєво необхідних потреб об'єкта управління [114, с. 202].

Таким чином, функції Департаменту кіберполіції Національної поліції України пропонуємо визначити наступним чином, - це комплекс закріплених

на нормативно-правовому рівні адміністративних, оперативно-розшукових, нормотворчих, кадрових, інформаційних і профілактичних напрямів діяльності цього правоохоронного органу, виконання яких зумовлено завданнями у сфері протидії кіберзлочинності.

Щодо існуючих класифікацій функцій поліції, то, наприклад, комплексний аналіз теорії та практики поліцейської діяльності дозволив О. С. Проневичу виокремити наступні функції поліції: 1) адміністративну (адміністративно-виконавчу; виконавчо-примусову); 2) оперативно-розшукову; 3) кримінально-процесуальну (слідчу); 4) превентивно-соціальну (профілактичну (попереджувально-профілактичну), соціально-сервісну); 5) охоронну [158, с. 142–145]. Водночас, Д. С. Денисюк на підставі аналізу закону України «Про Національну поліцію» та постанови Кабінету Міністрів України «Про затвердження Положення про Національну поліцію» виокремлює такі функції поліції: 1) соціальну та сервісну; 2) превентивну та профілактичну, спрямовані на запобігання вчиненню правопорушень; 3) кримінально-процесуальну; 4) оперативно-розшукову; 5) дозвільну; 6) охоронну; 7) матеріально-технічного забезпечення; 8) міжнародного співробітництва; 9) інформаційного забезпечення; 10) науково-методичну; 11) кадрову; 12) соціально-правового захисту [67, с. 115–117; 196, с. 16].

У контексті досліджуваного питання варто зазначити, що поняття функції Департаменту кіберполіції Національної поліції України не отримало свого законодавчого закріплення. Водночас законодавство, що регламентує діяльність Департаменту кіберполіції Національної поліції України, зокрема, як правоохоронного органу застосовує термін «функції». Зокрема, згідно із статтею 3 Положення «Про Департамент кіберполіції Національної поліції України» на своєму веб-сайті Департамент кіберполіції розмістив перелік основних функцій. Департамент відповідно до покладених на нього завдань: 1) визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на запобігання та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; 2) у межах своїх

повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; 3) визначає основні напрями роботи і тактики оперативно-службової діяльності у сфері протидії кіберзлочинності; 4) уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, що становлять оперативний інтерес, зокрема об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем із метою запобігання, виявлення та припинення кримінальних правопорушень; 5) організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності, дотримання службової дисципліни, режиму секретності, участь у комплексних перевірках службової діяльності цих підрозділів, ужиття заходів щодо усунення виявлених недоліків; 6) за погодженням із керівництвом Національної поліції України ініціює проведення в установленому порядку комплексних інспектувань, контрольних та інших перевірок діяльності підпорядкованих підрозділів; 7) проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті; 8) забезпечує в порядку, передбаченому законодавством України, формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; 9) організовує виконання у межах компетенції доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій у кримінальних провадженнях; 10) за погодженням із керівництвом Національної поліції України організація проведення комплексних і цільових оперативно-профілактичних заходів на території держави чи окремих регіонів, зокрема, за участю правоохоронних органів інших країн; 11) у межах компетенції розробляє рекомендації для підвищення професійного рівня і

поінформованості органів Національної поліції України, а також громадськості про результати діяльності кіберполіції; 12) вивчає позитивний вітчизняний і зарубіжний досвід боротьби з кримінальними правопорушеннями у сфері протидії кіберзлочинності та вносить пропозиції керівництву Національної поліції України щодо його впровадження; 13) уносить в установленому порядку пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також бере участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері; 14) відповідно до чинного законодавства створює та забезпечує функціонування цілодобової контактної мережі для надання невідкладної допомоги під час розслідування злочинів, пов'язаних із комп'ютерними системами та даними, переслідування осіб, що обвинувачуються у вчиненні таких злочинів, а також збирання доказів в електронній формі; 15) забезпечує функціонування локальних експертних лабораторій ДКП та мобільних груп швидкого реагування, призначених для залучення до місць учинення кримінальних правопорушень, з метою зняття даних із носіїв інформації; 16) аналізує та систематизує дані про кримінальні правопорушення, учинені у сфері протидії кіберзлочинності та з використанням високих технологій, що надходять від громадян каналами кол-центрів, електронними листами та терміналами зворотного зв'язку; 17) відповідно до чинного законодавства збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях, оцінює результати за окремими показниками службової діяльності, надає, відповідно до законодавства України, звіти про результати роботи та відповідну інформацію керівництву Національної поліції України, МВС, органів державної влади з питань запобігання та протидії кіберзлочинам; 18) у межах компетенції налагоджує та підтримує взаємодію і партнерські відносини з органами державної влади, іншими правоохоронними органами, приватним сектором і правоохоронними

органами іноземних держав, міжнародними установами та організаціями у сфері протидії кіберзлочинності для ефективного виконання завдань ДКП, а також підвищення довіри населення до органів Національної поліції України; 19) забезпечує своєчасний розгляд звернень і запитів громадян, підприємств, установ, організацій із питань, віднесених до компетенції кіберполіції, контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду; 20) сприяє правильному підбору, розстановці, навчанню та вихованню кадрів Департаменту та підпорядкованих йому підрозділів; 21) бере участь в організації та проведенні навчальних і науково-практичних заходів із питань протидії кіберзлочинності (тренінгів, конференцій, семінарів тощо); 22) проводить заслуховування результатів роботи підрозділів, здійснює підготовку та подання керівництву Національної поліції України пропозицій щодо вдосконалення діяльності цих підрозділів, порушує питання щодо вжиття заходів дисциплінарного впливу та заохочення їх працівників; 23) здійснює інші повноваження відповідно до вимог чинного законодавства [147; 15, с. 68-69].

На підставі аналізу Закону України «Про Національну поліцію» [149] та Наказу Національної поліції України «Про Положення про Департамент кіберполіції Національної поліції України» [147] пропонуємо виокремлювати такі функції:

- адміністративна (наприклад, організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності);

- оперативно-розшукова (наприклад, у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; організовує виконання у межах компетенції доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій у кримінальних провадженнях);

- нормотворча (наприклад, уносить в установленому порядку пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також бере участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері);

- кадрова (наприклад, сприяє правильному підбору, розстановці, навчанню та вихованню кадрів Департаменту та підпорядкованих йому підрозділів);

- інформаційного забезпечення (наприклад, забезпечує в порядку, передбаченому законодавством України, формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях; забезпечує своєчасний розгляд звернень і запитів громадян, підприємств, установ, організацій із питань, віднесених до компетенції кіберполіції, контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду);

- превентивна та профілактична (наприклад, визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на запобігання та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, захисту і протидії кіберзагрозам у повсякденному житті).

Також, слід виокремити функції Департаменту кіберполіції Національної поліції України у сфері протидії кіберзлочинності, зокрема [202]:

1) визначає, розробляє та забезпечує реалізацію комплексу заходів, спрямованих на попередження та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності;

2) у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності;

3) уживає передбачених чинним законодавством заходів зі збирання й узагальнення інформації стосовно об'єктів, у тому числі об'єктів сфери телекомунікацій, інтернет-послуг, банківських установ і платіжних систем з метою попередження, виявлення та припинення кримінальних правопорушень;

4) організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;

5) проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, а також захисту та протидії кіберзагрозам у повсякденному житті;

6) забезпечує формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності;

7) організовує виконання, у межах компетенції, доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій та негласних слідчих (розшукових) дій у кримінальних провадженнях та інші.

Отже, наведені вище положення дають змогу визначити функції Департаменту кіберполіції Національної поліції України як комплекс закріплених на нормативно-правовому рівні адміністративних, оперативно-розшукових, нормотворчих, кадрових, інформаційних і профілактичних напрямів діяльності цього правоохоронного органу, виконання яких зумовлено завданнями у сфері протидії кіберзлочинності.

Таким чином, завдання та функції Департаменту кіберполіції Національної поліції України є важливою складовою визначення особливостей його діяльності та адміністративно-правового статусу, оскільки

ефективне виконання Департаментом кіберполіції Національної поліції України своїх повноважень залежить від чіткого законодавчого розуміння його завдань та функцій як базового елемента адміністративно-правового статусу будь-якого органу державної влади.

2.2. Права й обов'язки Департаменту кіберполіції в Україні

Протидія злочинам, що спрямовані на електронне управління, електронне банківське обслуговування, електронну комерційну діяльність та інші високотехнологічні галузі, є найважливішим фактором будівництва правової держави, утвердження принципу соціальної справедливості, захисту прав і свобод громадян. Департамент кіберполіції Національної поліції України задля виконання поставлених перед ним завдань реалізує комплекс визначених на нормативно-правовому рівні функцій. Разом із тим задля того, аби реалізувати ту чи іншу функцію, Департамент кіберполіції Національної поліції України повинен бути наділений відповідним обсягом прав та обов'язків. Ось чому визначення прав та обов'язків (повноважень) Департаменту кіберполіції Національної поліції України має одне з першорядних та прикладних значень, особливо в питанні з'ясування його адміністративно-правового статусу в цілому [13, с. 30-31].

Для надання авторського визначення поняття повноважень Департаменту кіберполіції Національної поліції України, а також встановлення їх конкретного обсягу перш за все необхідно з'ясувати сутність та ознаки досліджуваного терміну в загальнотеоретичному значенні. Так, семантично поняття «повноваження» у Великому тлумачному словнику сучасної української мови визначається як право, надане кому-небудь для здійснення чогось; права, надані особі або підприємству органами влади [40; 13, с. 32]. Авторський колектив шеститомної юридичної енциклопедії під поняттям «повноваження» пропонує розуміти сукупність прав та обов'язків державних органів і громадських організацій, а також посадових та інших осіб, закріплених за ними у встановленому законодавством порядку для

здійснення покладених на них функцій. Обсяг повноважень конкретних державних органів та їх посадових осіб залежить від їх місця в ієрархічній структурі відповідних органів [42, с. 39; 13, с. 36].

Так, досліджуючи природу прав, В. М. Корельський і В. Д. Перевалов зазначають, що право – це обумовлена природою людини і суспільства система регулювання суспільних відносин, що виражає свободу особистості і якій властиві нормативність, формальна визначеність у офіційних джерелах і забезпеченість можливістю державного примусу [184, с. 226]. Зазначимо, що, досліджуючи права фізичних та юридичних осіб, традиційно в теорії права виділяють право об'єктивне та суб'єктивне.

На думку О. Ф. Скакун, об'єктивне юридичне право – це система діючих в державі правових норм і принципів [166, с. 226–227]. Вони встановлені (або визначені) державою в ролі регулятора суспільних відносин, забезпечені нею [166, с. 226–227]. Термін «об'єктивне» означає, що вони отримали об'єктивацію в офіційних державних актах і тому незалежні від індивідуального інтересу (волі) та свідомості суб'єкта права [166, с. 226–227]. Суб'єкт вступаючи в суспільне життя, вже має справу з існуючими юридичними нормами, які виникли до нього і незалежно від нього [166, с. 226–227]. Об'єктивне юридичне право – це система загальнообов'язкових правил фізичної поведінки – соціальних норм, встановлених або санкціонованих державою, які виражають волю домінуючої частини соціально неоднорідного суспільства, спрямовані на врегулювання суспільних відносин відповідно до цієї волі, а також на задоволення загальносоціальних потреб, і забезпечуються державою [160]. Об'єктивні права надаються уповноваженими державними органами фізичним та юридичним особам на основі спеціально передбачених законом процедур за наявності відповідних на те підстав [1]. Представники юриспруденції наголошують, що, оскільки існують об'єктивні права, які проголошуються Конституцією та Законами України, то повинні існувати і суб'єктивні права, які має у своєму розпорядженні щодо інших осіб кожна

людина, і які вона має за будь-яких обставин, а тому і без будь-яких попередніх домовленостей [204, с. 30].

Відповідно, у приватних суб'єктивних правах можливості та вимоги суб'єкт здійснює за власною волею (бажанням). Як з цього приводу зауважує Г. Єллінека, це й становить ядро всього приватного права. Натомість публічні суб'єктивні права прив'язуються безпосередньо до особистості та є невід'ємними від неї. Приватноправові вимоги виникають із суб'єктивних прав, тоді як публічно-правові – із самої особистості [234, с. 59–61; 46]. Своєю чергою, А. Єлістратов зазначав, що суб'єктивні права – це можливість здійснювати юридичні акти [73, с. 15]. Б. Кістяківський вказує, що відокремлення права та суб'єктивних прав від держави дозволить правильно пізнати не лише їх, а й державу також. Саме відмова від юридично-догматичного підходу під час аналізу суб'єктивних публічних прав, на думку автора, дозволяє визнати їх правами фізичної та юридичної особи [87, с. 550–551].

В. В. Береза зазначає, що право як одна зі складових повноважень Департаменту кіберполіції – це закріплена на нормативно-правовому рівні, забезпечувана й гарантована державою міра можливої поведінки даного органу, яку він використовує з метою протидії кіберзлочинності [13, с. 33].

Відповідно до Положення про Департамент кіберполіції Національної поліції України працівники Департаменту кіберполіції Національної поліції України мають право:

– 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;

– здійснювати оперативно-технічні заходи за оперативно-розшуковими справами, що знаходяться в їх провадженні;

– в установленому порядку запитувати та отримувати від посадових осіб 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;

– користуватися в установленому законодавством порядку базами даних Національної поліції України, МВС та інших державних органів з питань, що належать до компетенції управління, а також мають інші права, передбачені законодавством [147].

Також, відповідно до Закону України «Про Національну поліцію», працівники Департаменту кіберполіції мають право:

1) здійснювати превентивну та профілактичну діяльність, спрямовану на запобігання вчиненню правопорушень;

2) виявляти причини та умови, що сприяють вчиненню кримінальних та адміністративних правопорушень, вживати у межах своєї компетенції заходів для їх усунення;

3) вживати заходів з метою виявлення кримінальних, адміністративних правопорушень; припиняти виявлені кримінальні та адміністративні правопорушення;

4) вживати заходів, спрямованих на усунення загроз життю та здоров'ю фізичних осіб і публічній безпеці, що виникли внаслідок учинення кримінального, адміністративного правопорушення;

5) здійснювати своєчасне реагування на заяви та повідомлення про кримінальні, адміністративні правопорушення або події;

6) здійснювати досудове розслідування кримінальних правопорушень у межах визначеної підслідності;

7) розшукувати осіб, які переховуються від органів досудового розслідування, слідчого судді, суду, ухиляються від виконання кримінального покарання, пропали безвісти, та інших осіб у випадках, визначених законом;

8) здійснювати провадження у справах про адміністративні правопорушення, приймати рішення про застосування адміністративних стягнень та забезпечує їх виконання;

9) доставляти у випадках і порядку, визначених законом, затриманих осіб, підозрюваних у вчиненні кримінального правопорушення, та осіб, які вчинили адміністративне правопорушення;

10) вживати заходів для забезпечення публічної безпеки і порядку на вулицях, площах, у парках, скверах, на стадіонах, вокзалах, в аеропортах, морських та річкових портах, інших публічних місцях;

11) регулювати дорожній рух та здійснює контроль за дотриманням Правил дорожнього руху його учасниками та за правомірністю експлуатації транспортних засобів на вулично-дорожній мережі;

12) здійснювати супроводження транспортних засобів у випадках, визначених законом;

13) видавати відповідно до закону дозволи на рух окремих категорій транспортних засобів; у випадках, визначених законом, видає та погоджувати дозвільні документи у сфері безпеки дорожнього руху;

14) вживавати всіх можливих заходів для надання невідкладної, зокрема домедичної і медичної, допомоги особам, які постраждали внаслідок кримінальних чи адміністративних правопорушень, нещасних випадків, а також особам, які опинилися в ситуації, небезпечній для їхнього життя чи здоров’я;

15) вживати заходів для визначення осіб, які не здатні через стан здоров’я, вік або інші обставини повідомити інформацію про себе; встановлювати особу за невпізнаним трупом;

16) забезпечувати безпеку взятих під захист осіб на підставах та в порядку, визначених законом;

17) у межах своєї компетенції, визначеної законом, здійснювати контроль за дотриманням вимог законів та інших нормативно-правових актів щодо опіки, піклування над дітьми-сиротами та дітьми, позбавленими

батьківського піклування, вживати заходів щодо запобігання дитячій бездоглядності, правопорушенням серед дітей, а також соціального патронажу щодо дітей, які відбували покарання у виді позбавлення волі;

18) вживати заходів для запобігання та протидії домашньому насильству або насильству за ознакою статі;

19) здійснювати охорону об'єктів права державної власності у випадках та порядку, визначених законом та іншими нормативно-правовими актами, а також брати участь у здійсненні державної охорони;

20) здійснювати на договірних засадах охорону фізичних осіб та об'єктів права приватної і комунальної власності;

21) здійснювати контроль за дотриманням фізичними та юридичними особами спеціальних правил та порядку зберігання і використання зброї, спеціальних засобів індивідуального захисту та активної оборони, боєприпасів, вибухових речовин і матеріалів, інших предметів, матеріалів та речовин, на які поширюється дозвільна система органів внутрішніх справ;

22) здійснювати у визначеному законом порядку приймання, зберігання та знищення вилученої, добровільно зданої або знайденої вогнепальної, газової, холодної та іншої зброї, боєприпасів, набоїв, вибухових речовин та пристроїв, наркотичних засобів або психотропних речовин;

23) здійснювати контроль у межах своєї компетенції, визначеної законом, за дотриманням вимог режиму радіаційної безпеки у спеціально визначеній зоні радіоактивного забруднення;

24) сприяти забезпеченню відповідно до закону правового режиму воєнного або надзвичайного стану, зони надзвичайної екологічної ситуації у разі їх оголошення на всій території України або в окремій місцевості;

25) виконувати в межах компетенції запити органів правопорядку (правоохоронних органів) інших держав або міжнародних організацій поліції відповідно до закону та міжнародних договорів України;

26) здійснювати оперативно-розшукову діяльність відповідно до закону;

27) вживати заходів для забезпечення публічної безпеки і порядку під час примусового виконання судових рішень і рішень інших органів (посадових осіб), а також вживає заходів, спрямованих на усунення загроз життю та здоров'ю державних виконавців, приватних виконавців та інших осіб, які беруть участь у вчиненні виконавчих дій, здійснює привід у виконавчому провадженні, здійснювати розшук боржника чи дитини у виконавчому провадженні у випадках, передбачених законом або рішенням суду.

28) забезпечувати інформування Комісії з питань осіб, зниклих безвісти за особливих обставин, про хід досудового розслідування, вживати заходів для розшуку осіб, зниклих безвісти, у тому числі осіб, зниклих безвісти за особливих обставин, для внесення даних до Єдиного реєстру осіб, зниклих безвісти за особливих обставин;

29) виявляти транспортні засоби особистого користування, тимчасово ввезені на митну територію України громадянами більш як на 30 діб та не зареєстровані в Україні у встановлені законодавством строки;

30) вживати заходів для виявлення неправомірного керування транспортними засобами, щодо яких порушено обмеження, встановлені Митним кодексом України, а саме: порушено строки їх тимчасового ввезення та/або переміщення в митному режимі транзиту; транспортні засоби використовуються для цілей підприємницької діяльності та/або отримання доходів в Україні; транспортні засоби передано у володіння, користування або розпорядження особам, які не ввозили їх на митну територію України або не поміщували в митний режим транзиту, а також заходів для виявлення неправомірного розкомплектування таких транспортних засобів [149].

Отже, права як складовий елемент адміністративно-правового статусу Департаменту кіберполіції Національної поліції України – це закріплена на нормативно-правовому рівні, забезпечувана й гарантована державою міра

можливої поведінки даного органу, яку він використовує з метою протидії кіберзлочинності.

Поряд із визначенням прав у Департаменту кіберполіції Національної поліції України наявне широке коло кореспондуючих їм обов'язків.

Традиційно пропонуємо розпочати дослідження з визначення категорії «обов'язок». У словниковій літературі вказується, що «обов'язок» – це те, що підлягає безумовному виконанню ким-небудь [170]. В. Н. Вітрук розглядає обов'язки як соціально можливу необхідність визначеної поведінки особистості, встановленої державою [44, с. 10]. Обов'язок, як вказується у юридичній літературі, – це міра суспільно необхідної поведінки людини, покликана разом і з правами і свободами забезпечувати баланс, стійкість і динамізм правового регулювання [131, с. 92]. Своєю чергою, В. В. Кравченко наголошує, що обов'язки – це об'єктивно обумовлена вимога до особи діяти чітко визначеним у законі чином або утримуватися від здійснення певних дій [123, с. 91].

Юридичні обов'язки – це передбачені законодавством вид і міра належної поведінки особи, що забезпечується державою. Сутність юридичного обов'язку полягає у тому, що він існує лише відповідно до суб'єктивного права і має здійснюватися в межах, встановлених законом і гарантованих державою [167; 131, с. 92–93]. Правник Ю. К. Толстой вказує, що юридичний обов'язок – це визначена законом міра належного, яка виражає обов'язок певної поведінки, яку вимагає уповноважена особа від іншого суб'єкта з метою задоволення її власного інтересу [193, с. 46]. Своєю чергою, Р. Р. Карімова зазначає, що юридичний обов'язок виникає з інтересу, є необхідною дією (як потенційною, так і реальною), еквівалентною правам і свободам, заснованою на державній необхідності, яка реалізується добровільно чи силою державного примусу на основі внутрішньої і (чи) юридичної відповідальності [80].

Юридичний обов'язок також визначають як закріплену в юридичних нормах і забезпечувану державою необхідність певної поведінки суб'єкта,

спрямованої на здійснення його відповідного основоположного обов'язку [161, с. 100]. М. І. Матузов зазначає, що суть юридичного обов'язку полягає в необхідності певної поведінки, зміст – у конкретних проявах цієї необхідності (вид, міра, межі, час тощо), а структура – у чотирьох елементному складі змісту [120, с. 162–163]. Дослідник О. Ющик, аналізуючи розуміння обов'язку в теорії права, вказує, що обов'язок є домінуючим у правовідносинах, оскільки від поведінки зобов'язаної особи залежить можливість реалізації права іншою особою. По-перше, зазначає науковець, правовий обов'язок є безпосереднім виразом правової сили суб'єктивного права; по-друге, суб'єктивне волевиявлення зобов'язаного індивіда, що надає задоволення суб'єктивному праву, стає формою прояву своєї протилежності – законності вимог праводомагання; по-третє, здатність індивідуальної поведінки задовольняти домагання інших суб'єктів надає суб'єктивному волевиявленню, втіленому у правовому обов'язку, безпосередньо суспільну форму. Перевага права над обов'язком, про що часто говориться в теоретичних працях, полягає, на думку О. Ющика, лише у тому, що суб'єктивне право виражає інтерес свого суб'єкта, а обов'язок є формою, що відображає відсутність власного інтересу суб'єкта [225, с. 190; 81, с. 17].

Під юридичним обов'язком І. С. Окунєв розуміє міру конкретно визначеної суспільно необхідної поведінки, встановлену в нормативно-правовому акті, забезпечену можливістю застосування санкції юридичної норми в її негативному й позитивному розумінні [128, с. 14]. На думку О. С. Іоффе та М. Д. Шаргородського, визначення обов'язку багато в чому залежить від того, як трактується поняття суб'єктивного права. Учені вважають, що обов'язок варто визначати через право, оскільки обов'язок є забезпеченою законом мірою належної поведінки, якій слідує зобов'язана особа відповідно до вимог управомоченого [76, с. 223–224]. Аналогічну думку мають також Д. М. Чечот та М. Г. Александров [206, с. 25; 6, с. 226].

Визначаючи сутність поняття «юридичні обов’язки», слід погодитися із позицією О. В. Зайчук та Н. М. Оніщенко, які виділяють такі специфічні риси поняття «юридичний обов’язок», як:

а) міра необхідної поведінки, змістом якої є утримання від порушення заборон і необхідність виконання зобов’язань;

б) це необхідна поведінка, що покладається з метою задоволення інтересів уповноваженої особи;

в) це необхідна поведінка, яка має юридичний характер, тобто закріплена правовою нормою;

г) це необхідна поведінка, що покладається як на всіх осіб, що проживають на території держави (обов’язок платити податки та обов’язкові платежі, охороняти природу, поважати державні символи, дотримуватися Конституції та законів України), так і лише на громадян (обов’язок захищати Вітчизну, її незалежність і територію, проходження військової служби) [185].

Таким чином, юридичний обов’язок можна визначити як юридичний засіб реалізації державою впливу на правовідносини, змістом якого є встановлення чинним законодавством України імперативних вимог до виду і міри необхідної поведінки суб’єктів права, де виконання останніх забезпечується державним примусом та іншими правовими засобами.

Обов’язок слід розуміти як встановлену на нормативно-правовому рівні міру необхідної поведінки, якої має дотримуватися Департамент кіберполіції Національної поліції України під час реалізації ними своїх повноважень.

До таких обов’язків у діяльності керівника Департаменту кіберполіції Національної поліції України можемо віднести:

– розподіл обов’язків між заступниками та керівниками структурних підрозділів Департаменту, контроль їх виконання, визначення ступеня відповідальності першого заступника та заступників начальника Департаменту;

– забезпечення відбору, розстановки, переміщення і професійної підготовки особового складу, дотримання службової дисципліни та законності, затвердження посадових інструкцій (функціональних обов'язків) працівників Департаменту в установленому законодавством порядку;

– проведення відповідно до законодавства атестування особового складу Департаменту, подання пропозицій голові Національної поліції України про присвоєння працівникам спеціальних звань поліції та рангів державних службовців;

– підписання організаційно-розпорядчих документі (наказів, доручень), рішень оперативних нарад, протоколів, оглядів, інформаційних листів, повідомлень, які обов'язкові для виконання особовим складом Департаменту;

– у разі відсутності начальника Департаменту його обов'язки виконує перший заступник або один із заступників, на якого головою Національної поліції України покладено виконання обов'язків з урахуванням пропозицій начальника Департаменту кіберполіції. Невиконання або неналежне виконання наведених вище обов'язків тягне за собою настання юридичної відповідальності, особливості якої будуть розкриті в подальших дослідженнях у формі статей [147].

Окрім зазначеного, працівники Департаменту кіберполіції Національної поліції України відповідно до Закону України «Про Національну поліцію» зобов'язані:

1) неухильно дотримуватися положень Конституції України, законів України та інших нормативно-правових актів, що регламентують діяльність поліції, та Присяги поліцейського;

2) професійно виконувати свої службові обов'язки відповідно до вимог нормативно-правових актів, посадових (функціональних) обов'язків, наказів керівництва;

3) поважати і не порушувати прав і свобод людини;

4) надавати невідкладну, зокрема домедичну і медичну, допомогу особам, які постраждали внаслідок правопорушень, нещасних випадків, а

також особам, які опинилися в безпорадному стані або стані, небезпечному для їхнього життя чи здоров'я;

5) зберігати інформацію з обмеженим доступом, яка стала йому відома у зв'язку з виконанням службових обов'язків;

6) інформувати безпосереднього керівника про обставини, що унеможливлюють його подальшу службу в поліції або перебування на займаній посаді [149].

2. Поліцейський на всій території України незалежно від посади, яку він займає, місцезнаходження і часу доби в разі звернення до нього будь-якої особи із заявою чи повідомленням про події, що загрожують особистій чи публічній безпеці, або в разі безпосереднього виявлення таких подій зобов'язаний вжити необхідних заходів з метою рятування людей, надання допомоги особам, які її потребують, і повідомити про це найближчий орган поліції. Додаткові обов'язки, пов'язані з проходженням поліцейським служби в поліції, можуть бути покладені на нього виключно законом [149].

Таким чином, права та обов'язки Департаменту кіберполіції Національної поліції України – це система визначених на нормативно-правовому рівні юридичних прав (міри можливої поведінки) та юридичних обов'язків (міри необхідної поведінки), якими наділяється Департамент кіберполіції Національної поліції України з метою реалізації покладених на нього правоохоронних функцій [13, с. 36]. При цьому слід підкреслити, що невиконання або неналежне виконання своїх обов'язків, як зазначалося раніше, чи зловживання правом тягнуть за собою юридичну відповідальність, що може бути застосована до суб'єктів відповідних правовідносин, у тому числі й до Департаменту кіберполіції Національної поліції України.

2.3. Територіальна юрисдикція підрозділів Департаменту кіберполіції в Україні

Державні перетворення, які зумовлені курсом України на євроінтеграцію, стосуються усіх ланок державного апарату і потребують

удосконалення діяльності органів публічної адміністрації, зокрема їх правоохоронного блоку. У зв'язку прийняттям Закону України «Про Національну поліцію», відбулися докорінні зміни, що вилились у тотальну переатестацію особового складу колишніх органів внутрішніх справ та створення поліцейської інституції європейського зразка. Відповідно Національна поліція України сьогодні є центральним органом виконавчої влади, який служить суспільству шляхом забезпечення охорони прав і свобод людини, протидії злочинності, підтримання публічної безпеки і порядку [4, с. 34].

В той же час діяльність Національної поліції України ознаменувалася створенням принципово нових органів, які покликані реалізовувати вузький напрям державної політки у сфері протидії злочинності. Так, у 2015 році створено новий міжрегіональний орган у складі кримінального блоку поліції – Департамент кіберполіції Національної поліції України, діяльність якого сьогодні набуває особливо актуального значення у зв'язку із появою нових кіберзагроз та небезпек. А відтак, визначення юрисдикції вказаного органу є актуальним та необхідним задля усунення існуючих законодавчих прогалин та ефективної протидії кіберзлочинності в Україні.

Проблематикою актуальних питань юрисдикції державного органу та адміністративно-юрисдикційної діяльності поліції займалися вчені та науковці з адміністративного права. Зокрема: О. М. Бандурка, С. Г. Братель, В. О. Басс, В. М. Білик, С. І. Братков, В. І. Варивода, В. І. Великий, С. М. Гусаров, К. А. Гусєва, Ю. В. Делія, О. Ю. Дрозд, Н. І. Золотарьова, А. П. Калініченко, С. Ф. Константінов, Я. М. Квітка, В. О. Кудря, А. Т. Комзюк, Г. Б. Кузьміних, М. К. Либаш, О. М. Музичук, О. Ю. Салманова, В. В. Сокуренко, В. В. Чумак, Д. В. Швець, Д. П. Цвігун та інші.

Поняття «юрисдикція» з лат. jurisdictio, від jus (juris) – право + dico проголошую) розглядається у наступних значеннях:

1) компетенція судових органів із розгляду цивільних, кримінальних та інших справ; коло справ, які даний суд має право розглядати й вирішувати;

2) коло питань, що належать до відання установи або держави.;

3) область застосування можливостей суб'єктом компетенції [223]. У свою чергу, у міжнародному праві «юрисдикція» означає повноваження держави давати правову оцінку фактам, розв'язувати ті чи інші правові питання [223].

В міжнародному праві концепція юрисдикції застосовується у двох різних контекстах: 1) в значенні національної юрисдикції в міжнародному праві як повноваження держави, що походять від її суверенітету в міжнародному праві; 2) в значенні повноважень міжнародних судових органів виносити рішення з обов’язковою силою для сторін справи [232, с. 33-34; 231, с. 321; 230, с. 927].

В науці адміністративного права під юрисдикцією розуміють з одного боку, коло повноважень особи або органу з правової оцінки конкретних фактів, у тому числі з розв'язання спорів та застосування санкцій відповідно до закону. З іншого боку, юрисдикція – це встановлена законом (або іншим нормативним актом) сукупність повноважень відповідних органів та посадових осіб щодо вирішення правових спорів, вирішення справ про правопорушення, оцінки дій особи чи іншого суб'єкта з точки зору їх відповідності закону, застосування юридичних санкцій до правопорушників (за винятком звернення до суду) [5, с. 8].

Слід зазначити, що юрисдикція ототожнювалась із встановленою законом (чи іншим нормативним актом) сукупністю правових повноважень відповідних державних органів вирішувати правові спори, в тому числі вирішувати справи про правопорушення, тобто оцінювати дії особи чи іншого об’єкта права з точки зору їх правомірності, застосовувати юридичні санкції до правопорушників. З часом розуміння юрисдикції зазнало певних змін, і сьогодні вона охоплює не лише діяльність державних органів (приміром, суди, поліція), а й муніципальних органів (виконавчі комітети

сільських, селищних, міських рад, адміністративні комісії) [5, с. 201].Таким чином сьогодні можна казати про те, що адміністративна юрисдикція є сукупністю повноважень органів публічної адміністрації вирішувати правові спори і справи про правопорушення [5, с. 11-12]. Приєднуючись до позиції Ю. С. Педька, відмітимо, що адміністративна юрисдикція є одним із видів юрисдикційної діяльності органів публічної адміністрації, виступає складовою частиною реалізації публічної влади, являючись «специфічним різновидом правоохоронної діяльності її органів». Адміністративно-юрисдикційна діяльність є результатом практичної реалізації певної частини повноважень, які разом з предметами відання становлять компетенцію відповідних органів. За допомогою даного виду діяльності орган публічної адміністрації дає правову оцінку відповідності поведінки об'єкта владного впливу встановленим правовим вимогам. При цьому владний вплив органу публічної адміністрації має правоохоронне спрямування [134, с. 74; 4, с. 203].

Тобто, визначаючи юрисдикцію Департаменту кіберполіції Національної поліції України маємо на увазі її адміністративно-юрисдикційну діяльність. Відповідно більш широко адміністративна юрисдикція означає вирішення будь яких індивідуальних справ у випадку виникнення спору про право, тобто конфліктних ситуацій [2, с. 132]. Зокрема, О. М. Бандурка, М. М. Тищенко, а також А. С. Васильєв до юрисдикційних відносять три види адміністративних проваджень: провадження в справах про адміністративні правопорушення, дисциплінарне провадження і провадження щодо скарг громадян [10, с. 17; 39, с. 194].

На думку А. Т. Комзюка, таке визначення адміністративної юрисдикції не зовсім виправдане, оскільки в цьому випадку зміст адміністративно юрисдикційної діяльності розширено до меж розгляду будь-якої індивідуальної справи, тобто до меж всього адміністративного процесу [94, с. 203].

Отже, юрисдикційна діяльність органів публічної адміністрації може полягати у розгляді скарг громадян і юридичних осіб органами публічної

адміністрації, хоча і така діяльність повинна супроводжуватися прийняттям рішення про усунення порушень режиму законності і застосування, при необхідності, державно-примусових заходів до правопорушника. Тому можна погодитися із думкою окремих вчених, згідно з якою до системи юрисдикційних проваджень входить і провадження за скаргами громадян [10, с. 17; 4, с. 189].

Узагальнюючи погляди фахівців на сутність адміністративної юрисдикції С. М. Гусаров відзначив, що адміністративно-юрисдикційна діяльність має такі, властиві лише їй риси:

1) наявність правового спору (або правопорушення). Юрисдикція виникає тільки тоді, коли необхідно вирішити спір про право або у зв'язку з порушенням чинних правових норм. Щодо адміністративної юрисдикції такі спори виникають між сторонами суспільних відносин, що регулюються адміністративно-правовими нормами, набуваючи характеру адміністративно-правових спорів;

2) основою адміністративно-правових спорів, у процесі вирішення яких здійснюється правова оцінка поведінки (дій) сторін є індивідуальні адміністративні справи. Розгляд тільки спірних конкретних справ становить зміст юрисдикційного адміністративного процесу (наприклад, розгляд справ про адміністративне правопорушення, скарг громадян);

3) адміністративно-юрисдикційна діяльність через свою суспільну значущість потребує належного процесуально-правового регулювання. Установлення та доведення подій і фактів, їх юридична оцінка здійснюються в рамках особливої процесуальної форми, що є важливою й обов'язковою для юрисдикції. Адміністративна юрисдикція значно відрізняється від інших видів юрисдикційної діяльності, що існують у рамках кримінального та цивільного процесів [60, с. 21; 4, с. 193].

Враховуючи зазначене, слід наголосити, що адміністративно-юрисдикційна діяльність реалізується відповідно кожним підрозділом Національної поліції відповідно до специфіки діяльності.

Відповідно до Закону України «Про Національну поліцію», систему поліції в Україні складають: центральний орган управління поліцією та територіальні органи поліції. Зазначимо, що склад апарату центрального органу управління поліції включає в себе організаційно поєднані структурні підрозділи, що забезпечують діяльність керівника поліції, а також виконання покладених на поліцію завдань. Зокрема, у складі поліції функціонують: 1) кримінальна поліція; 2) патрульна поліція; 3) органи досудового розслідування; 4) поліція охорони; 5) спеціальна поліція; 6) поліція особливого призначення [149]. Також, у системі поліції можуть утворюватися науково-дослідні установи та установи забезпечення.

У свою чергу у відповідності зі ст. ст. 14, 15 вищезазначеного закону, наказом Національної поліції України затверджено структуру Центрального апарату Національної поліції України та територіальних органів поліції. Відповідно до вказаного нормативно-правового акта, структура Центрального апарату Національної поліції України передбачає: керівництво; департамент забезпечення діяльності Голови; департамент карного розшуку (у складі кримінальної поліції); департамент стратегічних розслідувань (у складі кримінальної поліції); департамент боротьби зі злочинами, пов’язаними з торгівлею людьми (у складі кримінальної поліції); департамент протидії наркозлочинності (у складі кримінальної поліції); департамент оперативної служби (у складі кримінальної поліції); департамент оперативно-технічних заходів (у складі кримінальної поліції); департамент забезпечення діяльності, пов’язаної з небезпечними матеріалами (у складі кримінальної поліції); департамент превентивної діяльності; департамент «Корпусу оперативно-раптової дії» (у складі поліції особливого призначення); департамент міжнародного поліцейського співробітництва; головне слідче управління; департамент організаційно-аналітичного забезпечення та оперативного реагування; департамент інформаційно-аналітичної підтримки; правовий департамент; департамент кадрового забезпечення; департамент комунікації; департамент фінансового

забезпечення та бухгалтерського обліку; департамент внутрішнього аудиту; департамент управління майном; департамент зв'язку та телекомунікацій; департамент документального забезпечення; департамент вибухотехнічної служби; управління режиму та технічного захисту інформації; управління забезпечення прав людини; управління з питань запобігання корупції та проведення люстрації; відділ організації кінологічної діяльності; відділ спеціального зв'язку; сектор з питань пенсійного забезпечення; управління кримінального аналізу (у складі кримінальної поліції); управління організації діяльності підрозділів поліції на воді та повітряної підтримки [149; 148].

У свою чергу територіальні органи поліції утворюються як юридичні особи публічного права в Автономній Республіці Крим, областях, містах Києві та Севастополі, районах, містах, районах у містах та як міжрегіональні (повноваження яких поширюються на декілька адміністративно-територіальних одиниць) територіальні органи у межах граничної чисельності поліції і коштів, визначених на її утримання [149; 182]. Територіальні органи поліції представлені в областях у вигляді Головних управлінь Національної поліції з відповідними відділами та відділеннями поліції.

Примірна структура головних управлінь Національної поліції в областях передбачає: 1) апарат, до складу якого входять: керівництво, слідче управління, управління (відділ) карного розшуку (у складі кримінальної поліції), управління (відділ) стратегічних розслідувань (у складі кримінальної поліції), управління (відділ) боротьби зі злочинами, пов'язаними з торгівлею людьми (у складі кримінальної поліції), управління (відділ) протидії наркозлочинності (у складі кримінальної поліції), управління (відділ) оперативної служби (у складі кримінальної поліції), управління оперативно-технічних заходів (у складі кримінальної поліції), відділ (сектор) кримінального аналізу (у складі кримінальної поліції), управління (відділ) превентивної діяльності (у складі патрульної поліції), управління «Корпусу оперативно-раптової дії» (у складі поліції особливого призначення), відділ

(сектор) міжнародного поліцейського співробітництва, управління (відділ) організаційно-аналітичного забезпечення та оперативного реагування, відділ (сектор) правового забезпечення, відділ (сектор) комунікації, відділ (сектор) організації діяльності ізоляторів тимчасового тримання, управління (відділ) кадрового забезпечення, управління (відділ) фінансового забезпечення та бухгалтерського обліку, відділ (сектор) внутрішнього аудиту, управління (відділ) логістики та матеріально-технічного забезпечення, відділ (сектор) документального забезпечення, управління (відділ) режиму та технічного захисту інформації, управління (відділ) інформаційно-аналітичної підтримки, управління (відділ) зв'язку та телекомунікацій, вибухотехнічне управління (відділ, сектор), відділ (сектор) спеціального зв'язку, сектор з питань пенсійного забезпечення; 2) відділ поліції, який складається з наступних підрозділів: керівництво, слідчий відділ (відділення), відділ (сектор) кримінальної поліції, відділ (сектор) превенції (у складі патрульної поліції), сектори реагування патрульної поліції №1-№4 (для відділів поліції, де відсутні підрозділи Департаменту патрульної поліції), сектор спеціальної поліції, відділ (сектор) моніторингу, сектор кадрового забезпечення, режимно-секретний сектор, канцелярія, сектор логістики та матеріально-технічного забезпечення, кінологічний сектор, сектор інформаційної підтримки, окремі посади спеціалістів зв'язку та спеціального зв'язку; 3) відділення поліції (у складі відділу поліції) передбачає: керівництво, слідче відділення, сектор кримінальної поліції, сектор превенції (у складі патрульної поліції), сектори реагування патрульної поліції №1-№4 (для відділень поліції, де відсутні підрозділи Департаменту патрульної поліції), чергова частина (за відсутності секторів реагування патрульної поліції), канцелярія, логістика, окремі посади спеціалістів з режиму секретності, кінологічної служби; також, це: - 4) центр забезпечення; 5) ізолятори тимчасового тримання; 6) стройовий підрозділ патрульної служби поліції особливого призначення; 7) стройовий підрозділ поліції особливого призначення; 8) тренінговий центр; 9) кінологічний центр; 10) приймальник-

розподільник для дітей (у складі патрульної поліції); 11) стройовий підрозділ реагування патрульної поліції (забезпечення супроводження (у складі патрульної поліції); 12) стройовий підрозділ конвойної служби та 13) оркестр [181; 182].

Наразі на території України функціонують наступні Головні управління Національної поліції в областях: у Вінницькій, Волинській, Дніпропетровській, Донецькій, Житомирській, Закарпатській, Запорізькій, Івано-Франківській, Київській, Кіровоградській, Луганській, Львівській, Миколаївській, Одеській, Полтавській, Рівненській, Сумській, Тернопільській, Харківській, Херсонській, Хмельницькій, Черкаській, Чернівецькій, Чернігівській, у м. Києві [182].

Окрім зазначених органів Національної поліції України, до структури Національної поліції України входять міжрегіональні територіальні органи поліції. Зокрема, до числа останніх належать: Департамент патрульної поліції, Департамент внутрішньої безпеки (у складі кримінальної поліції), Департамент кіберполіції (у складі кримінальної поліції), Департамент поліції охорони як міжрегіональний територіальний орган Національної поліції [181].

Як вже наголошено у попередніх підрозділах, Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Як новостворений міжрегіональний територіальний орган Національної поліції, Департамент має власну юрисдикцію, що поширюється одру на декілька регіонів. Утворений Департамент кіберполіції Національної поліції України 13 жовтня 2015 року постановою Кабінету Міністрів України «Про утворення територіального органу Національної поліції» [155].

Департамент кіберполіції Національної поліції України структурно передбачає: 1) апарат, що включає: керівництво, управління інформаційних технологій та програмування, управління протидії злочинам у сферах інтелектуальної власності та господарської діяльності, управління протидії злочинам у сфері інформаційної безпеки, відділ аналітичного забезпечення, відділ логістики, сектор Національного контактного пункту реагування на кіберзлочини, сектор кадрового забезпечення, відділ фінансового забезпечення та бухгалтерського обліку, режимно-секретний сектор; 2) територіальні (відокремлені) підрозділи: Донецьке управління кіберполіції (відділ протидії кіберзлочинам в Донецькій області, відділ протидії кіберзлочинам в Луганській області); Слобожанське управління кіберполіції (відділ протидії кіберзлочинам в Сумській області, відділ протидії кіберзлочинам в Харківській області, відділ протидії кіберзлочинам в Полтавській області); Придніпровське управління кіберполіції (відділ протидії кіберзлочинам в Кіровоградській області, відділ протидії кіберзлочинам в Дніпропетровській області, відділ протидії кіберзлочинам в Запорізькій області); Причорноморське управління кіберполіції (відділ протидії кіберзлочинам в Миколаївській області, відділ протидії кіберзлочинам в Одеській області, відділ протидії кіберзлочинам в Херсонській області); Київське управління кіберполіції (відділ протидії кіберзлочинам в Чернігівській області, відділ протидії кіберзлочинам в Черкаській області, відділ протидії кіберзлочинам у місті Києві, відділ протидії кіберзлочинам в Київській області), Подільське управління кіберполіції (відділ протидії кіберзлочинам в Тернопільській області, відділ протидії кіберзлочинам у Вінницькій області, відділ протидії кіберзлочинам у Хмельницькій області); Поліське управління кіберполіції (відділ протидії кіберзлочинам у Волинській області, відділ протидії кіберзлочинам в Житомирській області, відділ протидії кіберзлочинам в Рівненській області); Карпатське управління кіберполіції (відділ протидії кіберзлочинам в Івано-Франківській області, відділ протидії кіберзлочинам в Закарпатській області,

відділ протидії кіберзлочинам у Львівській області, відділ протидії кіберзлочинам в Чернівецькій області), Управління інформаційних технологій та програмування в західному регіоні, Управління інформаційних технологій та програмування в східному регіоні, Управління інформаційних технологій та програмування в південному регіоні [148].

До складу Департаменту кіберполіції входять структурні підрозділи, які діють за міжрегіональним принципом та безпосередньо підпорядковані начальникові Департаменту (Донецьке, Карпатське, Київське, Подільське, Придніпровське, Причорноморське та Слобожанське управління кіберполіції, а також управління інформаційних технологій та програмування в західному, південному та східному регіонах) [154].

Так за територіальною юрисдикцією:

Подільське управління кіберполіції Національної поліції України охоплює обслуговування Хмельницької, Вінницької та Тернопільської областей.

Поліське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Волинської, Рівненської та Житомирської областей.

Придніпровське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Дніпропетровської, Кіровоградської та Запорізької областей.

Донецьке управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Донецької та Луганської областей.

Карпатське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Львівської, Івано-Франківської, Чернівецької та Закарпатської областей.

Київське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування міста Києва, Київської, Черкаської та Чернігівської областей.

Причорноморське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Одеської, Миколаївської та Херсонської областей.

Слобожанське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Сумської, Харківської та Полтавської областей [154].

Отже, Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність [68]. Особливістю діяльності Департаменту кіберполіції Національної поліції України є визначення його територіальної юрисдикції, де остання визначена як передбачене нормативно-правовими актами коло повноважень кіберполіції залежно від території, на яку поширюється їх юрисдикція.

2.4. Юридичні гарантії підрозділів Департаменту кіберполіції в Україні

У сучасних умовах оновлення чинного поліцейського законодавства, велика увага з боку громадськості приділяється безпосередньо самому працівникові як поліції загалом так і Департаменту кіберполіції зокрема. Суспільство, як вказує І. І. Сенчук, менше цікавить присутність поліцейських, більше уваги приділяється безпосередньо особі поліцейського, рівню його професійної підготовки та компетентності, освіти, його фізичній формі та здатності адекватно реагувати на виклики, які постають при виконанні службових обов’язків [164, с. 88]. У зв’язку з цим діяльність поліцейських в Україні повинна відповідати викликам сьогодення та бути адаптована до сучасного стану розвитку правовідносин. Особливу роль в даному контексті відіграє система юридичних гарантій діяльності

державного органу та його посадових (службових) осіб, що виступає своєрідним засобом забезпечення законності професійної діяльності посадових (службових) осіб та забезпечення їх трудових, соціально-економічних та інших прав та інтересів. В. А. Троян наголошує, що забезпечення гарантій професійної діяльності органів та підрозділів Національної поліції України є важливим елементом правового порядку держави в цілому. Розгляд зазначених питань сьогодні набуває важливого значення в умовах побудови демократичної, правової держави, адже закріплення гарантій у законодавстві України сприятиме реалізації основоположних прав і свобод людини і громадянина [195, с. 176]. Гарантії посіли особливе місце в механізмі реалізації прав і свобод людини та громадянина, оскільки покликанні забезпечити режим найбільшого сприяння під час здійснення відповідних суб'єктивних прав індивідів і виступають як реальний важіль, що дозволяє за потреби забезпечити здійснення нормативно закріпленої юридичної можливості [102, с. 121].

Науковець В. В. Чумак вказує, що успішний зарубіжний досвід протидії корупції в органах внутрішніх справ характеризується побудовою нової системи юридичних гарантій діяльності поліції, яка відіграє важливу роль у формуванні демократичної поліцейської служби та налагодження принципово нових відносин із суспільством [208, с. 150].

Науково-теоретичне підґрунтя дослідження юридичних гарантій діяльності Департаменту кіберполіції Національної поліції України стали праці таких провідних науковців та вчених з адміністративного права та поліціїстики як: О. М. Бандурка, Б. М. Бевзенко, О. І. Безпалова, Ю. П. Битяк, С. М. Бортник, С. М. Гусаров, О. П. Ківалов, А. М. Клочко, Т. О. Коломоєць, В. К. Колпаков, А. Т. Комзюк, Л. В. Могілевський, О. П. Рябченко, В. В. Сокуренко, В. А. Троян, В. В. Чумак, Д. В. Швець та інші.

Визначаючи юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України слід розпочати дослідження із визначення загального поняття гарантій. Довідкова література надає наступне

визначення поняття «гарантії», – 1) порука в чомусь, забезпечення чого-небудь; 2) умови, що забезпечують успіх чого-небудь [173, с. 29]. Юридичний словник визначає поняття «гарантії» у спеціальному правовому значенні, де останні – це один із способів забезпечення зобов'язань у відносинах між сторонами [220, с. 59].

На думку дослідника А. Ф. Нікітіна, гарантії – це обов'язки держави захищати людину, створювати правові, соціальні і культурні умови для реалізації її прав і свобод, а також діяльність міжнародних і державних організацій щодо захисту прав людини [171, с. 76].

Теорія держави і права визначає гарантії як умови, що необхідні для реалізації тих чи інших прав громадян або інших учасників правовідносин [43, с. 30]. Наголошуючи на важливості визначення юридичних гарантій, у науковій літературі зазначають, що як сукупність конкретних засобів юридичні гарантії носять юридичний і загальнообов'язковий характер, завдяки чому можливе всебічне забезпечення ефективного здійснення, охорони і захисту прав особистості. Без гарантованості суб'єктивних прав складно говорити про повне забезпечення такими правами. Тим паче вторинними стають питання практичного використання суб'єктом своїх прав. Різні підходи до визначення «юридичні гарантії» обумовлені сферою застосування зазначеного поняття [47, с. 269]. Також, в науковій літературі досить часто зустріти розуміння гарантій як сукупність об'єктивних та суб'єктивних факторів, що спрямовані на забезпечення і реалізацію прав, свобод громадян, на усунення можливих причин та перегляд їх неповного або неналежного здійснення і захист прав від цих порушень. Ці фактори є різноманітними, і за своєю природою виступають як умови, засоби, прийоми та методи забезпечення процесу реалізації прав та свобод учасників суспільних відносин [8, с. 26-30].

Дослідник І. Л. Бородін вказує, що зміст юридичних гарантій становлять правові та організаційно-правові засоби і способи, за допомогою яких забезпечуються реалізація та всебічна охорона прав суб'єктів

правовідносин [25, с. 34]. В. В. Чумак зазначає, що важливою складовою організаційно-правових засад державного органу є система юридичних гарантій його діяльності, що визначаються з урахуванням європейських стандартів та успішного зарубіжного досвіду [212, с. 60]. В. Ф. Сіренко визначає гарантії прав як сукупність об'єктивних та суб'єктивних факторів, спрямованих на забезпечення фактичної реалізації прав громадян, на усунення можливих причин і перешкод їх неповного чи неналежного здійснення, захист прав від будь-яких порушень [165, с. 76].

Так, О. Ф. Скакун зауважує, що коли немає юридичних гарантій, то права, обов'язки й свободи людини і громадянина набувають форми «заяв про наміри» [166, с. 203].

З етимологічної точки зору «гарантії» – це порука у чомусь, забезпечення чого-небудь [173]. До того ж з французької це поняття («гарантія») у перекладі також означає поруку, забезпечення (чого-небудь). Це соціальне явище, що забезпечує досягнення конкретного результату, створює умови для функціонування певних суспільних відносин [172, с. 130]. Слід зазначити, що на сьогодні щодо визначення поняття «гарантії» в юридичній науці панують різні точки зору. Як слушно зазначає А. В. Пономаренко, поняття гарантії охоплює сукупність об'єктивних і суб'єктивних чинників, спрямованих на практичну реалізацію прав і свобод, усунення можливих перешкод їх повного або належного здійснення [139, с. 38].

У широкому сенсі Б.І. Стахура під «гарантіями» має на увазі всю сукупність об'єктивних і суб'єктивних чинників, які спрямовані на повну реалізацію і всебічну охорону прав і свобод громадян, на усунення причин і умов їх неналежного здійснення і захист від порушень. Встановлюючи зміст і обсяг прав і свобод людини, держава бере на себе гарантію виконання цих установок [177, с. 91].

Автор М. С. Малеїн під юридичними гарантіями розуміє норми права, які передбачають у своїй сукупності правовий механізм, покликаний сприяти

реалізації законів. Якісна характеристика юридичних гарантій передбачає оцінку всієї діючої системи права в цілому, з точки зору повноти охоплення правовим інструментарієм усіх найбільш важливих взаємовідносин державних органів та громадян, а також громадян між собою [112, с. 43]. А. Ф. Нікітін визначає гарантії як обов'язки держави захищати людину, створювати правові, соціальні та культурні умови для реалізації її прав і свобод, а також діяльність міжнародних і державних організацій щодо захисту прав людини [171, с.76]. В. Ф. Сіренко визначає гарантії прав як сукупність об'єктивних і суб'єктивних факторів, спрямованих на забезпечення фактичної реалізації прав громадян, на усунення можливих причин і перешкод їх неповного чи неналежного здійснення, захист прав від будь-яких порушень [165, с. 76].

На думку С. С. Строгович, гарантії – це встановлені законом, нормами права засоби, способи, якими охороняються і захищаються права громадян, припиняються та усуваються їх порушення, відновлюються порушені права [180, с. 180]. О. Ф. Скакун під гарантіями прав, свобод та обов'язків людини та громадянина розуміє систему соціально-економічних, політичних, юридичних умов, способів і засобів, які забезпечують їхню фактичну реалізацію, охорону та надійний захист [168, с. 203; 139, с. 37].

Вбачається, що гарантії щодо будь-якої діяльності виступають необхідними засобами (способами, заходами, умовами) її ефективного, належного здійснення. Слід вказати, що наведений підхід до визначення сутності юридичних гарантій є доволі поширеним серед учених [135, с. 305; 115, с. 27; 119, с. 26; 27, с. 58].

На думку С. С. Алексєєва, гарантіями є умови й особливі юридичні механізми, покликані забезпечити фактичну реалізацію законоположень [7, с. 135]. Своєю чергою В. Д. Шахов вважає, що гарантії – це різні правові інститути, принципи, різноманітні пільги, переваги, заохочення [214, с. 79]. В. Ф. Сіренко визначає гарантії прав як сукупність об'єктивних та суб'єктивних факторів, спрямованих на забезпечення фактичної реалізації

прав громадян, на усунення можливих причин і перешкод їх неповного чи неналежного здійснення, захист прав від будь-яких порушень [165, с. 76; 139, с. 37].

Досліджуючи питання юридичних гарантій людини і громадянина, Л. Л. Богачова зазначає, що в європейському праві під гарантіями прав і свобод людини (у вузькому, юридичному сенсі) розуміють засоби захисту прав від порушень, процедури поновлення порушених прав і порядок відшкодування завданої шкоди [22, с. 58]. З точки зору Л. П. Гарчевої і О. Н. Ярмиша, гарантії основних прав і свобод громадян є системою норм, принципів, умов і вимог, які забезпечують додержання прав, свобод і законних інтересів громадян [49, с. 128]. На думку А. Ф. Нікітіна, гарантії – це обов'язки держави захищати людину, створювати правові, соціальні та культурні умови для реалізації її прав і свобод, а також діяльність міжнародних і державних організацій щодо захисту прав людини [171, с. 76; 139, с. 37].

Своєю чергою, А. С. Мордовець зазначає, що гарантії являють собою складне соціально-політичне та юридичне явище, для розуміння сутності якого враховувати такі його аспекти:

- пізнавальний – дозволяє розкрити предметні теоретичні знання про об'єкт їх впливу, отримати практичні знання про соціальну та правову політику держави;

- ідеологічний – використовується політичною владою як засіб пропаганди демократичних ідей всередині країни та за її межами;

- практичний – визначається як інструментарій юриспруденції, передумова задоволення соціальних благ особи. Звідси, вказує автор, слідує, що гарантії – система соціально-економічних, політичних, юридичних, організаційних передумов, умов, засобів і способів, що створюють можливості особистості для здійснення своїх прав, свобод, інтересів [183, с. 275].

В юридичній енциклопедії юридичні гарантії прав і свобод людини та громадянина визначені як правові норми й інститути, що забезпечують можливість безперешкодного здійснення прав особи, їх охорону, а в разі протиправних посягань – захист і поновлення юридичної гарантії, встановленої Конституцією та іншими законами України [222, с. 555; 139, с. 37]. С. М. Шило висловлює позицію, що під гарантіями законності в адміністративній діяльності міліції необхідно розуміти способи, умови і засоби, що позитивно впливають на державну структуру як зсередини, так і ззовні, забезпечують процес реалізації законності і тим самим формують таку впорядкованість соціальних відносин, що сприяє руху країни до розвитку демократії і формування правової держави [218, с. 290].

Професор Ю. С. Шемшученко під гарантіями прав та свобод громадян розуміє умови, засоби, способи, що забезпечують реалізацію та всебічну охорону прав та свобод людини і громадянина. Поняття «гарантії», на думку вченого, охоплює усю сукупність об'єктивних і суб'єктивних чинників, спрямованих на практичну реалізацію прав і свобод громадян, на усунення можливих перешкод їх повного або можливого здійснення [113, с. 41; 222, с. 555; 139, с. 40].А О. В. Міцкевич вважає, що юридичні гарантії – це встановлений державою порядок діяльності державних органів та установ, громадських організацій, спрямований на попередження й припинення посягань на права громадян, на відновлення цих прав і залучення до відповідальності за порушення цих прав [122, с. 16]. Тим часом В. Ф. Погорілко наголошує на тому, що юридичні гарантії – це передбачені законом спеціальні засоби практичного забезпечення прав і свобод людини і громадянина [138, с. 40; 139, с. 41].

Дослідник В. О. Патюлін надає таке визначення юридичним гарантіям – це правові норми, що визначають специфічні юридичні засоби, умови та порядок реалізації прав, юридичні засоби їх охорони та захисту у випадку порушення [133, с. 237]. О. П. Нагорний, своєю чергою, вказує, що гарантії – це закріплена в нормах права система адміністративно-правових засобів, що

сприяють реалізації визначених правових норм, що регламентують адміністративну діяльність міліції, а також спеціально вироблені державою способи, що забезпечують у цій сфері діяльності точне дотримання, застосування законів і підзаконних нормативних актів, правильне використання прав, виконання обов'язків усіма учасниками адміністративних правовідносин із притягненням правопорушників до юридичної відповідальності [125, с. 46].

У своєму дисертаційному дослідженні, що присвячене аналізу адміністративно-правового статусу регіональних управлінь Державної фіскальної служби України В.А. Грушевський вказує, що така категорія як «юридичні гарантії» є досить спірною для фіскального апарату. Для того щоб сформувати юридичні гарантії діяльності територіальних органів ДФС України варто дослідити чималу кількість «дотичних» нормативно-правових актів, оскільки ні Положення про Державну фіскальну службу України, ні інші типові положення про територіальні підрозділи ДФС України не містять їх чіткого переліку [58, с. 133-134].

З аналізу викладеного випливає той факт, що одностайного розуміння щодо визначення сутності юридичних гарантій серед науковців немає. В цілому наукові здобутки з цього приводу, на наш погляд, доцільно буде згрупувати у дві групи (щодо визначення категорії «юридичні гарантії):

1) юридичні гарантії – це уся сукупність об'єктивних і суб'єктивних умов, що сприяють реалізації основоположних прав, свобод і законних інтересів людини і громадянина (широке розуміння);

2) юридичні гарантії – це сукупність засобів, за допомогою яких реалізується юридично значуща діяльність і здійснюється захист прав, свобод і законних інтересів не лише громадян, але й державних службовців (вузьке розуміння).

Визначаючи юридичні гарантії діяльності митних органів України В. Т. Комзюк правові гарантії діяльності митних органів України розглядає як умови, засоби, фактори, що є необхідними для забезпечення та реалізації

громадянами прав, свобод та інтересів у сфері митних правовідносин, а також як умови і засоби, які є необхідними для забезпечення нормального функціонування митних органів та їх посадових осіб, що виражається в їх нормативному закріпленні та реальному здійсненні, забезпеченні як з боку вищих органів відносно нижчих, так і з боку держави [95, с. 71].

Зазначимо, що правові гарантії здебільшого поділяються на види. Так, загальновизнаним є поділ гарантій на такі види: особистісні, політичні, економічні, ідеологічні та правові (юридичні). У свою чергу, К. П. Уржинський розглядає соціально-економічні, політичні, ідеологічні, організаційні та правові гарантії [200, с. 4]. О. Смирнов виділяє такі види гарантій: економічні, юридичні і соціальні [174, с. 163].

Ми пропонуємо юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України класифікувати на наступні групи: 1) юридичні гарантії професійної діяльності Департаменту кіберполіції; 2) правові гарантії діяльності Департаменту кіберполіції; 3) матеріально-технічні гарантії діяльності Департаменту кіберполіції; 4) соціально-економічні гарантії діяльності Департаменту кіберполіції.

Правову основу юридичних гарантій професійної діяльності Національної поліції України взагалі та Департаменту кіберполіції Національної поліції України зокрема становить ст. 62 Закону України «Про Національну поліцію» [149]. Відповідно до зазначеної статті закону, поліцейські Департаменту кіберполіції Національної поліції України під час виконання покладених на них повноважень є представником держави. Законодавець визначив, що вимоги поліцейського є законними та обов’язковими для виконання фізичними та юридичними особами без винятку.

Працівник Департаменту кіберполіції Національної поліції України під час виконання покладених на нього обов’язків підпорядковується виключно своєму безпосередньому керівникові. Зазначається, що ніхто, за винятком випадків, що визначені законом, окрім безпосереднього керівника не має

права надавати будь-які письмові або усні вказівки, вимоги, доручення працівникові Департаменту кіберполіції Національної поліції України або іншим способом втручатися в його законну діяльність, у тому числі діяльність, що пов'язана зі здійсненням кримінального провадження. Законодавець встановив, що поліцейський Департаменту кіберполіції Національної поліції України має право надавати пояснення з приводу справ та матеріалів, що перебувають у нього в провадженні, а також зобов'язаний надавати їх для ознайомлення у випадках та в порядку, що визначені законом [149].

Серед юридичних гарантій професійної діяльності Департаменту кіберполіції Національної поліції України є наступні: 1) ніхто не має права покласти на працівника Департаменту кіберполіції виконання обов'язків, що не передбачені чинним законодавством; 2) забороняється будь-яке втручання в діяльність працівника Департаменту кіберполіції та перешкоджання виконанню ним відповідних повноважень, а також невиконання законних вимог працівника Департаменту кіберполіції. У випадку якщо вчиненні будь-які інші протиправні дії стосовно поліцейського Департаменту кіберполіції мають наслідком юридичну відповідальність відповідно до законодавства; 3) вчинення правопорушення відносно поліцейського Департаменту кіберполіції або його близьких родичів у зв'язку з його службовою діяльністю, мають наслідком юридичну відповідальність відповідно до законодавства [149].

Також, серед юридичних гарантій професійної діяльності поліцейських Департаменту кіберполіції Національної поліції України слід виокремити наступні:

1) поліцейські Департаменту кіберполіції Національної поліції України забезпечуються належними умовами для виконання покладених на них службових прав та обов'язків;

2) поліцейські Департаменту кіберполіції Національної поліції України мають право отримувати в органах Національної поліції України

інформацію, у тому числі з обмеженим доступом, та матеріали, що необхідні для належного виконання покладених на нього завдань у встановленому законом порядку;

3) поліцейські Департаменту кіберполіції Національної поліції України користуються повноваженнями, що визначені Законом України «Про Національну поліцію», незалежно від посади, яку він обіймає, його місцезнаходження та часу;

4) Департамент кіберполіції Національної поліції України своєчасно і в повному обсязі отримує грошове забезпечення та інші компенсаційні виплати відповідно до чинного законодавства України;

5) Департамент кіберполіції Національної поліції України у повному обсязі користується гарантіями соціального та правового захисту, що закріплені Законом України «Про Національну поліцію» та іншими актами законодавства;

6) Департамент кіберполіції Національної поліції України захищає свої права, свободи та законні інтереси всіма способами, що передбачені законом;

7) під час виконання своїх повноважень поліцейські Департаменту кіберполіції Національної поліції України користуються безоплатно всіма видами громадського транспорту міського, приміського і місцевого сполучення (за винятком таксі), а також попутним транспортом. Поліцейські Департаменту кіберполіції, які виконують повноваження поліції на транспортних засобах, окрім вищенаведеного, мають право на безоплатний проїзд у поїздах, на річкових і морських суднах. Під час службових відряджень поліцейські Департаменту кіберполіції мають право на позачергове придбання квитків на всі види транспорту і розміщення в готелях при пред’явленні службового посвідчення та посвідчення про відрядження;

8) атестований працівник Департаменту кіберполіції може бути переміщений по службі залежно від результатів виконання покладених на нього обов’язків та своїх професійних, особистих якостей [149].

Правові гарантії діяльності Департаменту кіберполіції Національної поліції України передбачають можливість утворювати професійні спілки. Зазначається, що обмеження прав професійних спілок поліцейських порівняно з іншими професійними спілками не допускається. Важливою складовою правових гарантій діяльності Департаменту кіберполіції Національної поліції України є визначення його адміністративно-правового статусу – зокрема, Департамент є юридичною особою публічного права, має власну печатку та штампи, а міжрегіональні управління самостійно реалізують надані їм законом повноваження.

Не менш важливою правовою гарантією є право працівників Департаменту кіберполіції Національної поліції України застосовувати вогнепальну зброю, спеціальні засоби та фізичний вплив. Так, зокрема, чинний Кримінальний Кодекс України містить низку статей, що передбачають кримінальну відповідальність за протиправні дії щодо працівника поліції: ст. 342 «Опір представникові влади, працівникові правоохоронного органу, державному виконавцю, члену громадського формування з охорони громадського порядку і державного кордону або військовослужбовцеві, уповноваженій особі Фонду гарантування вкладів фізичних осіб», ст. 343 «Втручання в діяльність працівника правоохоронного органу, працівника державної виконавчої служби», ст. 345 «Погроза або насильство щодо працівника правоохоронного органу», ст. 348 «Посягання на життя працівника правоохоронного органу, члена громадського формування з охорони громадського порядку і державного кордону або військовослужбовця» та інші [98].

Закон України «Про оперативно-розшукову діяльність» визначає наступні правові гарантії оперативних підрозділів Департаменту кіберполіції Національної поліції України, які здійснюють оперативно-розшукову діяльність. На працівників, які здійснюють оперативно-розшукову діяльність, поширюються гарантії правового і соціального захисту, передбачені законами України. Працівникам, які здійснюють оперативно-розшукову

діяльність, надаються додаткові пільги в питаннях соціально-побутового та фінансового забезпечення в порядку, встановленому Кабінетом Міністрів України. При наявності даних про загрозу життю, здоров'ю або майну працівника та його близьких родичів у зв'язку із здійсненням ним оперативно-розшукової діяльності в інтересах безпеки України, або по виявленню тяжкого та особливо тяжкого злочину, або викриттю організованої злочинної групи оперативний підрозділ зобов'язаний вжити спеціальних заходів для забезпечення їх безпеки - зміна даних про особу, зміна місця проживання, роботи і навчання, інших даних у порядку, що визначається Кабінетом Міністрів України [150].

До числа матеріально-технічних гарантій діяльності Департаменту кіберполіції Національної поліції України належать: фінансування і матеріально-технічне забезпечення поліції здійснюються за рахунок коштів Державного бюджету України, а також інших джерел, не заборонених законом. Майно поліції є державною власністю і належить їй на праві оперативного управління. Органи поліції здійснюють володіння, користування та розпорядження майном у порядку, визначеному законом. Правовий режим земельних ділянок, на яких розміщуються органи (заклади, установи) поліції, визначається законом. Поліція для виконання покладених на неї завдань і повноважень може використовувати службові, у тому числі спеціалізовані, транспортні засоби. Виконавчі комітети сільських, селищних, міських рад надають безоплатно органам і підрозділам поліції службові приміщення, обладнані меблями і засобами зв'язку, транспорт та інші матеріально-технічні засоби. Комунальні та приватні підприємства можуть виділяти органам та підрозділам поліції кошти, транспорт та інші матеріально-технічні засоби, необхідні для виконання повноважень поліції [149].

Соціальні гарантії діяльності Департаменту кіберполіції Національної поліції України передбачають можливість поліцейським, які виконували службові обов'язки у вихідні, святкові та неробочі дні, крім поліцейських, які

працюють у змінному режимі, відповідний час для відпочинку в порядку компенсації надається протягом двох наступних місяців [149]. Також, до соціальних гарантій діяльності Департаменту кіберполіції Національної поліції України належать: щорічні чергові оплачувані відпустки в порядку та тривалістю, визначених цим Законом, а також додаткові відпустки у зв'язку з навчанням, творчі відпустки, соціальні відпустки, відпустки без збереження заробітної плати (грошового забезпечення) та інші види відпусток відповідно до законодавства про відпустки; грошове забезпечення поліцейських; медичне забезпечення поліцейських; житлове забезпечення поліцейських; одноразова грошова допомога в разі загибелі (смерті) чи втрати працездатності поліцейського; пенсійне забезпечення поліцейських.

Таким чином, юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України – це відображені у нормативно-правових актах сукупність умов, способів та засобів, за допомогою яких визначаються умови і порядок реалізації, здійснення прав і свобод працівників, а також їх охорону, захист та відновлення у разі порушення. Юридичним гарантіям притаманні ознаки, які мають важливе значення, адже вони відображають специфічні властивості, за допомогою яких можливо відокремити юридичні гарантії від інших видів гарантій. Юридичні гарантії в сукупності з притаманними їм ознаками ефективніше діють та забезпечують реалізацію й захист прав, в іншому випадку можна поставити під сумнів їх фактичну реалізацію. Тому пошук оптимальних шляхів забезпечення функціонування юридичних гарантій потребує подальшого наукового дослідження в адміністративному праві [139, с. 40-41].

Висновки до розділу 2

Визначено, що завдання та функції Департаменту кіберполіції Національної поліції України є важливою складовою визначення особливостей його діяльності та адміністративно-правового статусу, оскільки ефективне виконання Департаментом кіберполіції Національної поліції

України своїх повноважень залежить від чіткого законодавчого розуміння його завдань та функцій як базового елемента адміністративно-правового статусу будь-якого органу державної влади [187-192].

Обґрунтовано під завданнями Департаменту кіберполіції Національної поліції України розуміти визначені на нормативно-правовому рівні шляхи досягнення конкретної мети діяльності, а саме – реалізація державної політики у галузі протидії кіберзлочинності, інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до компетенції кіберполіції.

Запропоновано до загальних завдань Департаменту кіберполіції Національної поліції відносити: забезпечення публічної безпеки та публічного порядку; охорона основоположних прав і свобод людини, а також інтересів суспільства і держави; протидія кіберзлочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

До спеціальних завдань Департаменту кіберполіції Національної поліції України запропоновано віднести наступні: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів.

Наголошено, що до завдань, що не пов’язані із державною таємницею належать: формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Запропоновано наступну класифікацію завдань Департаменту кіберполіції Національної поліції України у сфері протидії злочинності у відповідності до кіберзлочинів, а саме: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); 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 (ст. 361-2); 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 (ст. 362); 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 (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) та деякі інші.

Обґрунтовано, що права та обов’язки Департаменту кіберполіції Національної поліції України (повноваження) – це система визначених на нормативно-правовому рівні юридичних прав та юридичних обов’язків, якими наділяється Департамент кіберполіції Національної поліції України з метою реалізації покладених на нього завдань та функцій.

Запропоновано під територіальною юрисдикцією Департаменту кіберполіції Національної поліції України розуміти передбачене нормативно-правовими актами коло повноважень кіберполіції залежно від території, на яку поширюється їх юрисдикція.

З’ясовано, що за територіальною юрисдикцією управління кіберполіції Департаменту кіберполіції Національної поліції України поділяються: Подільське управління кіберполіції Національної поліції України охоплює обслуговування Хмельницької, Вінницької та Тернопільської областей. Поліське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Волинської, Рівненської та Житомирської областей. Придніпровське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Дніпропетровської, Кіровоградської та Запорізької областей. Донецьке управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Донецької та Луганської областей. Карпатське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Львівської, Івано-Франківської, Чернівецької та Закарпатської областей. Київське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування міста Києва, Київської, Черкаської та Чернігівської областей. Причорноморське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Одеської, Миколаївської та Херсонської областей. Слобожанське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Сумської, Харківської та Полтавської областей .

Наголошено, що Департамент кіберполіції Національної поліції України є міжрегіональним територіальним органом Національної поліції України, який входить до структури кримінальної поліції Національної поліції та відповідно до законодавства України забезпечує реалізацію державної політики у сфері боротьби з кіберзлочинністю, організовує та здійснює відповідно до законодавства оперативно-розшукову діяльність.

Визначено, що особливістю діяльності Департаменту кіберполіції Національної поліції України є визначення його територіальної юрисдикції, де остання визначена як передбачене нормативно-правовими актами коло

повноважень кіберполіції залежно від території, на яку поширюється їх юрисдикція.

Встановлено, що юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України – це відображені у нормативно-правових актах сукупність умов, способів та засобів, за допомогою яких визначаються умови і порядок реалізації, здійснення прав і свобод працівників, а також їх охорону, захист та відновлення у разі порушення.

Встановлено, що до юридичних гарантій діяльності Департаменту кіберполіції Національної поліції України віднесені: 1) юридичні гарантії професійної діяльності Департаменту кіберполіції; 2) правові гарантії діяльності Департаменту кіберполіції; 3) організаційні гарантії діяльності Департаменту кіберполіції; 4) матеріально-технічні гарантії діяльності Департаменту кіберполіції; 5) соціально-економічні гарантії діяльності Департаменту кіберполіції; 6) психологічні гарантії діяльності Департаменту кіберполіції.

РОЗДІЛ 3
УДОСКОНАЛЕННЯ АДМІНІСТРАТИВНО-ПРАВОВОГО СТАТУСУ ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ В УКРАЇНІ

3.1. Зарубіжний досвід діяльності органів поліції у сфері протидії кіберзлочинам та можливості його використання в Україні

Сьогодні, в умовах удосконалення діяльності органів державної влади, особливого значення набуває дослідження позитивного зарубіжного досвіду діяльності органів державної влади, діяльність яких спрямована на забезпечення кібербезпеки держави та протидії кіберзлочинності. Одним із таких суб'єктів є органи та підрозділи поліції, що виступають суб'єктом забезпечення як внутрішньої складової безпеки держави так й зовнішнього блоку національної безпеки держави. При цьому, окрему увагу слід приділити тим державам, які першими стали на шлях побудови національного законодавства у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності. Такими державами є країни Європейського Союзу та Сполучених Штатів Америки, а також країни пост-радянського простору (Латвія, Литва. Естонія та деякі інші).

Таким чином, дослідження діяльності органів поліції зазначених держав та їх національного законодавства є на сьогодні вельми актуальним та своєчасним в умовах удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України.

Питання забезпечення кібербезпеки та протидії кіберзлочинності неодноразово ставали предметом наукових дискусій та досліджень. Так, зазначена проблематика знайшла своє відображення у працях таких вітчизняних вчених та науковців як: В. Б. Авер'янов, О. Ф. Андрійко, О. М. Бандурка, В. Ю. Баскаков, В. В. Береза, К. І. Бєляков, О. В. Бойченко, В. М. Бутузов, В. В. Василевич, В. П. Горбулін, С. М. Гусаров, І. В. Діордіца, Є. В. Додін, О. Ю. Дрозд, М. Г. Каращук, Н. В. Коваленко, Т. О. Коломоєць,

В. К. Колпаков, А. Т. Комзюк, О. Є. Користін, В. І. Куріло, А. М. Лобода, В. А. Ліпкан, Ю. Є. Максименко, В. В. Марков, Л. В. Могілевський, О. М. Музичук, О. А. М. Новицький, О. П. Орлюк, Ю. Салманова, Р. Ю. Сень, О. Ю. Синявська, Т. Л. Сироїд, В. С. Сідак, В. В. Сокуренко, В. О. Тімашов, В. В. Чернєй, В. В. Чумак, Д. В. Швець, О. В. Шепета та інші. В той же час, наразі недостатньо уваги приділено діяльності спеціалізованих державних в тому числі міжнародних органів та організацій у сфері протидії кіберзлочинності як сучасного виду злочинності в Україні та за кордоном. У зв'язку з чим наразі активізуються питання щодо дослідження зарубіжного та міжнародного досвіду діяльності органів, уповноважених на вжиття заходів з протидії кіберзлочинності та забезпечення кібербезпеки держави.

Таким чином, необхідність удосконалення вітчизняного законодавства у сфері забезпечення кібербезпеки та протидії злочинності, недосконаліть нормативно-правового регулювання функціонування Департаменту кіберполіції Національної поліції України, а також недостатня кількість наукових розробок у зазначеній сфері обумовлюють наукові дослідження успішного зарубіжного досвіду діяльності уповноважених державних та міжнародних органів у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності.

Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, що обумовлюється необхідністю обміну досвідом на міжнародному рівні. Ці питання координуються кожною країною відповідно до розробленої та діючої стратегії кібербезпеки: Сполучені Штати Америки та більшість країн-учасниць Європейського Союзу у своїх стратегіях виносять питання боротьби з кіберзлочинністю на передові позиції [136, с. 55]. Відповідно наразі слушним є дослідження досвіду тих держав, котрі першими запровадили політику забезпечення кібербезпеки держави та протидії злочинності.

Насамперед, вбачаємо цілком слушним розпочати дослідження успішного (позитивного) зарубіжного досвіду діяльності органів поліції у

сфері протидії кіберзлочинності такої потужної держави як Сполучені Штати Америки (далі – США). Оскільки саме вказана держава стала однією з перших, хто визначив на національному рівні визначила та прийняла низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави. Причинами такого оперативного затвердження концепцій т стратегій протидії інформаційним злочинам та кібератакам стали події 11 вересня 2001 року, коли було скоєно серію терактів, членами терористичної організації «Аль-Каїда».

Першочергово зазначимо, що в США відсутнє єдине поліцейське управління, оскільки у кожному штаті діють свої закони та функціонують органи, діяльність яких може відрізнятися від функціонування аналогічних органів інших штатів. Так, Департамент кіберполіції Нью-Йорку, що створений у 1845 році, є одним із найбільших підрозділів муніципальної поліції США.

Структурно Департамент поліції штату Нью-Йорк складається із бюро та офісів, серед яких: Бюро патрульної служби [34], Бюро спеціальних операцій [37], Транзитне бюро [194], Бюро по боротьбі з тероризмом [35], Бюро по боротьбі зі злочинністю [36], Бюро детективів [33] та інші.

Окрему увагу слід приділити функціонуванню Бюро по боротьбі з тероризмом [35], оскільки його діяльність спрямована на захист штату від внутрішніх та міжнародних (зовнішніх) загроз терористичного характеру, а тому числі кіберзагроз. На території штату діє так звана «Команда критичного реагування», що здійснює: прогноз можливих кіберзагроз та загроз тероризму; здійснює розробку новаторською та довгострокової політики та механізмів захисту від кібератака, інформаційних та комп’ютерних злочинів; готує до оперативного втручання служби первинного реагування та спеціальні підрозділи; а також, нарощує потенціал розвідувальних спроможностей для виявлення та протидії кібератакам та терористичним загрозам. При цьому, слід вказати, що діяльність Команди критичного реагування здійснюється у відповідності з національним та

федеральним законодавством, а її функціонування координується федеральними, штатними та іншими правоохоронними органами з метою збору оперативної інформації щодо кібератак та загроз тероризму.

Команда критичного реагування Бюро по боротьбі з тероризмом є однією з перших груп оперативного реагування та захисту Департаменту поліції Нью-Йорка та штату від терористичних атак та кіберзагроз. Співробітники Команди критичного реагування, пройшовши відповідну спеціальну підготовку, мають навички володіння спеціальними видами зброї, в тому числі, великої дальності, виявлення слідів вибухових речовин, радіологічного та ядерного опромінення, обізнані про біологічну та хімічну зброю та оснащені технікою для виявлення кібератак. Команда критичного реагування Бюро по боротьбі з тероризмом з метою постійної готовності до нових кіберзагроз та загроз тероризму, проводить щоденні контр терористичні розгортання на критично важливих об’єктах інфраструктури по всьому штату Нью-Йорк.

Загалом, Бюро по боротьбі з тероризмом [35], має наступні повноваження:

1) розробка та реалізація великомасштабних контр терористичних проектів, та проектів протидії кіберзлочинності як: «Ініціатива з безпеки Нижнього Манхеттена», «Операція Sentinel»;

2) розробка і впровадження навчальних курсів по боротьбі з тероризмом, кібератаками включаючи курси для інших правоохоронних органів і організацій;

3) моніторинг сучасного стану кіберзагроз, визначення критично важливих об'єктів інфраструктури;

4) розробка стратегій захисту для приватного сектору;

5) дослідження та випробування нових інформаційних та комп’ютерних технологій, що використовуються для виявлення і боротьби з хімічною, біологічною, радіологічною, ядерною і вибуховою зброєю, а також для виявлення та боротьби із різними видами кіберзлочинності;

6) розробка планів і політики використання інформаційних та комп’ютерних технологій;

7) розробка систем і програм для підвищення безпеки на території порту; використання системи визначення характеристик тактичного радіологічного збору даних (TRACS) для про активного розгортання і картування фонового випромінювання в порту Нью-Йорк / Нью-Джерсі;

8) здійснення заходів управлінського державно-приватного партнерства в області безпеки штату, навчання та інформування для приватного сектора і вирішення проблем, пов'язаних з приватним сектором у сфері кіберзлочинності та протидії тероризму та деякі інші.

Також, слід зазначити, що окрім Команди критичного реагування Бюро по боротьбі з тероризмом, з метою протидії кіберзлочинності та тероризму в Бюро по боротьбі з тероризмом функціонують також такі групи: Об’єднана оперативна група з питань тероризму та кіберзлочинності; група забезпечення кібербезпеки Нижнього Манхеттена; та група з аналізу ризиків та загроз тероризму та кіберзлочинності. Кожна із зазначених груп виконує ряд своїх завдань та функцій, що в кінцевому підсумку спрямовані на вжиття заходів з протидії кіберзлочинності та тероризму.

Зокрема, Об’єднана оперативна група з питань тероризму та кіберзлочинності розслідує факти кіберзлочинності та тероризму, що вчиненні на території штату Нью-Йорк, а також здійснюють систематизацію вчинених злочинів та їх аналіз.

Група забезпечення кібербезпеки Нижнього Манхеттена призначена виявляти та попереджувати загрози кібератак та тероризму на території Нижнього Манхеттена.

Група з аналізу ризиків та загроз тероризму та кіберзлочинності здійснює заходи стратегічної розвідки щодо виявлення кібератак та загроз тероризму та веде їх аналіз.

Таким чином, при Департаменті поліції Нью-Йорка функціонує ряд поліцейських підрозділів, що здійснюють завдання протидії кіберзлочинності та тероризму.

В той же час, належний рівень функціонування поліцейських органів, що здійснюють заходи боротьби з кіберзлочинністю залежить від належного рівня їх нормативно-правового регулювання, що в США складає досить потужну базу для ефективної реалізації національної політики забезпечення кібебезпеки держави.

Так, на державному рівні в США прийняті такі важливі програмні документи, що створюють фундамент для боротьби з кіберзлочинністю, як: Міжнародна стратегія для кіберпростору «Процвітання, безпека, відкритість у мережевому світі» (2011); Кіберстратегія Міністерства оборони від квітня 2015 року; Міжвідомчий план дій з кібербезпеки систем управління (Cross-Sector Roadmap for Cybersecurity of Control Systems); План дій з посилення кібербезпеки найважливіших об’єктів інфраструктури (Roadmap for Improving Critical Infrastructure Cybersecurity, 2014); План дій з забезпечення кібербезпеки систем енергопостачання (Roadmap to Achieve Energy Delivery Systems Cybersecurity) [136, с. 55]. У 2016 році були прийняті Національний план з протидії кіберзлочинності [227] та Директива-41 Президентської політики (PPD-41) [235; 106, с. 198].

Зазначена нормативно-правова база заклала потужний фундамент для успішного виконання спеціалізованими суб’єктами своїх повноважень у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності.

Взявши до уваги позитивний досвід США, слід наголосити, що Україною, зокрема, Міністерством внутрішніх справ України та США, у напрямку протидії кіберзлочинності сьогодні здійснено ряд заходів. Зокрема, у січні 2020 року Міністр внутрішніх справ України та заступник держсекретаря США Джорган Ендрюс обговорили спільні напрями взаємодії щодо протидії наркозлочинності та кіберзлочинам [199]. В. В. Чумак з цього приводу вказує, що налагодження міжнародної співпраці з потужними

країнами світу безумовно є запорукою успішної імплементації міжнародного законодавства у сфері забезпечення кібербезпеки держави [205, с. 395]. При цьому, особлива увага приділяється функціонуванню такого органу в США є Федеральне бюро розслідувань (далі – ФБР), що головним суб'єктом забезпечення кібербезпеки держави та протидії кіберзлочинності на всій території США.

ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібер-вторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001 року [86]. Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина [209, с. 310].

З метою забезпечення кібербезпеки держави т протидії всім формам кіберзлочинності, в ФБР створені:

– кібер-відділ в штаб-квартирі ФБР для скоординованої і узгодженої боротьби з кіберзлочинністю;

– спеціально навчені кібер-дружини в штаб-квартирі ФБР і в кожному з офісів на місцях, де працюють з агентами і аналітиками, які захищають від і розслідування комп'ютерних вторгнень, крадіжки інтелектуальної власності та особистої інформації, дитячої порнографії та експлуатації, а також онлайн -шахрайства;

– нові групи по кібер-діям, які в будь-який момент подорожують по всьому світу, щоб допомогти у випадках комп'ютерного вторгнення з метою збору життєво важливих відомостей, що допомагають виявляти кіберзлочини, що є найбільш небезпечними для національної безпеки і для економіки;

– цільові групи з комп'ютерних злочинів, які поєднують в собі найсучасніші технології і ресурси федеральних, штатних і місцевих колег.

Реалізуючи програму по боротьбі з кіберзлочинністю, ФБР тісно співпрацює з Міністерством оборони та Міністерством національної безпеки, що часто вирішують схожі задачі. Для найбільш оперативного отримання інформації щодо вчинених комп’ютерних злочинів, у рамках ФБР створено Центр з прийому заяв стосовно вчинених інтернет-злочинів (Inernet Crime Complaint Center), де як потерпілі, так і треті особи, заповнивши спеціальну форму онлайн або просто зателефонувавши, можуть надати інформацію стосовно вчинених злочинів у мережі Інтернет [106, с. 199].

Також, при ФБР створено інтернет-центр скарг на кіберзлочини, місією якого є розгляд скарг на злочин в Інтернеті, надання громадськості надійний і зручний механізм звітності про підозрюваних, схеми шахрайства з використанням Інтернету і створення ефективних альянсів з правоохоронними органами та галузевими партнерами. Інформація аналізується і поширюється в слідчих і розвідувальних цілях серед співробітників правоохоронних органів і для інформування громадськості [86].

Кожен громадянина США має право подати скаргу до інтернет-центру скаргу на кіберзлочини, при цьому він має вказати наступні інформацію:

- ім'я жертви, адресу, телефон і адресу електронної пошти;

- інформацію про фінансові транзакції (наприклад, інформація про рахунок, дата і сума транзакції, хто отримав грошові кошти);

- ім'я суб'єкта, адреса, телефон, адреса електронної пошти, веб-сайт і IP-адреса;

- конкретні деталі того, як ви стали жертвою;

- обов’язково вказується тема електронної пошти

- будь-яка інша важлива інформація, яку ви вважаєте необхідною для підтримки вашої скарги.

Також на офіційному сайті інтернет-центру скарг на кіберзлочини, міститься розділ, що визначає поради по попередженню злочинності в мережі Інтернет. Так, розділ містить наступні теми:

- «Шахрайство на аукціоні»;
- «Фальшивий касовий чек»;
- «Шахрайство з кредитними картами»;
- «Ліквідація заборгованості»;
- «UPS DHL»;
- «Можливості працевлаштування / бізнесу»;
- Ескроу-Сервіс Шахрайство»;
- «Крадіжка особистих даних»;
- «Інтернет-вимагання»;
- «Інвестиційне шахрайство»;
- «Кібербулінг»;
- «Фішинг»;
- «Спам»;
- «Сторонній одержувач коштів» та деякі інші [77].

Також, з метою попередження вчинення кіберзлочинності, на офіційному сайті ФБР розміщені матеріали щодо захисту своїх персональних даних у віртуальному просторі. Зокрема, також є наявна інструкція захисту свого персонального комп’ютера від різних програм та шпигунського програмного забезпечення. Така інструкція передбачає наступні кроки для користувача:

1) тримайте брандмауер включеним: брандмауер захистить ваш комп'ютер від хакерів, які можуть спробувати отримати доступ, або зламати його, видалити інформацію або навіть вкрасти паролі або іншу конфіденційну інформацію. Програмні брандмауери широко рекомендуються для окремих комп'ютерів. Програмне забезпечення попередньо упаковано в деяких операційних системах або може бути придбано для окремих

комп'ютерів. Для кількох мережевих комп'ютерів апаратні маршрутизатори зазвичай забезпечують захист брандмауера;

2) встановіть або оновіть антивірусне програмне забезпечення. Антивірусне програмне забезпечення призначене для запобігання вбудовування шкідливих програм в ваш комп'ютер. Якщо він виявляє шкідливий код, такий як вірус або черв'як, він знімає або видаляє його. Віруси можуть заразити комп'ютери без відома користувача. Більшість типів антивірусного програмного забезпечення можна налаштувати для автоматичного оновлення;

3) встановіть або оновіть свою технологію захисту від шпигунських програм: шпигунські програми - це те програмне забезпечення, що таємно встановлюється на ваш комп'ютер, щоб дозволити іншим вдивлятися в ваші дії на комп'ютері. Деякі шпигунські програми збирають інформацію про вас без вашої згоди або створюють небажані спливаючі вікна у вашому веб-браузері. Деякі операційні системи пропонують безкоштовний захист від програм-шпигунів, а недороге програмне забезпечення легко доступно для завантаження через Інтернет або в вашому місцевому комп'ютерному магазині. Остерігайтеся реклами в Інтернеті, що пропонує завантажувані антишпигунські програми - в деяких випадках ці продукти можуть бути підробленими і можуть фактично містити шпигунське ПЗ або інший шкідливий код. Це схоже на покупку продуктів - магазин, де ви довіряєте;

4) підтримуйте свою операційну систему в актуальному стані: комп'ютерні операційні системи періодично оновлюються, щоб відповідати технологічним вимогам і усувати діри в безпеці. Обов'язково встановіть оновлення, щоб забезпечити новий захист вашого комп'ютера;

5) будьте уважні з тим, що ви завантажуєте: необережне завантаження вкладень електронної пошти може обійти навіть саме пильне антивірусне програмне забезпечення. Ніколи не відкривайте вкладення електронної пошти від кого-то, кого ви не знаєте, і будьте обережні з переадресацією

вкладень від людей, яких ви знаєте. Вони можуть мати мимоволі просунутий шкідливий код;

6) вимкніть комп'ютер. З ростом швидкості високошвидкісного підключення до Інтернету багато хто воліє залишати свої комп'ютери ввімкненими і готовими до дії. Недоліком є те, що «завжди включений» робить комп'ютери більш сприйнятливими. Крім того, відключення комп'ютера ефективно розриває з'єднання зловмисника - будь то шпигунське ПЗ або ботнет, який використовує ресурси вашого комп'ютера для зв'язку з іншими мимовільними користувачами.

Також, новелою у американському законодавстві у сфері кібербезпеки є затвердження програми ФБР щодо безпечного онлайн-серфінгу (FBI-SOS) - це загальнонаціональна ініціатива, покликана інформувати дітей 3-8 класів про кібернебезпеки, з якими вони стикаються в Інтернеті, і сприяти запобіганню злочинів проти дітей. Він просуває кібер громатні ідей та положення серед студентів, залучаючи їх у веселу, відповідну віку, конкурентоспроможну онлайн-програму, де вони вчаться безпечного і відповідального використання Інтернету.Програма підкреслює важливість питань кібербезпеки, таких як захист паролем, розумні звички серфінгу та захист особистої інформації. Аналогічні програми існують у Латвії [213, с. 146].

Зазначена програма має вигляд яскравих картинок для конкретного віку дітей з інтерактивними іграми. Кожна гра передбачає проходження по черзі рівнів гри, що мають відповідну назву.

Окрім зазначених дитячих програм та інструкцій, в США при ФБР функціонує проект «Безпечне дитинство», що реалізується спільно з Міністерством юстиції США.

Зазначений проект – це загальнонаціональна ініціатива з боротьби зі зростаючою епідемією сексуальної експлуатації та наруги над дітьми в мережі Інтернет, запущена міністерством юстиції в травні 2006 року. На чолі з офісами адвокатів США і Секцією по експлуатації і непристойності дітей

(CEOS), Кримінального відділу проекту «Безпечне дитинство» збираються федеральні, штатні і місцеві ресурси для кращого пошуку, затримання і переслідування осіб, які експлуатують дітей через Інтернет, а також для виявлення і рятувати жертв [156].

В рамках зазначеного проекту створена робоча група з питань протидії кібербулінгу, що має назву stopbullying.gov, та активно веде інтернет-блог з актуальних питань протидії кібербулінгу. Працівниками групи stopbullying.gov здійснюються систематичні заходи в школах та інших освітніх закладах, щоб допомогти учням дізнатися про профілактику кібербулінгу. Приклади занять з кібербулінгу включають в себе:

- Інтернет або бібліотечні дослідження, такі як пошук типів знущань, як їм запобігти і як діти повинні реагувати;

- Презентації, такі як мова або рольова гра про припинення кібербулінгу;

- Обговорення таких тем, як повідомлення про кібербулінг;

- Письменницька творчість, таке як вірш, що виступає проти кібербулінгу, або розповідь або пародія, навчальні свідків того, як допомогти;

- Художні твори, такі як колаж про повагу або наслідки від дії кібеобулерів;

- Зустрічі в класі, щоб поговорити про відносини з однолітками [159]. Також, в межах діяльності робочої групи постійно дії практичний дитячий психолог, який завжди готовий допомогти у скрутній для дитини ситуації.

Таким чином, в США при ФБР спільно з іншими державними органами створено ряд бюро та робочих груп з питань протидії кіберзлочинності з різними категоріями громадян та у відповідності до їх соціального статусу. Особливу цінність на наш погляд складає досвід щодо врегулювання питання забезпечення кібербезпеки дітей у Інтернет-просторі та протидії кібербулінгу.

Задовго до того, як кіберзлочинність була визнана серйозною загрозою злочинності для національної безпеки, ФБР підтримало ініціативу щодо створення перспективної організації для активного вирішення проблеми кіберзлочинності. Названа Національним альянсом по кібер-криміналістиці і навчання (NCFTA) організація, створена в 1997 році, що базується в Піттсбурзі, стала міжнародною моделлю для об'єднання зусиль правоохоронних органів, приватного сектора і наукових кіл для створення та обміну ресурсами, стратегічною інформацією і аналіз загроз для виявлення і припинення виникають кіберзагроз та вжиття заходів щодо їх протидії.

З моменту свого створення NCFTA розвивалася, щоб йти в ногу з мінливим ландшафтом кіберзлочинності. Сьогодні організація займається обробкою та протидією погроз з боку транснаціональних злочинних груп, включаючи спам, ботнети, схеми маніпулювання запасами, крадіжки інтелектуальної власності, фармацевтичне шахрайство, шахрайство в сфері телекомунікацій і інші схеми фінансового шахрайства, які призводять до збитків для компаній і споживачів в мільярди доларів.

Підрозділ Cyber Initiative and Resource (CIRFU) кібервідділу ФБР співпрацює з NCFTA, що спирається на інформацію сотень членів NCFTA з приватного сектора, аналітиків NCFTA, групи реагування на комп'ютерні інциденти (CERT) при Університеті Карнегі-Меллона та інтернету ФБР. Ця велика база знань допомогла CIRFU зіграти ключову стратегічну роль в деяких з найбільш значних кібер-справ ФБР за останні кілька років.

Навіть після виконання своїх обов'язків щодо забезпечення національної безпеки після 11 вересня ФБР продовжує грати ключову роль в боротьбі з насильницькими злочинами в великих містах і місцевих громадах по всій території Сполучених Штатів.

Через глобальне охоплення кіберзлочинності жодна організація, агентство або країна не можуть захиститися від нього. Життєво важливі партнерства, такі як NCFTA, є ключем до захисту кіберпростору і

забезпечення більш безпечного кібер-майбутнього для наших громадян і країн по всьому світу [86].

Оскільки кіберзагрози продовжують з'являтися майже кожного дня, для ФБР в області кримінальної та національної безпеки, вкрай важливо залучення державних і приватних партнерів щодо обміну інформацією поряд з правоохоронними та розвідувальними колами. Щоб залучити надійних галузевих партнерів в розвідувальну групу, ФБР спростило свою систему відстеження та управління погрозами Guardian з метою захищеного інформаційного порталу, що дозволяє окремим партнерам в галузі повідомляти про інциденти, пов'язані з кіберзлочинністю, в режимі реального часу.

iGuardian надає приватним компаніям стандартизований спосіб повідомляти інформацію в ФБР, якщо вони стають жертвами комп'ютерних вторгнень. Портал iGuardian - це еволюція платформи, через яку правоохоронні партнери ФБР надають потенційні загрози тероризму і повідомлення про підозрілі дії. У той час як eGuardian залучає співробітників правоохоронних органів, iGuardian був розроблений спеціально для партнерів в критичних секторах телекомунікацій, оборони, банківської справи та фінансів, а також в області енергетичної інфраструктури і доступний через чутливу, але несекретну мережу InfraGard.

InfraGard - це коаліція ФБР щодо захисту державної і приватної інфраструктури, в яку входять тисячі перевірених і націлених на галузь членів. Організація підтримує свою власну захищену мережу для поширення попереджень та бюлетенів ФБР і дозволяє обмінюватися інформацією про ключові загрози серед своїх членів. Використовуючи систему iGuardian, учасникам пропонується направляти інформацію про вторгнення безпосередньо в ФБР, в тому числі детальну інформацію про зараження шкідливим ПЗ, псування веб-сайтів і атаках типу «відмова в обслуговуванні». Програма iGuardian також надає партнерів InfraGard доступ до інформації та відомостями, отриманими в результаті пов'язаних інцидентів [26, с. 136].

Кожен звіт про інцидент в iGuardian направляється через Guardian в CyWatch, цілодобовий центр кібер-операцій ФБР, де агенти і аналітики сортують і знімають конфлікт з вхідних даних, повідомляють раніше невідомих жертв вторгнення і призначають висновки до відповідних польові офіси для подальшого розслідування. Таке централізоване управління кіберзлочинами в області кримінальної безпеки і національної безпеки дозволяє ФБР більш ефективно працювати з нашими партнерами, щоб використовувати відомі розвіддані і проводити розслідування і операції в очікуванні. Оскільки iGuardian надає важливий, додаткове джерело відповідної інформації про кібер-вторгнення, він також дозволяє сфокусуватися на загальному уявленні про загрозу, яку представляють терористи, національні держави і злочинні групи, які проводять мережеві операції проти США. Створення цієї широкої бази загроз обізнаність і партнерство дуже важливі для кібер місії ФБР [233].

Окрім, зазначеної платформи iGuardian, в США на постійній основі діє Національна об'єднана оперативна група з кібер-розслідувань (NCIJTF), що була офіційно створена в 2008 році. Національна об'єднана оперативна група по кібер-розслідувань складається з більш ніж 20 партнерських агентств з правоохоронних органів, розвідувального співтовариства та Міністерства оборони, представники яких знаходяться в одному місці і працюють спільно, щоб виконати місію організації з точки зору всього уряду. Будучи унікальним кібер-центром Національна об'єднана оперативна група з кібер-розслідувань несе головну відповідальність за координацію, інтеграцію та обмін інформацією для підтримки розслідувань кіберзагроз, надання та підтримки аналітичного аналізу для осіб, які приймають рішення в співтоваристві, і для забезпечення цінності інших поточних зусиль в боротьбі. проти кіберзагрози нації [126].

Національна об'єднана оперативна група з кібер-розслідувань також синхронізує спільні зусилля, спрямовані на виявлення, переслідування і знищення реальних терористів, шпигунів і злочинців, які прагнуть

експлуатувати системи нашої країни. Для досягнення цієї мети цільова група використовує колективні повноваження і можливості своїх членів і співпрацює з міжнародними партнерами і партнерами з приватного сектора, щоб задіяти всі наявні ресурси для боротьби з внутрішніми кіберзагрозами і їх виконавцями.

За допомогою координації, співпраці і обміну інформацією, яка відбувається в NCIJTF, члени уряду США працюють над тим, щоб посадити кіберзлочинців за ґрати і видалити їх з національних мереж. NCIJTF слід букві і духу закону, щоб забезпечити захист прав на недоторканність приватного життя всіх американців в ході розслідувань і зусиль, які він координує і підтримує [23, с. 231].

Підсумовуючи викладене, зазначимо, в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі.

Поряд з США активну боротьбу з кіберзлочинністю проводить в країнах Європейського Союзу (далі – ЄС). В ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору [136, с. 56].

Стратегія кібербезпеки ЄС була прийнята в 2013 році. Її особливістю є те, що стратегією були охоплені різні аспекти кіберпростору, зокрема, внутрішній ринок, правосуддя, внутрішня та зовнішня політика. Разом із Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС [211, с. 152].

Пріоритетами міжнародної політики ЄС у кіберпросторі визначені

– свобода та відкритість: стратегія визначає принципи користування основоположними правами людини та громадянина у кіберпросторі;

– застосування законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі. Відповідальність за безпеку кіберпростору лежить на усьому суспільстві: від звичайних громадян до цілих держав;

– розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством [229].

Зауважимо також, що в країнах ЄС активно створюються спеціальні органи боротьби з кіберзлочинністю. В загальному ці органи можна поділити на дві групи. Першу групу складають органи, що займаються формуванням та реалізацією національної політики по боротьбі з кіберзлочинністю. Другу групу складають органи, що здійснюють запобігання та розслідування злочинів, що вчиняються в кіберпросторі [136, с. 56].

Поряд з успішним досвідом протидії кіберзлочинності у США, заслуговує на увагу досвід забезпечення кібербезпеки у Франції, що наразі є активною державою забезпечення прав у віртуальному просторі.

Першочерговим наголосимо, що фахівці правоохоронних органів Франції виділяють дві форми кіберзлочинності. Перша з них – 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 та інші. Друга форма кіберзлочинів – вважається більш розвинутою і динамічною, використовує глобальні інформаційні мережі. До неї відносять розповсюдження сайтів, пов’язаних з наступним контентом:

− дитячою порнографією;

− збутом наркотиків;

− расистською, ксенофобною або антисемітської спрямованістю;

− терористичного толку;

− про замахи на приватне життя;

− з інструкціями з експлуатації вибухових речовин;

− повідомлень, реклами в шахрайських цілях [9, с. 174].

Міністром внутрішніх справ Франції Мішель Алліот-Марі 14 лютого 2008 року була оприлюднена французька Стратегія з питань боротьби з кіберзлочинністю. Мета Стратегії – співпраця між приватним бізнесом (постачальниками інформаційно-телекомунікаційних послуг) та правоохоронними органами з обміну інформацією та питаннях щодо об’єднання зусиль у боротьбі з кіберзлочинністю [28, с. 2; 29, с. 241].

У 2015 році Франція прийняла Національну стратегію інформаційної безпеки. Вона спрямована на супровід переходу французького суспільства до цифрових технологій і на рішення нових завдань, пов'язаних зі зміною використання цифрових технологій і викликаними цим погрозами. У ній виділено п'ять напрямків роботи:

- забезпечення державного суверенітету

- ефективне реагування на зловмисні дії в комп'ютерних системах і мережах;

- інформування широкої громадськості;

- перетворення інформаційної безпеки в конкурентну перевагу французьких підприємств;

- підвищення впливу Франції на міжнародній арені.

Цю стратегію доповнили:

1) Міжнародна стратегія Франції в області інформаційних технологій, була представлена міністром Європи і закордонних справ в грудні 2017 року. У ній узагальнені всі стратегічні цілі, які Франція підтримує в області інформаційних технологій в трьох основних сферах: управління, економіка і безпека;

2) Стратегічний огляд з питань кіберзахисту, що складений генеральним секретарем з питань оборони і національної безпеки за дорученням прем'єр-міністра, був представлений в лютому 2018 року. У ньому визначається доктрина управління кіберкрізісамі. Огляд також роз'яснює цілі національної стратегії в області кіберзахисту, підтверджує

ефективність французької моделі і покладає основну відповідальність в цій галузі на державу [30, с. 316].

На технічному і оперативному рівні ефективності французької системи сприяє ряд учасників:

- Французьке агентство безпеки інформаційних систем (ANSSI), створене в 2009 році, є національним органом, що відповідає за кібербезпека. Виступаючи у французькому кіберпросторі як "рятівника", ANSSI забезпечує запобігання (в тому числі з нормативно-правової точки зору) і реагування на інциденти в сфері IT, що зачіпають стратегічно важливі установи. Агентство також забезпечує відпрацювання управління в кризових ситуаціях на національному рівні. В даний час в агентстві працює 600 чоловік, і його штат продовжує зростати.

- Міністерство збройних сил виконує подвійну місію по захисту мереж, що забезпечують його діяльність, і по інтеграції цифрового протидії в військові операції. З метою підтримки діяльності міністерства в цій сфері на початку 2017 року було створено штаб кіберзахисту (COMCYBER), переданий під командування начальника штабу збройних сил.

- Міністерство внутрішніх справ веде боротьбу з усіма формами кіберзлочинності, спрямованої як проти національних установ та інтересів, господарюючих суб'єктів і державних органів, так і проти фізичних осіб. З цією метою міністерство спирається на спеціалізовані центральні служби та територіальні мережі національної поліції, національної жандармерії і сил внутрішньої безпеки. Їм доручено ведення слідчої діяльності з метою виявлення та притягнення до судової відповідальності осіб, винних у зловмисних діях в комп'ютерних системах і мережах. Ці служби також беруть участь в профілактичній та інформаційній роботі з відповідним категоріям громадян.

У 2001 р Франція підписала, і в 2006 році ратифікувала Конвенцію по боротьбі з кібер-злочинністю Ради Європи (відому як Будапештська конвенція). В даний час країна гармонізує своє законодавство і розробляє

кілька законопроектів в області боротьби з кіберзлочинністю. Уряд Франції підтримує ідею спрощення юридичного співробітництва між країнами ЄС для полегшення обміну даними з метою боротьби з кіберзлочинністю [83].

Протягом останніх декількох років Франція повністю переформатувала свої пріоритети в області оборони і національної безпеки, з огляду на збільшення обсягу, рівня, інтенсивності та складності національних кібер-загроз, в тому числі кібер-злочинності, політичного і економічного шпигунства, нападів на найважливіші об'єкти інфраструктури, а також інших кібер-порушень. «Біла книга з питань національної оборони і безпеки» 2008 року була першим основоположним документом, адресованим виключно проблематики національних кібер-загроз як основного ризику для національної безпеки і суверенітету. У ній визначалися нові пріоритети, такі як запобігання і реагування на кібератаки, а також передбачалися інституційні зміни, необхідні для забезпечення національної безпеки [48, с. 40].

Штаб із кіберзахисту як один із суб’єктів забезпечення кібербезпеки держави визначив основні (ключові) поняття для сфери кібербезпеки. Кіберзахист- це всі дії, здійснювані з метою військового втручання або втручання в кіберпростір, щоб гарантувати ефективність дій збройних сил, виконання доручених місій і належне функціонування міністерства. Кіберзахист слід відрізняти від кіберзлочинності, яка відповідає всім традиційним і новим злочинам і злочинам, що вчиняються за допомогою цифрових мереж [57, с. 40].

Кіберпростір - це глобальна галузь, куди входять комірчастої мережі інфраструктур інформаційних технологій (включаючи Інтернет), телекомунікаційних мереж, комп'ютерних систем, процесорів і інтегрованих механізмів управління. Він включає в себе як цифрову інформацію, так і операторів онлайн-послуг [84].

Кібератаки: зловмисний акт злому в кіберпросторі. Кібератаки можуть бути діями ізольованого людини, групи, держави. Вони включають

дезінформацію, електронне шпигунство, який може послабити конкурентну перевагу нації, таємну модифікацію конфіденційних даних на поле бою або руйнування критично важливої інфраструктури країни (вода, електрика, газ, зв'язок). , Комерційні мережі). Кібер міністерства направлена на виявлення і протидія кібератакам, мета і призначення яких пов'язані з Міністерством оборони.

Безпека інформаційної системи: всі технічні та нетехнічні заходи захисту, що дозволяють інформаційній системі протистояти подіям, які можуть поставити під загрозу доступність, цілісність або конфіденційність збережених, оброблюваних або переданих даних і послуг пов'язані системи, які ці системи пропонують або роблять доступними [62, с. 42].

Штаб із кіберзахисту Франції (COMCYBER) є оперативним підрозділом, командувачем, органічно або функціонально, усіма силами кіберзахисту французьких армій. Що знаходиться під безпосереднім керівництвом начальника штабу оборони, COMCYBER відповідає за загальний кібер-маневр. Створений в 2017 році [74, с. 143].

Штаб із кіберзахисту Франції виконує наступні завдання:

- захист інформаційних систем, що знаходяться під відповідальністю начальника штабу оборони в якості компетентного органу з безпеки інформаційних систем;

- захист інформаційних систем Міністерства збройних сил, за винятком систем Генерального директорату зовнішньої безпеки (DGSE) і Управління військової розвідки і безпеки (DRSD);

- розробка, планування і проведення військових операцій з кіберзахисту під керівництвом заступника начальника штабу з «операціями»;

- внесок в розробку кадрової політики в області кіберзахисту;

- внесок армій і спільних організацій в національну та міжнародну політику в області кіберзахисту, зокрема в розробку і реалізацію планів співробітництва;

- визначення конкретних технічних потреб для кіберзахисту;

- узгодженість моделі кіберзахисту департаменту і загальної координації;

- розробка та управління резервом кіберзахисту.

Штаб із кіберзахисту Франції здійснює оперативний нагляд за майже 3400 кібер-комбатантами в міністерстві. Для виконання своїх місій, Штаб із кіберзахисту Франції має штат і має повноваження над трьома спільними організаціями: CALID, CASSI і CPROC.

CALID - Центр аналізу в області захисного комп'ютерного контролю (CALID) є експертом операційного центру в області захисного комп'ютерного контролю. Він контролює виявлення, обробку та реагування на кібератаки 24 години на добу. CALID також включає в себе експертний потенціал високого рівня. Він розгорнуто у Франції і за кордоном, в очікуванні або у відповідь на кризу

Місія CALID полягає:

- в захисті цифрового простору армій (комп'ютерних мереж, бойових систем, командних систем і т. д) від погроз і атак, спрямованих на нього. Він передбачає потенційні загрози і атаки, відстежує мережі для виявлення цих атак, а потім вживає заходів з протидії їм і збереженню оперативних завдань, які залежать від цих систем;

- він перевіряє чи оцінює якість, ефективність та узгодженість вимірюваних пристроїв і процедур безпеки;

- він розгортає зонди зброї і командних систем в операціях, шукає сліди атак на інформаційні системи;

- він координує спеціалізовані групи дій або дії мережевих адміністраторів.

CASSI – Центр аудиту безпеки інформаційних систем, є національним центром, чия місія з аудиту охоплює дві області: безпека інформаційних систем (SSI) і компрометація хибних сигналів (SPC). Він працює як на материковій Франції, так і за кордоном, а також на театрах зовнішніх операцій.

CASSI проводить аудит відповідності та допомагає сертифікувати інформаційні системи. Процес розслідування до або під час впровадження інформаційних систем включає діагностику, що веде до рекомендацій.

CPROC – Центр кіберзахисту і Центр оперативної підготовки (CRPOC) є основним гравцем в наборі і управлінні резервістів кіберзахисту. Він також відповідає за навчання персоналу, управління та служби (EMDS). Він відповідає за набір, управління і навчання резервів кіберзахисту. CRPOC, спільно з COMCYBER і збройними силами, також відповідає за організацію національних та міжнародних навчань з кіберзахисту, таких як: 1) щорічні спільні навчання DEFNET, в яких реалізується реалістичний і динамічний сценарій для перевірки координації між різними підрозділами департаменту в разі великої кібератаки; 2) вчення «НАТО блокує щити», яке об'єднує багато країн і направлено на оцінку можливостей захисту складної комп'ютерної мережі від кібератак, зроблених фіктивним державою.

Таким чином, з метою забезпечення кібербезпеки держави у Франції створено належну нормативно-правову базу функціонування уповноважених на забезпечення кібербезпеки держави органів. При цьому, захист кібернетичного простору та протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюється не лише органами поліції (жандармерії), але й також на рівні Міністерства оборони та спеціально створених органів.

Окрему увагу на наш погляд доцільно приділити дослідженню позитивного досвіду протидії кіберзлочинності як Німеччина, що є однією з провідних держав-членів ЄС.

Спочатку наголосимо, що Німеччина сьогодні досягла значних показників у сфері забезпечення кібербезпеки держави та протидії злочинності.

Німеччина продемонструвала прихильність пріоритету забезпечення безпеки і боротьби з кібер-злочинністю підписавши (в 2001 році) і ратифікувавши (у 2009 році) Міжнародну конвенцію по кібер-злочинів Ради

Європи, також відому, як Будапештська конвенція, а також зробивши ряд кроків для її реалізації в країні. Німеччина також підписала і ратифікувала Додаткові протоколи до Конвенції по кібер-злочинів, які криміналізують расистську і ксенофобську діяльність, здійснену за допомогою комп'ютерних систем. У своїй Національної стратегії кібер-безпеки Німеччина підтвердила свою прихильність подальших зусиль в області гармонізації міжнародного кримінального права на основі Будапештської конвенції [82].

У липні 2015 року в Німеччині був прийнятий Акт про інформаційну безпеку (IT Security Act), метою якого є запобігання шкоди найважливішим IT-систем, таким, наприклад, як системи Міністерства внутрішніх справ (BSI), провайдерів телекомунікаційних послуг, операторів критично важливих елементів інфраструктури та ін. в даний час, BSI займається реалізацією положень цього Акта, який включає в себе мінімальні стандарти кібербезпеки для понад 2000 критично важливих інфраструктурних компаній.

Відповідно до законодавства, такі мінімальні стандарти безпеки забезпечуються за рахунок розвитку доступності, автентичності, конфіденційності та цілісності систем кібер-безпеки в усій країні; підвищення рівня інтернет-безпеки для громадян; а також підвищеного рівня захисту критично важливих в національному масштабі елементів інфраструктури.

Крім іншого, в Німеччині діють і інші закони, що забороняють такі злочинні дії, як комп'ютерне шахрайство, фальсифікація даних, комп'ютерний саботаж, кібер-шпигунство, фішинг, а також інші подібні кібер-злочину, які, відповідно до національного законодавства, переслідуються нарівні з звичайними злочинами [82].

Протягом двох років після прийняття Акта всі згадані в ньому оператори зобов'язані реалізувати необхідні організаційні та технічні заходи безпеки для захисту своїх кібер-систем, їх компонентів або процесів, що мають відношення до функціонування таких систем. Серед зазначених

заходів - застосування найсучасніших технологічних новинок. Більш того, оператори критично важливих систем повинні проходити процедуру аудиту в сфері кібер-безпеки або процедуру сертифікації як мінімум кожні два роки. Також, вони отримують можливість самостійно пропонувати нові стандарти безпеки в своїй області діяльності [82].

Що стосується правоохоронної діяльності, в Німеччині створені достатні умови для протидії різним видам кібер-злочинності. NCAZ, BSI і BKA спільно працюють в області боротьби з кібер-злочинністю в національному масштабі. Зокрема, NCAZ об'єднує ресурси різних урядових агентств, в т.ч. Федеральної поліції і Федеральної розвідувальної служби, а також приватного сектора.

У свою чергу, національна стратегія кібер-безпеки 2011 року передбачає розвиток потенціалу правоохоронних органів, BSI, а також приватного сектора, в області боротьби з кіберзлочинністю, а також в галузі захисту країни від шпигунства і саботажу. У Німеччині створено «органи спільного реагування за участю приватного сектора і компетентних правоохоронних органів». Як вказується в Акті про інформаційну безпеку 2015 року, для успішної реалізації зазначених завдань будуть потрібні додаткові зусилля і подальший прогрес. В кінці 2017 року стане відомо, наскільки успішно співпрацювали до цього моменту уряд і приватний сектор, щоб значно знизити рівень кіберзлочинності. З огляду на все сказане, варто все ж зазначити, що залишається поки неясним, чи існують в країні успішні ініціативи в галузі навчання суддів, прокурорів, юристів, співробітників правоохоронних органів, криміналістів, і також інших фахівців [82].

Німеччина вступила до лав країн НАТО та надала альянсу власні кібер можливості в боротьбі з кібервзломами та електронної війною, повідомило в лютому 2019 року інформаційне агентство Agence France-Presse [50]. НАТО визначає кіберпростір як область конфлікту поряд із сушею, морем і повітрям, в зв'язку з почастішанням електронними атаками з боку держав, кіберзлочинців і так званих «хактівістів», а також з огляду на можливі

наслідки загроз. Серед країн, готових надати альянсу свої кібер спроможності, вже числяться США, Великобританія, Данія, Нідерланди, Латвія та Естонія [89, с. 287].

Цілями наступальних кібер операцій можуть бути будь-які підключені до інтернету об'єкти - від комп'ютерів і смартфонів до пристроїв, які контролюють ключові механізми на електростанціях і в транспортних мережах.

У липні 2017 року керівництво підрозділу безпеки військової авіації Німеччини започаткувало нову ініціативу щодо протистояння кіберзагроз після того, було оприлюднено дослідження, що показало, що хакери можуть зламувати військові літаки з допомогою недорого обладнання.

Представник німецького міністерства оборони повідомив, що розробка нової «авіаційної кібер експертизи» буде охоплювати всілякі області - від підвищення усвідомленості наслідків хакерських нападів до технічних досліджень і оснащення повітряних суден захисними системами.

У Німеччині також в рядах збройних сил з'явився кіберпідрозділ, діяльність якого буде спрямована на протистояння російським хакерам. Чисельність нової структури складе 13500 кіберзахисників, трохи менше, ніж німецький корпус морської піхоти, який налічує 16000 бійців [85].

Таким чином, в Німеччині з метою забезпечення кібербезпеки держави створено ряд спеціальних органів, зокрема – кібернетичну авіацію, що є важливою складовою протидії кіберзлочинності.

З метою посилення кібербезпеки країн Європейського союзу, Єврокомісія запропонувала в вересні 2017 року пакет заходів, що включає створення Агентства кібербезпеки ЄС і введення сертифікатів для продукції, що випускається в ЄС цифрової продукції і послуг. Сьогодні зазначене агентство успішно функціонує на території країн-членів ЄС.

Агентство ЄС з кібербезпеки у відповідності зі Стратегією ЄС керується у своїй діяльності також прийнятою Директивою ЄС з інформаційної безпеки [69]. В межах зазначеної Директиви ЄС, створено

групу реагування на кіберінциденти як групу стратегічної співпраці, в якій держави-члени ЄС співпрацюють, обмінюються інформацією і домовляються про те, як послідовно виконувати директиву по всьому ЄС. Група реагування на кіберінциденти також дає стратегічне керівництво основної мережі CSIRT ЄС. Членами групи реагування на кіберінциденти є представники відповідних національних міністерств і національних агентств з кібербезпеки.

Окрім, зазначених держав, на початку березня 2020 роки шість європейських країн підписали угоду, щоб створити загальні кібернетичні війська, очолювані Литвою. Так, Естонія, Литва, Хорватія, Польща, Нідерланди та Румунія підписали меморандум про взаєморозуміння в Загребі, де відбулася неформальна зустріч міністрів оборони ЄС. Відповідно до угоди, в усіх цих країнах будуть створені міжнародні команди, готові відповісти на кібератаку в будь-який час. Меморандум на законних підставах дозволяє використовувати ці сили в юрисдикціях різних країн, визначає механізм роботи команд, їх правовий статус, роль і процедури [221].

При цьому зазначимо, Литва підняла ідею створення сил швидкого реагування на кіберзагрози в ЄС ще в 2017 році. Багатонаціональна організація для реагування на кіберінциденти, що складається з литовців, голландців, поляків і румунів, знаходиться в режимі очікування з початку 2020 року. Нещодавно створені кібергрупи, названі Групою загальноєвропейського реагування в кіберпросторі (European Union Cyber Rapid Response Teams, CRRT), стали частиною організації Постійного структурованого співробітництва Європейського Союзу (PESCO), заснованої в 2018 році. Вона дозволяє державам-членам ЄС розширювати співпрацю в області оборони [228].

Таким чином, підсумовуючи, зазначимо, що важливою умовою для успішної діяльності Департаменту кіберполіції Національної поліції України є врахування специфіки різних видів діяльності органів влади щодо забезпечення кібербезпеки за кордоном, а також вибір оптимальних форм і

методів та способів протидії кіберзлочинності, що базуються на міжнародних принципах та стандартах.

3.2. Шляхи удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції в Україні

Дослідження успішного зарубіжного досвіду нормативно-правового забезпечення та особливостей діяльності органів поліції щодо протидії кіберзлочинності та забезпечення кібербезпеки держави свідчить про те, що наразі в Україні доцільно переглянути існуючі законодавчі положення у сфері забезпечення кібербезпеки держави з урахуванням реальних та потенційних кіберзагроз національній безпеці України. Зокрема, зважаючи на необхідність оптимізації загальнодержавної системи протидії кіберзлочинності, доцільно звернути увагу на те, що одним із пріоритетних напрямів державної політики у зазначеній сфері є реалізація в законодавстві запобіжних важелів, спрямованих на виявлення та усунення причин і умов, що породжують кіберзлочинність, викриття ознак злочинних проявів у віртуальному просторі, недопущення їх перетворення на реальні дії. Зважаючи на важливість вказаного виду діяльності для протидії кіберзлочинності, його правове регулювання потребує оптимізації [101, с. 238].

В умовах сьогодення, враховуючи особливості діяльності Департаменту кіберполіції Національної поліції України як основного суб’єкта забезпечення кібербезпеки держави, протидії кіберзлочинності та захисту прав та основоположних свобод у кіберпросторі, нагальним є перегляд існуючих законодавчих завдань кіберполіції Національної поліції України. Зокрема ми пропонуємо: визначити загальні та спеціальні завдання Департаменту кіберполіції Національної поліції України; завдання, що пов’язані та такі, що не пов’язані із державною таємницею; а також, завдання Департаменту кіберполіції у сфері протидії злочинності.

Запропоновано до загальних завдань Департаменту кіберполіції Національної поліції відносити: забезпечення публічної безпеки та публічного порядку; охорона основоположних прав і свобод людини, а також інтересів суспільства і держави; протидія кіберзлочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

До спеціальних завдань Департаменту кіберполіції Національної поліції України запропоновано віднести наступні: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, що будуть надходити по каналах Національної Цілодобової мережі контактних пунктів.

Наголошено, що до завдань, що не пов’язані із державною таємницею належать: формування та забезпечення реалізації державної політики щодо попередження та протидії кримінальним правопорушенням, механізм підготовки, вчинення або приховування яких передбачає використання електронно-обчислювальних машин (комп’ютерів), систем та комп’ютерних мереж і мереж електрозв’язку.

Серед завдань Департаменту кіберполіції Національної поліції України у сфері протидії злочинності у відповідності до кіберзлочинів, ми пропонуємо відносити: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); 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 (ст. 361-2); 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 (ст. 362); 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 (ст. 363); перешкоджання роботі електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) та деякі інші.

Поряд із визначенням завдань Департаменту кіберполіції Національної поліції України, ми пропонуємо визначити наступні його функції, а саме:

– адміністративна - організовує та контролює діяльність підпорядкованих підрозділів кіберполіції щодо виконання вимог законодавства України у сфері протидії кіберзлочинності;

– оперативно-розшукова - у межах своїх повноважень уживає необхідних оперативно-розшукових заходів щодо викриття причин і умов, які призводять до вчинення кримінальних правопорушень у сфері протидії кіберзлочинності; організовує виконання у межах компетенції доручень слідчого, прокурора щодо проведення слідчих (розшукових) дій і негласних слідчих (розшукових) дій у кримінальних провадженнях;

– нормотворча - уносить в установленому порядку пропозиції щодо вдосконалення законодавства у сфері протидії кіберзлочинності, а також бере участь у розробленні та опрацюванні проектів законодавчих та інших нормативно-правових актів у цій сфері;

– кадрова (наприклад, сприяє правильному підбору, розстановці, навчанню та вихованню кадрів Департаменту та підпорядкованих йому підрозділів);

– інформаційного забезпечення - забезпечує в порядку, передбаченому законодавством України, формування й наповнення інформаційних масивів даних, автоматизованих інформаційних систем відповідно до потреб службової діяльності; збирає, узагальнює, систематизує та аналізує інформацію про криміногенні процеси та стан боротьби зі злочинністю за напрямом діяльності Департаменту на загальнодержавному та регіональному рівнях; забезпечує своєчасний розгляд звернень і запитів громадян, підприємств, установ, організацій із питань, віднесених до компетенції кіберполіції, контроль за належним дотриманням порядку їх прийняття, реєстрації, обліку і розгляду;

– превентивна та профілактична - визначає, розробляє та забезпечує реалізацію комплексу організаційних і практичних заходів, спрямованих на запобігання та протидію кримінальним правопорушенням у сфері протидії кіберзлочинності; проводить серед населення роз'яснювальну роботу з питань дотримання законодавства України у сфері використання новітніх технологій, захисту і протидії кіберзагрозам у повсякденному житті.

Беручи до уваги успішний та досить позитивний досвіду протидії кіберзлочинності у США, доцільним вбачаємо запровадити в Україні аналогічний проект щодо безпеки дітей в мережі Інтернет. З цією метою необхідно запровадити на законодавчому рівні національну програму з безпечного інтернет-простору для дітей, де визначити ці та напрямки реалізації проекту, а також перспективи його запровадження в школах. В рамках зазначеного проекту доцільним вбачаємо розробку та впровадження аналогічної США інтерактивної гри, що спрямована на розвиток у дітей навичок щодо користування інформаційними технологіями та уникнення можливих кіберзагроз. Реалізацію вказаного проекту слушним вбачаємо покласти на співробітників превентивного блоку Національної поліції України.

Також, з метою успішної реалізації Департаментом кіберполіції Національної поліції України своїх завдань та функцій, слушним вбачаємо

створення інтернет-центру скарг на кіберзлочини, що повинен діяти при кожному управлінню кіберполіції в Україні. Зазначений інтернет-центр повинен працювати систематично 24/7 з метою оперативного реагування на кіберінциденти та факти кіберзлочинності та вжиття заходів щодо ліквідації форм кіберзлочинності.

Окрім зазначеного, з метою удосконалення практичної діяльності співробітників кіберполіції України необхідним є запровадження щорічних міжнародних навчань з питань кіберзахисту, що можуть проводитися у формі: міжнародного стажування, проведення міжнародних конференцій та симпозіумів, тренувань та навчань, а також спільних брифінгів та налагодження співпраці з міжнародними органами та установами з протидії кіберзлочинності.

Таким чином, з метою удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції Національної поліції України, ми пропонуємо:

– розробити та затвердити оновлену Стратегію забезпечення кібербезпеки держави та протидії злочинності, що буде визначати сучасні пріоритети у кібербезпековій сфері, кіберзагрози та можливі їх виклики, механізми прогнозування та аналізу кібератак на критично важливі об’єкти інфраструктури тощо;

– розробити та затвердити Закон України «Про систему національної кібербезпеки України», в якому визначити основні поняття для кібербезпекової сфери, структуру системи національної кібербезпеки, її об’єкти та суб’єктів здійснення, механізми реалізації тощо;

– розробити та прийняти Закон України «Про комплекс заходів, що здійснюються співробітниками Департаменту кіберполіції Національної поліції України у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності» з поміткою «для службового користування», оскільки діяльність Департаменту кіберполіції Національної поліції України здійснюється під грифом «таємно»;

– удосконалити існуючі механізми взаємодії Департаменту кіберполіції Національної поліції України та його міжрегіональних управлінь з іншими суб'єктами забезпечення кібербезпеки держави та протидії кіберзлочинності, зокрема: Службою безпеки України, територіальними управліннями Національної поліції (слідчими та управліннями та управліннями карного розшуку), іншими органами державної влади та інститутами громадянського суспільства. Зокрема, ми пропонуємо затвердити Концепцію взаємодії кіберполіції України з іншими органами державної влади, органами місцевого самоврядування та інститутами громадянського суспільства, де визначити напрямки їх взаємодії, форми та методи спільної діяльності тощо;

– удосконалити систему оперативного реагування на кіберзагрози, кібератаки та кіберінциденти з метою забезпечення адекватного реагування на реальні кіберзагрози безпеці України, стану правопорядку та протидії кіберзлочинності;

–визначити та закріпити на законодавчому рівні правовий статус співробітників Департаменту кіберполіції Національної поліції України з метою якісної реалізації ними своїх повноважень. В даному контексті окремої уваги слід приділити удосконаленню системи соціальних та трудових гарантій діяльності співробітників кіберполіції особливо у сучасних умовах удосконалення діяльності Національної поліції України та підвищення престижу поліцейської служби.

Зазначимо, що зазначені пропозиції не є вичерпними, а можуть бути змінені чи доповнені залежно від актуального стану кібербезпеки в державі. Загалом, сьогодні діяльність Департаменту кіберполіції Національної поліції України набуває докорінно іншого значення у зв'язку з удосконаленням їх діяльності та визначенням чітких притаманних лише їм завдань та функцій.

Розробка на доктринальному рівні зазначених пропозицій та рекомендацій у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності мають стати ключовими на найближчу історичну перспективу для успішного функціонування Департаменту кіберполіції

Національної поліції України. Тому наразі набувають актуальності питання особливостей адміністративно-правового забезпечення діяльності Департаменту кіберполіції Національної поліції України, їх адміністративно-правового статусу та організації їх функціонування у зв'язку з посиленням прагнень України до налагодження співпраці з міжнародними установами та організаціями у сфері протидії кіберзлочинності, досягнення оперативної злагодженості дій Департаменту кіберполіції Національної поліції України та інших правоохоронних органів та досягнення оптимального ступеня впорядкованості діяльності органів управління.

Висновки до розділу 3

Наголошено, що з метою удосконалення адміністративного національного законодавства, що регламентує діяльність Департаменту кіберполіції Національної поліції України є коригування, в першу чергу, основних завдань та функцій як базового та основного елементу їх адміністративно-правового статусу з урахуванням практики організації та діяльності аналогічних органів держав-членів ЄС з метою забезпечення кібербезпеки та протидії кіберзлочинності.

Аналіз функціонування органів та підрозділів, що здійснюють протидію кіберзлочинності у США, Франції, Німеччині, Латвії, Литві, Естонії, Хорватії, Нідерландах, дав підстави дійти висновку, що у сучасних умовах сьогодення удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України є актуальним та своєчасним, що також підтверджується прагненням України налагодити міжнародну співпрацю у зазначеній сфері.

Встановлено, що ФБР є провідним федеральним агентством США з розслідування кібератак, що вчиняються злочинцями, зарубіжними противниками і терористами. Оскільки кібер-вторгнення стають все більш поширеним явищем, сьогодні діяльність ФБР постійно удосконалюється, щоб краще протистояти терористичній загрозі після терактів 11 вересня 2001

року. Поряд із цим, одним із пріоритетних напрямків протидії кіберзлочинності в США є протидія торгівлі людьми, що здійснюється із застосуванням інформаційних технологій у віртуальному просторі та завдає шкоди охоронюваним законом правам та основоположним свободам людини й громадянина.

Визначено, що в США з метою ефективної боротьби з кіберзлочинністю та забезпечення кібербезпеки держави, створено належне правове поле діяльності спеціалізованих суб'єктів боротьби з кіберзлочинністю та створено дієву систему органів, основними функціями визначено забезпечення кіберзахисту та протидії всім проявам кіберзлочинності, що беззаперечно суттєво впливає на стан правопорядку в державі.

Наголошено на пріоритетах міжнародної політики ЄС у кіберпросторі, а саме: свобода та відкритість – тобто принципи користування основоположними правами людини та громадянина у кіберпросторі; застосування законодавства ЄС у кіберпросторі в тій самій мірі, як і у фізичному світі; розвиток потенціалу кібербезпеки через співробітництво з міжнародними партнерами та організаціями, приватним сектором та громадянським суспільством.

Кіберпростір в ЄС визначається як глобальна галузь, куди входять комірчастої мережі інфраструктур інформаційних технологій (включаючи Інтернет), телекомунікаційних мереж, комп'ютерних систем, процесорів і інтегрованих механізмів управління. Він включає в себе як цифрову інформацію, так і операторів онлайн-послуг.

Узагальнено зарубіжний досвід протидії кіберзлочинності в Франції, де повноцінно та досить ефективно функціонує Штаб із кіберзахисту, який виконує такі завдання:захист інформаційних систем, що знаходяться під відповідальністю начальника штабу оборони в якості компетентного органу з безпеки інформаційних систем; захист інформаційних систем Міністерства збройних сил, за винятком систем Генерального директорату зовнішньої

безпеки (DGSE) і Управління військової розвідки і безпеки (DRSD); розробка, планування і проведення військових операцій з кіберзахисту під керівництвом заступника начальника штабу з «операціями»; внесок в розробку кадрової політики в області кіберзахисту; внесок армій і спільних організацій в національну та міжнародну політику в області кіберзахисту, зокрема в розробку і реалізацію планів співробітництва; визначення конкретних технічних потреб для кіберзахисту; узгодженість моделі кіберзахисту департаменту і загальної координації; розробка та управління резервом кіберзахисту.

Розкрито, що з метою забезпечення кібербезпеки держави у Франції створено належну нормативно-правову базу функціонування уповноважених на забезпечення кібербезпеки держави органів. При цьому, захист кібернетичного простору та протидія кіберзлочинності вважаються пріоритетом для забезпечення національної безпеки Франції та здійснюється не лише органами поліції (жандармерії), але й також на рівні Міністерства оборони та спеціально створених органів.

У Німеччині з метою забезпечення кібербезпеки держави створено ряд спеціальних органів, зокрема – кібернетичну авіацію, що є важливою складовою протидії кіберзлочинності.

Беручи до уваги успішний та досить позитивний досвіду протидії кіберзлочинності у США, доцільним вбачаємо запровадити в Україні аналогічний проект щодо безпеки дітей в мережі Інтернет. З цією метою необхідно запровадити на законодавчому рівні національну програму з безпечного інтернет-простору для дітей, де визначити ці та напрямки реалізації проекту, а також перспективи його запровадження в школах. В рамках зазначеного проекту доцільним вбачаємо розробку та впровадження аналогічної США інтерактивної гри, що спрямована на розвиток у дітей навичок щодо користування інформаційними технологіями та уникнення можливих кіберзагроз. Реалізацію вказаного проекту слушним вбачаємо

покласти на співробітників превентивного блоку Національної поліції України.

Також, з метою успішної реалізації Департаментом кіберполіції Національної поліції України своїх завдань та функцій, слушним вбачаємо створення інтернет-центру скарг на кіберзлочини, що повинен діяти при кожному управлінню кіберполіції в Україні. Зазначений інтернет-центр повинен працювати систематично 24/7 з метою оперативного реагування на кіберінциденти та факти кіберзлочинності та вжиття заходів щодо ліквідації форм кіберзлочинності.

Окрім зазначеного, з метою удосконалення практичної діяльності співробітників кіберполіції України необхідним є запровадження щорічних міжнародних навчань з питань кіберзахисту, що можуть проводитися у формі: міжнародного стажування, проведення міжнародних конференцій та симпозіумів, тренувань та навчань, а також спільних брифінгів та налагодження співпраці з міжнародними органами та установами з протидії кіберзлочинності.

Таким чином, з метою удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції Національної поліції України, ми пропонуємо:

– розробити та затвердити оновлену Стратегію забезпечення кібербезпеки держави та протидії злочинності, що буде визначати сучасні пріоритети у кібербезпековій сфері, кіберзагрози та можливі їх виклики, механізми прогнозування та аналізу кібератак на критично важливі об’єкти інфраструктури тощо;

– розробити та затвердити Закон України «Про систему національної кібербезпеки України», в якому визначити основні поняття для кібербезпекової сфери, структуру системи національної кібербезпеки, її об’єкти та суб’єктів здійснення, механізми реалізації тощо;

– розробити та прийняти Закон України «Про комплекс заходів, що здійснюються співробітниками Департаменту кіберполіції Національної

поліції України у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності» з поміткою «для службового користування», оскільки діяльність Департаменту кіберполіції Національної поліції України здійснюється під грифом «таємно»;

– удосконалити існуючі механізми взаємодії Департаменту кіберполіції Національної поліції України та його міжрегіональних управлінь з іншими суб'єктами забезпечення кібербезпеки держави та протидії кіберзлочинності, зокрема: Службою безпеки України, територіальними управліннями Національної поліції (слідчими та управліннями та управліннями карного розшуку), іншими органами державної влади та інститутами громадянського суспільства. Зокрема, ми пропонуємо затвердити Концепцію взаємодії кіберполіції України з іншими органами державної влади, органами місцевого самоврядування та інститутами громадянського суспільства, де визначити напрямки їх взаємодії, форми та методи спільної діяльності тощо;

– удосконалити систему оперативного реагування на кіберзагрози, кібератаки та кіберінциденти з метою забезпечення адекватного реагування на реальні кіберзагрози безпеці України, стану правопорядку та протидії кіберзлочинності;

–визначити та закріпити на законодавчому рівні правовий статус співробітників Департаменту кіберполіції Національної поліції України з метою якісної реалізації ними своїх повноважень. В даному контексті окремої уваги слід приділити удосконаленню системи соціальних та трудових гарантій діяльності співробітників кіберполіції особливо у сучасних умовах удосконалення діяльності Національної поліції України та підвищення престижу поліцейської служби.

Зазначимо, що зазначені пропозиції не є вичерпними, а можуть бути змінені чи доповнені залежно від актуального стану кібербезпеки в державі. Загалом, сьогодні діяльність Департаменту кіберполіції Національної поліції України набуває докорінно іншого значення у зв'язку з удосконаленням їх діяльності та визначенням чітких притаманних лише їм завдань та функцій.

Розробка на доктринальному рівні зазначених пропозицій та рекомендацій у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності мають стати ключовими на найближчу історичну перспективу для успішного функціонування Департаменту кіберполіції Національної поліції України. Тому наразі набувають актуальності питання особливостей адміністративно-правового забезпечення діяльності Департаменту кіберполіції Національної поліції України, їх адміністративно-правового статусу та організації їх функціонування у зв’язку з посиленням прагнень України до налагодження співпраці з міжнародними установами та організаціями у сфері протидії кіберзлочинності, досягнення оперативної злагодженості дій Департаменту кіберполіції Національної поліції України та інших правоохоронних органів та досягнення оптимального ступеня впорядкованості діяльності органів управління.

ВИСНОВКИ

У **дисертації** здійснено теоретичне узагальнення та запропоновано нове вирішення наукового завдання, що полягає у визначенні адміністративно-правового статусу Департаменту кіберполіції Національної поліції України, а також шляхів його удосконалення. Узагальнення зроблені в ході дослідження дозволили розробити та репрезентувати низку наукових положень:

1. Встановлено поняття та сучасний стан кібербезпеки в Україні, а також надано характеристику органів Національної поліції України як суб'єкта забезпечення кібербезпеки. Зокрема, визначено, що кіберпростір – це нове середовище для встановлення зв'язків суб'єктів правовідносин, який відрізняється від фізичного рядом специфічних ознак: 1) виникає в результаті функціонування інформаційних (автоматизованих), телекомунікаційних та інформаційно-телекомунікаційних систем ; 2) не має чітко визначених територіальних меж та кордонів (не може вважатися територією); 3) глобальність; 4) не передбачає фізичного контакту суб'єктів правовідносин, які можуть бути і не ідентифікованими; 5) комунікація за допомогою цифровізації зв'язків шляхом використання програмного та апаратного забезпечення на основі спеціальних протоколів.

Кібербезпека – це стан захищеності кіберпростору від реальних і потенційних загроз; охорони та захисту важливих інтересів людини і громадянина, суспільства та держави під час його використання як умови сталого розвитку інформаційного суспільства та цифрового комунікативного середовища. Цей стан досягається через діяльність по забезпеченню кібербезпеки, яка має вигляд заходів різнорідного характеру суб'єктів національної системи кібербезпеки, та суб'єктів, які безпосередньо здійснюють у межах своєї компетенції заходи із забезпечення кібербезпеки.

Доцільними для розмежування є категорії національної системи кібербезпеки та системи забезпечення кібербезпеки, з яких першу доцільно розуміти як сукупність всіх компонентів, за допомогою яких досягається кібербезпека: 1) суб'єктів та здійснюваних ними заходів (система забезпечення кібербезпеки), 2) об'єктів кібербезпеки та кіберзахисту як частини системи, які зазнають впливу з боку суб'єктів, 3) норм права, що є основою для забезпечення кібербезпеки через встановлення зв'язків між суб'єктом та об'єктом: прямих та зворотних.

2. Підхід до обмеження основних суб'єктів національної системи кібербезпеки та суб'єкту їх координації виключно інституціями держави доцільний для перегляду з точки зору необхідності врахування потреб всіх суб'єктів забезпечення кібербезпеки в Україні. Доцільним для організації є центр взаємодії та координації, що об'єднував би всіх суб'єктів забезпечення кібербезпеки на засадах партнерства.

Напрямами вирішення проблем забезпечення кібербезпеки Національною поліцією України доцільно визначити: 1) підвищення рівня оплати праці; 2) вирішення кадрового питання; 2) розробку вітчизняного програмного та матеріально-технічного забезпечення; 3) систематичне інформування про стан кібербезпеки, кіберзлочинність всіх зацікавлених суб'єктів; 4) налагодження координації та взаємодії суб'єктів забезпечення кібербезпеки на партнерських засадах як на національному, так і на міжнародному рівнях; 5) моніторинг кіберзагроз, кібератак та кіберінцедентів як основа для попередження кіберзлочинності, розробки методологічних рекомендацій по забезпеченню кібербезпеки, моделювання та прогнозування кібератак, виявлення та нейтралізації кіберзагроз; 6) удосконалення нормативно-правового регулювання забезпечення кібербезпеки, в тому числі доцільним для прийняття є спеціальний нормативно-правовий акт про кібер поліцію, яким би було докладно врегульовано статус відповідного міжрегіонального територіального органу поліції, включаючи принципи організації та діяльності, мету, завдання,

повноваження, компетенцію, особливості умов та підстав прийняття на службу, відповідальність та інші питання адміністративно-правового статусу органу та його службовців; 7) подальший розвиток міжнародного співробітництва у сфері забезпеченні кібербезпеки, включаючи співпрацю України та НАТО.

3. Адміністративно-правовий статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції являє собою характеристику правового положення відповідного суб'єкту забезпечення кібербезпеки та включає наступні елементи: 1) порядок утворення та припинення, найменування та місце в структурі апарату та механізму держави; 2) правові норми, які встановлюють статус Департаменту кіберполіції України як міжрегіонального територіального органу поліції; 3) принципи служби в поліції; 4) цілі та завдання; 5) компетенцію (предмет відання та функції), 6) повноваження; 7) правові форми і методи їх реалізації; 8) гарантії; 9) правові обмеження.

4. Визначено, що завдання та функції Департаменту кіберполіції Національної поліції України є важливою складовою визначення особливостей його діяльності та адміністративно-правового статусу, оскільки ефективне виконання Департаментом кіберполіції Національної поліції України своїх повноважень залежить від чіткого законодавчого розуміння його завдань та функцій як базового елемента адміністративно-правового статусу будь-якого органу державної влади.

Обґрунтовано під завданнями Департаменту кіберполіції Національної поліції України розуміти визначені на нормативно-правовому рівні шляхи досягнення конкретної мети діяльності, а саме – реалізація державної політики у галузі протидії кіберзлочинності, інформаційно-аналітичне забезпечення керівництва Національної поліції України та органів державної влади про стан вирішення питань, віднесених до компетенції кіберполіції.

Запропоновано до загальних завдань Департаменту кіберполіції Національної поліції відносити: забезпечення публічної безпеки та

публічного порядку; охорона основоположних прав і свобод людини, а також інтересів суспільства і держави; протидія кіберзлочинності; надання в межах, визначених законом, послуг з допомоги особам, які з особистих, економічних, соціальних причин або внаслідок надзвичайних ситуацій потребують такої допомоги.

До спеціальних завдань Департаменту кіберполіції Національної поліції України запропоновано віднести наступні: реалізація державної політики в сфері протидії кіберзлочинності; завчасне інформування населення про появу нових кіберзлочинців; впровадження програмних засобів для систематизації кіберінцидентів; реагування на запити зарубіжних партнерів, які будуть надходити по каналах Національної Цілодобової мережі контактних пунктів.

Запропоновано наступну класифікацію завдань Департаменту кіберполіції Національної поліції України у сфері протидії злочинності у відповідності до кіберзлочинів, а саме: несанкціоноване втручання в роботу електронно-обчислювальних машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку (ст. 361 КК України); створення з метою використання, розповсюдження або збуту шкідливих програмних чи технічних засобів, а також їх розповсюдження або збут (ст. 361-1); 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 (ст. 361-2); 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 (ст. 362); 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 (ст. 363); перешкоджання роботі електронно-обчислювальних

машин (комп'ютерів), автоматизованих систем, комп'ютерних мереж чи мереж електрозв'язку шляхом масового розповсюдження повідомлень електрозв'язку (ст. 363-1) та деякі інші.

5. Обґрунтовано, що права та обов’язки Департаменту кіберполіції Національної поліції України (повноваження) – це система визначених на нормативно-правовому рівні юридичних прав та юридичних обов’язків, якими наділяється Департамент кіберполіції Національної поліції України з метою реалізації покладених на нього завдань та функцій.

6. Запропоновано під територіальною юрисдикцією Департаменту кіберполіції Національної поліції України розуміти передбачене нормативно-правовими актами коло повноважень кіберполіції залежно від території, на яку поширюється їх юрисдикція.

З’ясовано, що за територіальною юрисдикцією управління кіберполіції Департаменту кіберполіції Національної поліції України поділяються: Подільське управління кіберполіції Національної поліції України охоплює обслуговування Хмельницької, Вінницької та Тернопільської областей. Поліське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Волинської, Рівненської та Житомирської областей. Придніпровське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Дніпропетровської, Кіровоградської та Запорізької областей. Донецьке управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Донецької та Луганської областей. Карпатське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Львівської, Івано-Франківської, Чернівецької та Закарпатської областей. Київське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування міста Києва, Київської, Черкаської та Чернігівської областей. Причорноморське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Одеської,

Миколаївської та Херсонської областей. Слобожанське управління кіберполіції Департаменту кіберполіції Національної поліції України охоплює обслуговування Сумської, Харківської та Полтавської областей .

7. Встановлено, що до юридичних гарантій діяльності Департаменту кіберполіції Національної поліції України віднесені: 1) юридичні гарантії професійної діяльності Департаменту кіберполіції; 2) правові гарантії діяльності Департаменту кіберполіції; 3) організаційні гарантії діяльності Департаменту кіберполіції; 4) матеріально-технічні гарантії діяльності Департаменту кіберполіції; 5) соціально-економічні гарантії діяльності Департаменту кіберполіції; 6) психологічні гарантії діяльності Департаменту кіберполіції.

8. Наголошено, що з метою удосконалення адміністративного національного законодавства, що регламентує діяльність Департаменту кіберполіції Національної поліції України є коригування, в першу чергу, основних завдань та функцій як базового та основного елементу їх адміністративно-правового статусу з урахуванням практики організації та діяльності аналогічних органів держав-членів ЄС з метою забезпечення кібербезпеки та протидії кіберзлочинності.

Аналіз функціонування органів та підрозділів, що здійснюють протидію кіберзлочинності у США, Франції, Німеччині, Латвії, Литві, Естонії, Хорватії, Нідерландах, дав підстави дійти висновку, що у сучасних умовах сьогодення удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України є актуальним та своєчасним, що також підтверджується прагненням України налагодити міжнародну співпрацю у зазначеній сфері.

Наголошено, що беручи до уваги успішний та досить позитивний досвіду протидії кіберзлочинності у США, доцільним вбачаємо запровадити в Україні аналогічний проект щодо безпеки дітей в мережі Інтернет. З цією метою необхідно запровадити на законодавчому рівні національну програму з безпечного інтернет-простору для дітей, де визначити ці та напрямки

реалізації проекту, а також перспективи його запровадження в школах. В рамках зазначеного проекту доцільним вбачаємо розробку та впровадження аналогічної США інтерактивної гри, що спрямована на розвиток у дітей навичок щодо користування інформаційними технологіями та уникнення можливих кіберзагроз. Реалізацію вказаного проекту слушним вбачаємо покласти на співробітників превентивного блоку Національної поліції України.

Встановлено, що з метою успішної реалізації Департаментом кіберполіції Національної поліції України своїх завдань та функцій, слушним вбачаємо створення інтернет-центру скарг на кіберзлочини, що повинен діяти при кожному управлінню кіберполіції в Україні. Зазначений інтернет-центр повинен працювати систематично 24/7 з метою оперативного реагування на кіберінциденти та факти кіберзлочинності та вжиття заходів щодо ліквідації форм кіберзлочинності.

9. З метою удосконалення національного законодавства, що регламентує діяльність Департаменту кіберполіції Національної поліції України, запропоновано:

– розробити та затвердити оновлену Стратегію забезпечення кібербезпеки держави та протидії злочинності, що буде визначати сучасні пріоритети у кібербезпековій сфері, кіберзагрози та можливі їх виклики, механізми прогнозування та аналізу кібератак на критично важливі об’єкти інфраструктури тощо;

– розробити та затвердити Закон України «Про систему національної кібербезпеки України», в якому визначити основні поняття для кібербезпекової сфери, структуру системи національної кібербезпеки, її об’єкти та суб’єктів здійснення, механізми реалізації тощо;

– розробити та прийняти Закон України «Про комплекс заходів, що здійснюються співробітниками Департаменту кіберполіції Національної поліції України у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності» з поміткою «для службового користування», оскільки

діяльність Департаменту кіберполіції Національної поліції України здійснюється під грифом «таємно»;

– удосконалити існуючі механізми взаємодії Департаменту кіберполіції Національної поліції України та його міжрегіональних управлінь з іншими суб'єктами забезпечення кібербезпеки держави та протидії кіберзлочинності, зокрема: Службою безпеки України, територіальними управліннями Національної поліції (слідчими та управліннями та управліннями карного розшуку), іншими органами державної влади та інститутами громадянського суспільства. Зокрема, ми пропонуємо затвердити Концепцію взаємодії кіберполіції України з іншими органами державної влади, органами місцевого самоврядування та інститутами громадянського суспільства, де визначити напрямки їх взаємодії, форми та методи спільної діяльності тощо;

– удосконалити систему оперативного реагування на кіберзагрози, кібератаки та кіберінциденти з метою забезпечення адекватного реагування на реальні кіберзагрози безпеці України, стану правопорядку та протидії кіберзлочинності;

– визначити та закріпити на законодавчому рівні правовий статус співробітників Департаменту кіберполіції Національної поліції України з метою якісної реалізації ними своїх повноважень. В даному контексті окремої уваги слід приділити удосконаленню системи соціальних та трудових гарантій діяльності співробітників кіберполіції особливо у сучасних умовах удосконалення діяльності Національної поліції України та підвищення престижу поліцейської служби.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Адміністративна відповідальність (загальні положення та правопорушення у сфері обігу наркотиків) : навч. посіб. / за заг. ред. І. П. Голосніченка. Київ : КІВС, 2003. 112 с.

2. Адміністративна діяльність органів внутрішніх справ. Загальна частина : підручник. Київ : Українська академія внутрішніх справ, 1995. 177 с.

3. Адміністративне право України. Академічний курс : підручник / [голова ред. кол. В. Б. Авер'янов]. Київ : Юридична думка, 2004. Т. 1. Загальна частина. 584 с.

4. Адміністративно-юрисдикційна діяльність Національної поліції України : навч. посіб. / за заг. ред. Засл. юриста України В. А. Глуховері. Дніпро : Дніпроп. держ. ун-т внутр. справ, 2016. 264 с.

5. Адміністративно-юрисдикційна діяльність поліції : навч. посіб. Київ : Центр учбової літератури, 2016. 336 с.

6. Александров Н. Г. Право и законность в период развернутого строительства коммунизма. М. : Госюриздат, 1961. 271 с.

7. Алексеев С. С. Право и перестройка: вопросы, раздумья, прогнозы. М. : Юрид. лит,1983. 234 с.

8. Алексеев С. С. Право: азбука – теория – философия : опыт комплексного исследования. М. : Статут, 1999. 243 с.

9. Арешонков В. В. Окремі міжнародно-правові проблеми боротьби з кіберзлочинністю в умовах глобалізації. *Вісник Луганського державного ун-ту внутр. справ*. 2013. № 5. Спецвип. С. 173–176.

10. Бандурка А. М., Тищенко Н. М. Административный процесс : учебник. Харьков : Нац. акад. внутр. справ, 2001. 352 с.

11. Барегамян С. Х. Система забезпечення безпеки кіберпростору в Україні. *Кібербезпека та системи захисту інформації: виклики сьогодення* :

зб. матеріалів круглого столу (м. Маріуполь, 26 жовт. 2017 р.) / [уклад. Ы. Б. Тимофєєва] ; Маріупольський державний університет ; Кафедра математичних методів та системного аналізу. Маріуполь, 2017. С. 23–26.

12. Бахрах Д. Н. Государственная служба: основные понятия, ее составляющие, содержание, принципы. *Государство и право*. 1996. № 12. С. 10–18.

13. Береза В. В. Поняття та класифікація повноважень Департаменту кіберполіції Національної поліції України. *Вісник Харківського національного університету внутрішніх справ*. 2018. № 3 (82). С. 30–39.

14. Береза В. В. Принципи діяльності Департаменту кіберполіції Національної поліції України: теоретико-правові аспекти. *Форум права* : електрон. наук. фахове вид. 2017. № 5. С. 44–48. URL: http://nbuv.gov.ua/UJRN/FP_index.

15. Береза В. В. Щодо визначення функцій департаменту кіберполіції Національної поліції України. *Держава та регіони*. Серія : Право. 2019. № 1 (63). С. 66–70.

16. Берлач Н. А. Трансформація відносин між виконавчою владою та суспільством у процесі здійснення адміністративної реформи в Україні. *Університетські наукові записки*. 2012. № 1. С. 509–515.

17. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96–102.

18. Білобров Т. В. Роль та місце департаменту кіберполіції національної поліції України у системі суб’єктів забезпечення кібербезпеки держави. *Правові новели*. 2020. № 11. С. 122–128.

19. Білобров Т. В. Сучасний стан та перспективи забезпечення кібербезпеки в Україні Національною поліцією. *Юридична наука України: історія, сучасність, майбутнє* : міжнар. наук.-практ. конф. (м. Харків, 1–2 листоп. 2019 р.). Харків, 2019. С. 78–80.

20. Білобров Т. В. Права та обов’язки департаменту кіберполіції національної поліції України як елемент адміністративно-правового статусу.

Право як ефективний суспільний регулятор : матеріали міжнар. наук.-практ. конф. (м. Львів, 14–15 лют. 2020 р.). Львів, 2020. С. 45–47.

21. Битяк Ю. П. Напрями розвитку системи державного управління та її правове забезпечення. *Теорія та практика державного управління*. 2014. Вип. 4. С. 10–20.

22. Богачова Л. Л. Юридичні гарантії прав і свобод людини і громадянина в європейському та національному праві. *Державне будівництво та місцеве самоврядування.* 2011. Вип. 22. С. 56–70.

23. Богданов С. С. Международно-правовые инструменты регулирования отношений в киберпространстве в условиях глобализации. *Вісник Луганського державного ун-ту внутрішніх справ*. 2013. № 5. Спецвип. С. 230–233.

24. Боднарчук В. Сутність і зміст поняття "компетенція" в державному управлінні. *Державне управління та місцеве самоврядування*. 2016. Вип. 2. С. 19–26.

25. Бородін І. Л. Права та свободи громадян, їх класифікація, гарантії реалізації. *Право України.* 2001. № 12. С. 32–34.

26. Борьба с преступностью в Интернете (онлайновая преступность). Інформаційний бюлетень Міжвід. наук.-дослід. центру з проблем боротьби з орг. злочинністю. 2006. № 7. С. 133–141.

27. Бояринцева М. А. Адміністративно-правовий статус громадянина України : дис. … канд. юрид. наук : 12.00.07. Київ, 2005. 213 с.

28. Бутузов В. М. Міжнародний досвід : ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. 2008. С. 1–5. URL: file:///C:/Users/User/Downloads/boz_2008_19_28.pdf.

29. Бутузов В. М. Міжнародний досвід: ініціатива правоохоронних органів Франції з протидії комп'ютерній злочинності. *Боротьба з організованою злочинністю і корупцією (теорія і практика).* 2009. № 19. С. 240–247.

30. Бутузов В. М. Сучасні загрози: комп'ютерний тероризм. *Боротьба з організованою злочинністю і корупцією (теорія і практика)*. 2007. № 17. С. 316–325.

31. Бухарєв В. В. Адміністративно-правові засади забезпечення кібербезпеки України : дис. ... канд. юрид. наук : 12.00.07. Суми, 2018. 221 с.

32. Буяджи С. А. Правове регулювання боротьби із кіберзлочинністю: теоретико-правовий аспект : дис. ... канд. юрид. наук : 12.00.01. Івано-Франківськ, 2018. 203 с.

33. Бюро детективів : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/investigative/detectives.page.

34. Бюро патрульної служби : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/patrol/patrol-landing.page.

35. Бюро по боротьбі з тероризмом : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page.

36. Бюро по боротьбі зі злочинністю : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/investigative/crime-control-strategies.page.

37. Бюро спеціальних операцій : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/patrol/citywide-operations.page.

38. Валюшко І. О. Кібербезпека України: наукові та практичні виміри сучасності. *Вісник Національного технічного університету України «Київський політехнічний інститут»*. Політологія. Соціологія. Право. 2016. № 3–4. С. 117–124.

39. Васильев А. С. Административное право Украины (Общая часть) : учеб. пособ. Харьков : Одиссей, 2001. 288 с.

40. Великий тлумачний словник сучасної української мови (з дод., допов. та CD) / [уклад. і голов. ред. В. Т. Бусел]. Київ ; Ірпінь : Перун, 2009. 1736 с.

41. Верин А. Ю. К вопросу о структуре правового статуса личности. *Вестник экономики, права и социологии*. 2012. № 2. С. 113–116.

42. Винник О. В. Повноваження штабних підрозділів органів внутрішніх справ. *Форум права* : електрон. наук. фахове вид. 2014. № 4. С. 38–42. URL: http://nbuv.gov.ua/UJRN/FP_index.htm_2014_4_9.

43. Витрук Н. В. Общая теория правового положения личности. М. : НОРМА, 2008. 624 с.

44. Витрук Н. В. Правовой статус личности в СССР. М. : Юрид. лит., 1985. 176 с.

45. Вінаков А. В. Зміст підготовки фахівців для підрозділів боротьби з кіберзлочинністю в в сучасних умовах. *Використання інноваційних технологій у попередженні злочинів* : матеріали наук.-практ. семінару (м. Харків, 6 груд. 2012 р.) / МВС України ; Харк. нац. ун-т внутр. справ. Харків, 2012. С. 34–36.

46. Войтович Н. Суб'єктивні права людини та громадянина в науковій інтерпретації Б. Кістяківського. *Юридичний вісник.* 2014. № 6. С. 234–238.

47. Воронін Я. Г. Дозвільна діяльність у нафтогазовому комплексі України: адміністративно-правовий аспект : дис. … д-ра юрид. наук : 12.00.07. Харків, 2016. 486 с.

48. Гавловський В. Д., Тітуніна К. В. Актуальні питання міжнародного співробітництва у боротьбі з комп'ютерною злочинністю. *Організація протидії у сфері інтелектуальної власності та комп'ютерних технологій* : доповіді провідних вчених, представників громадськості, державних службовців та працівників підрозділів ДСБЕЗ на міжвід. сем. Київ, 2009. С. 36–42.

49. Гарчева Л. П., Ярмыш А. Н. Конституционное право Украины : учеб. пособ. Симферополь : ДОЛЯ, 2000. 336 с.

50. Германия поделится с НАТО своими кибервозможностями. *SecurityLab.ru. Новости* : [сайт]. URL: https://www.securitylab.ru/news/497967.php.

51. Гібридна війна і журналістика. Проблеми інформаційної безпеки : навч. посіб. / [ред.-упор. : О. І. Харитоненко, Ю. С. Полтавець] ; за заг. ред. В. О. Жадька. Київ : НПУ імені М. П. Драгоманова, 2018. 356 с.

52. Голіна В. В., Головкін Б. М. Кримінологія. Загальна та особлива частини : навч. посіб. Харків : Право, 2014. 513 с.

53. Голосніченко І. П., Голосніченко Д. І. Теорія повноважень, їх легітимність та врахування потреб і інтересів при встановленні на законодавчому рівні. *Вісник НТУУ «КПІ».* Політологія. Соціологія. Право : зб. наук. праць. 2011. № 1 (9). С. 147–155.

54. Гончаренко О. І. Правоохоронна діяльність щодо попередження кіберзлочинів. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. матеріалів Всеукр. наук.-практ. конф. (23 листоп. 2018 р., м. Харків) / МВС України ; Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 29–32.

55. Гребенюк М. В. Деякі питання організаційно-правового забезпечення кібербезпеки: огляд кращих практик зарубіжного досвіду. *Підприємництво, господарство і право.* 2019. № 2. С. 203–207.

56. Грицун О. О. Безпека в кіберпросторі: міжнародно-правові аспекти. *Науковий вісник Херсонського державного університету.* Серія : Юридичні науки. 2014. Вип. 6–1, т. 4. С. 197–202.

57. Грубий М. В. Шляхи вдосконалення міжнародного співробітництва у сфері протидії кіберзлочинності. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ: стан, проблеми та шляхи вирішення* : матеріали всеукр. наук.-практ. конф. (9 груд. 2011 р.). Донецьк, 2012. С. 39–42.

58. Грушевський В. А. Адміністративно-правовий статус регіональних управлінь Державної фіскальної служби України : дис. ... канд. юрид. наук : 12.00.07. Харків, 2016. 212 с.

59. Гумін О. М., Пряхін Є. В. Адміністративно-правовий статус особи: поняття та структура. *Наше право*. 2014. № 5. С. 32–37.

60. Гусаров С. М. Адміністративно-юрисдикційна діяльність органів внутрішніх справ : дис. ... д-ра юрид. наук : 12.00.07. Київ, 2009. 432 с.

61. Даль В. И. Толковый словарь русского языка. М. : Эксмо, 2011. 896 с.

62. Дейнека П. В. Використання зарубіжного досвіду в розкритті комп'ютерних злочинів. *Протидія злочинності у сфері інтелектуальної власності та комп'ютерних технологій органами внутрішніх справ : стан, проблеми та шляхи вирішення* : матеріали всеукр. наук.-практ. конф. (9 груд. 2011 р.) Донецьк, 2012. С. 42–45.

63. Демедюк С. В. Адміністративно-правове регулювання відносин у сфері забезпечення кібербезпеки в Україні. *Південноукраїнський правничий часопис*. 2015. № 3. С. 119–123.

64. Демедюк С. В. Окремі питання адміністративно-правового та організаційного забезпечення кібербезпеки. *Південноукраїнський правничий часопис*. 2015. № 2. С. 144–147.

65. Демедюк С. В., Марков В. В. Кіберполіція України. *Наше право*. 2015. № 6. С. 87–93.

66. Денисюк Д. С. Завдання Національної поліції України: проблеми законодавчого закріплення. *Підприємництво, господарства і право.* 2016. № 8. С. 100–104.

67. Денисюк Д. С. Функції Національної поліції України: поняття та класифікація. *Юридичний науковий електронний журнал*. 2016. № 4. С. 114–117. URL: http://lsej.org.ua/4_2016/32.pdf.

68. Департамент кіберполіції : [сайт]. URL: https://cyberpolice.gov.ua/contacts/.

69. Директива (ЕС) 2016/1148 Европейского парламента и Совета от 6 июля 2016 года о мерах по обеспечению высокого общего уровня безопасности сетевых и информационных систем в рамках Союза. *Доступ к законодасельству Европейского Союза* : [сайт]. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

70. Діордіца І. В. Система забезпечення кібербезпеки: сутність та призначення. *Підприємництво, господарство і право*. 2017. № 7. С. 109–116.

71. Діордіца І. В. Адміністративно-правове регулювання кібербезпеки України : автореф. дис. ... д-ра юрид. наук : 12.00.07. Запоріжжя, 2018. 32 с.

72. Діордіца І. В. Основні поняття та ідеї кібернетики як засади виділення кібернетичної функції держави. *Науковий вісник Міжнародного гуманітарного університету.* Серія : Юриспруденція. 2017. Вип. 30 (1). С. 86–88.

73. Елистратов А. И. Понятие о публичном субъективном праве. М. : Печ. А. И. Снегиревой, 1913. 39 с.

74. Жевелєва І. С. Зарубіжний досвід взаємодії правоохоронних органів із суб'єктами господарювання у процесі захисту інформації з обмеженим доступом. *Боротьба з організованою злочинністю і корупцією (теорія і практика*). 2014. № 1. С. 140–145.

75. Загородня Н. В. Адміністративно-правовий статус громадян України. *Науковий вісник Міжнародного гуманітарного університету*. Серія : Юриспруденція. 2018. Вип. 33. С. 75–77.

76. Иоффе О. С., Шаргородский М. Д. Вопросы теории права. М. : Госюриздат, 1961. 380 с.

77. Інтернет-центр скарг на кіберзлочини : [сайт]. URL: https://www.ic3.gov/preventiontips.aspx.

78. Інформаційна та кібербезпека: соціотехнічний аспект : підручник / [В. Л. Бурячок, В. Б. Толубко, В. О. Хорошко, С. В. Толюпа] ; за заг. ред. д-ра техн. наук, проф. В. Б. Толубка. Київ : ДУТ, 2015. 288 с.

79. Камчатний М. В. Основні ознаки поняття "кібервійна" в сучасному міжнародному праві. *Альманах міжнародного права*. 2017. Вип. 15. С. 12–22.

80. Каримова Р. Р. Юридические обязанности: сущность и проблемы реализации : автореф. дис. … канд. юрид. наук : 12.00.01. Екатеринбург, 2008. 22 с.

81. Карманюк О. П. Юридичні обов'язки і законність: теоретичні аспекти взаємодії. *Science and Education a New Dimension. Humanities and Social Sciences*. 2016. IV(16), I.: 95. С. 15–19. URL: https://seanewdim.com/uploads/3/4/5/1/34511564/karmanyuk_o._legal_duties_and_legality_theoretical_aspects_their_interaction.pdf.

82. Киберготовность Германии 2.0: киберпреступность и охрана правопорядка. *Digital* : [сайт]. URL: https://digital.report/kibergotovnost-germanii-2-0-kiber-prestupnost-i-ohrana-pravoporyadka/.

83. Киберготовность Франции 2.0: киберпреступность и охрана правопорядка. *Digital* : [сайт]. URL: https://digital.report/kibergotovnost-frantsii-2-0-kiberprestupnost-i-ohrana-pravoporyadka/.

84. Киберзащита: главная проблема для отдела. *Кибер-центр* : [сайт]. URL: https://www.defense.gouv.fr/portail/enjeux2/la-cyberdefense/la-cyberdefense/presentation.

85. Киберпреступность и киберконфликты : Европа. *TAdviser* : [сайт]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B0#.D0.AD.D1.81.D1.82.D0.BE.D0.BD.D0.B8.D1.8F.2C_.D0.9F.D0.BE.D0.BB.D1.8C.D1.88.D0.B0.2C_.D0.A5.D0.BE.D1.80.D0.B2.D0.B0.D1.82.D0.B8.D1.8F.2C_.D0.9D.D0.B8.D0.B4.D0.B5.D1.80.D0.BB.D0.B0.D0.BD.D0.B4.D1.8B.2C_.D0.A0.D1.83.D0.BC.D1.8B.D0.BD.D0.B8.D1.8F_.D0.B8_.D0.9B.D0.B8.D1.82.D0.B2.D0.B0_.D1.81.D0.BE.D0.B7.D0.B4.D0.B0.D0.BB.D0.B8_.D0.BE.D0.B1.D1.89.D0.B8.D

0.B5_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B8.D0.B5_.D0.B2.D0.BE.D0.B9.D1.81.D0.BA.D0.B0.

86. Кибер-преступность. *ФБР* : [сайт]. URL: https://www.fbi.gov/investigate/cyber.

87. Кистяковский Б. А. Социальные науки и право. Очерки по методологии социальных наук и общей теории права. М. : Изд. М. и С. Сабашниковых, 1916. 704 с.

88. Кіберполіція. Завдання кіберполіції. *Департамент кіберполіції* : [сайт]. URL: https://cyberpolice.gov.ua/.

89. Кісілюк І. І. Міжнародне співробітництво у боротьбі з кіберзлочинністю. *Модернізація Конституції України та вдосконалення правоохоронної діяльності* : матеріали підсумк. наук.-практ. конф. (Київ. 25 квіт. 2014 р.) / Нац. акад. внутр. справ ; Нац. акад. прав. наук. Київ, 2014. С. 286–289.

90. Климков В. О. Організаційно-правові засади діяльності спеціального органу з питань банкрутства : дис. … канд. юрид. наук : 12.00.07. Київ, 2010. 205 с.

91. Ковалевіч І. П. Теоретичні засади забезпечення зворотного зв’язку в державному управлінні. *Державне будівництво*. 2008. № 2. URL: http://www.kbuapa.kharkov.ua/e-book/db/2008-2/doc/1/15.pdf.

92. Коваль Л. Адміністративне право України. (Загальна частина) : курс лекцій. Київ : Основи, 1994. 154 с.

93. Коваль Л. В. Административно-деликтное отношение. Киев : Вища школа, 1979. 230 с.

94. Комзюк А. Т. Заходи адміністративного примусу в правоохоронній діяльності міліції: поняття, види та організаційно-правові питання реалізації : монографія / за заг. ред. проф. О. М. Бандурки Харків : Нац. ун-т внутр. справ, 2002. 336 с.

95. Комзюк В. Т. Правові гарантії діяльності митних органів України. *Право і Безпека*. 2015. № 2. С. 70–74.

96. Комісаров О. Г. Процес цілепокладання в організації діяльності органів внутрішніх справ України на сучасному етапі розвитку : дис. … канд. юрид. наук : 12.00.07. Запоріжжя, 2002. 237 с.

97. Костюков А. Н. Должностное лицо: административно-правовой статус. *Изв. вузов. Правоведение.* 1987. № 2. С. 20–26.

98. Кримінальний кодекс України : Закон України від 05 квіт. 2001 р. № 2341-III. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2341-14#n2.

99. Крищенко А. Є. Завдання та функції Національної поліції як учасника адміністративно-правових відносин у сфері забезпечення публічної безпеки і порядку. *Науковий вісник Національної академії внутрішніх справ.* 2017. № 2 (103). С. 121–128.

100. Кряжков В. А. Конституционное правосудие в субъектах Российской Федерации (правовые основы и практика). М. : Формула права, 1999. 768 с.

101. Кудінов С. Шляхи удосконалення правового регулювання забезпечення Службою безпеки України антитерористичної безпеки. *Підприємництво, господарство і право.* 2019. № 2. С. 234–239.

102. Кузенко Л. В. Правове регулювання права громадян на інформацію в сфері державного управління : дис. … канд. юрид. наук : 12.00.07. Харків, 2003. 173 с.

103. Курко М. Н. Зміст державного управління (теоретико-правовий аспект). *Юридичний вісник. Повітряне і космічне право*. 2015. № 1. С. 36–40.

104. Лазарев Б. М. Компетенция органов управления / Академия наук СССР ; Институт государства и права. М. : Юрид. лит., 1972. 280 с.

105. Лазор О. Я., Хорошенюк О. В. Публічна служба в Україні: компетенції та повноваження : монографія. Хмельницький : ХЕПА, 2009. Ч. ІІ. 440 с.

106. Лапта С. П. ФБР у боротьбі з кіберзлочинністю. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : матеріали всеукр.

наук.-практ. конф. (Харків, 27 листоп. 2017 р.) / МВС України ; Харків. нац. ун-т внутр. справ. Харків, 2017. С. 197–199.

107. Лебідь Н. В. Адміністративно-правовий статус державних інспекцій в Україні : дис. … канд. юрид. наук : 12.00.07. Харків, 2004. 185 с.

108. Литвин О. В. Адміністративно-правове регулювання статусу державного службовця в Україні : автореф. дис. … канд. юрид. наук : 12.00.07. Ірпінь, 2009. 20 с.

109. Ліпкан В. А., Діордіца І. В. Національна система кібербезпеки як складова частина системи забезпечення національної безпеки України. *Підприємництво, господарство і право*. 2017. № 5. С. 174–180.

110. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. Серія : Державне управління. 2015. № 4. С. 50–56.

111. Макарчук В. В. Поняття «правовий статус особи» в теоретично-правовій літературі. *Право.ua*. 2015. № 3. С. 18–23.

112. Малеин Н. С. Охрана прав личности советским законодательством / отв. ред. А. И. Масляев. М. : Наука, 1985. 165 с.

113. Малеин Н. С. Повышение роли закона в охране личных и имущественных прав граждан. *Советское государство и право*. 1977. № 6. С. 41–46.

114. Малиновський Я. В. Державне управління : навч. посіб. [2-е вид., допов. та перероб.]. Київ : Атіка, 2003. 576 с.

115. Малихіна Я. В. Юридичні гарантії реалізації права на працю особами віком до 18 років : дис. … канд. юрид. наук : 12.00.05. Харків, 2009. 176 с.

116. Малько А. В. Стимулы и ограничения как парные юридические категории. *Изв. вузов. Правоведение*. 1995. № 1. С. 3–13.

117. Мандичев Д. В. Державні інспекції в Україні: адміністративно-правовий статус. *Вісник Академії митної служби України*. 2010. № 1. С. 112–117.

118. Мандичев Д. В. Поняття адміністративно-правового статусу органу виконавчої влади. *Право і суспільство*. 2010. № 5. С. 117–121.

119. Мартиненко Б. Д. Гарантії суб'єктів провадження у справах про адміністративні проступки : дис. … канд. юрид. наук : 12.00.07. Львів, 2017. 195 с.

120. Матузов Н. И. Личность. Права. Демократия. Теоретические проблемы субъективного права. Саратов : Сарат. ун-т, 1972. 292 с.

121. Микульця І. І. Адміністративно-правовий статус органів юстиції України : дис. ... канд. юрид. наук : 12.00.07. Херсон, 2014. 203 с.

122. Мицкевич А. В. О гарантиях прав и свобод советских граждан в общенародном социальном государстве. *Советское государство и право*. 1963. № 8. С. 15–21.

123. Місцеве самоврядування в Україні : історія, сучасність, перспективи розвитку : навч. посіб. / [В. В. Кравченко, Н. В. Кравченко, В. П. Лисюченко, В. А. Негода, М. В. Пітцик, Л. Є. Подобед, М. О. Пухтинський]. Київ : Арарат-Центр, 2000. 206 с.

124. Могілевський Л. В. Співвідношення системи трудового права та системи трудового законодавства України. *Підприємництво, господарство і право*. 2016. № 2. С. 87–91.

125. Нагорний О. П. Законність в адміністративній діяльності органів внутрішніх справ та шляхи її удосконалення : дис. … канд. юрид. наук : 12.00.07. Київ, 2003. 205 с.

126. Національна об'єднана оперативна група з кібер-розслідувань. *ФБР* : [сайт]. URL: https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force.

127. Окінавська хартія глобального інформаційного суспільства : прийнята 22 лип. 2000 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/998_163.

128. Окунєв І. С. Загальнотеоретичні засади правового статусу суб'єкта права : автореф. дис. … канд. юрид. наук : 12.00.01. Київ, 2009. 23 с.

129. Орлов О. В., Онищенко Ю. М. Попередження кіберзлочинності – складова частина державної політики в Україні. *Теорія та практика державного управління.* 2014. Вип. 1. С. 9–15.

130. Орловська І. Г. Адміністративно-правовий статус суддів, прокурорів, адвокатів і нотаріусів. *Науковий вісник Ужгородського національного університету*. Серія : Право. 2013. Т. 2, вип. 22, ч. 1. С. 205–208.

131. Падалка О. А. Адміністративно-правовий статус Національної поліції України : дис. … канд. юрид. наук : 12.00.07. Харків, 2016. 207 с.

132. Панасюк О. А. До питання про співвідношення понять «повноваження» та «компетенція» суду в кримінальному провадженні. *Публічне право*. 2013. № 4. С. 282–290.

133. Патюлин В. А. Государство и личность в СССР. (Правовые аспекты взаимоотношений). М. : Наука, 1974. 246 с.

134. Педько Ю. С. Адміністративна юстиція і адміністративна юрисдикція: деякі теоретичні та практичні питання співвідношення. *Право України*. 2001. № 10. С. 72–75.

135. Петренко І. В. Характеристика юридичних гарантій діяльності судів. *Форум права* : електрон. наук. фахове вид. 2017. № 5. С. 305–310.

136. Петровський О. М., Лівчук С. Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. *Молодий вчений*. 2019. № 12.1 (76.1). С. 55–59.

137. Підсумки 2018 року у цифрах. *Департамент кіберполіції Національної поліції України*. *Новини* : [сайт]. URL: https://cyberpolice.gov.ua/results/2018/.

138. Погорілко В. Ф., Головченко В. В., Сірий М. І. Права та свободи людини і громадянина в Україні. Київ : Ін Юре, 1997. 52 с.

139. Пономаренко А. В. Поняття "юридичні гарантії" в трудовому праві. *Збірник наукових праць Харківського національного педагогічного університету імені Г. С. Сковороди*. Серія : Право. 2013. Вип. 20. С. 37–41.

140. Пономарьов О. В. Адміністративно-правовий статус податкової міліції України : дис. … канд. юрид. наук : 12.00.07. Київ, 2015. 179 с.

141. Прилипко С. М., Ярошенко О. М. Трудове право України : підручник. Харків : Вапнярчук Н. М., 2008. 664 с.

142. Присяжнюк М. М., Цифра Є. І Особливості забезпечення кібербезпеки. *Реєстрація, зберігання і обробка даних*. 2017. Т. 19, № 2. С. 61–68.

143. Про виклики та загрози національній безпеці України у 2011 році : рішення Ради національної безпеки і оборони України від 17 листоп. 2010 р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/n0008525-10.

144. Про державну службу : Закон України від 10 груд. 2015 р. № 889-VIII. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/889-19.

145. Про державну службу : Закон України від 16 груд. 1993 р. № 3723-XII. *Відомості Верховної Ради України*. 1993. № 52. Ст. 490.

146. Про запобігання корупції : Закон України від 14 жовт. 2014 р. № 1700-VII. *Відомості Верховної Ради України*. 2014. № 49. Ст. 2056.

147. Про затвердження Положення про Департамент кіберполіції Національної поліції України : наказ Національної поліції України від 10 листоп. 2015 р. № 85. *Національна поліція* : [сайт]. URL: http://old.npu.gov.ua/mvs/control/main/uk/publish/ printable_article/1816252.

148. Про затвердження структури Національної поліції України : наказ Національної поліції України від 06 листоп. 2015 р. № 1. *Єдиний загальнодержавний публічний ресурс законодавчих та нормативно-правових*

актів, які стосуються діяльності поліцейських : [сайт]. URL: http://tranzit.ltd.ua/nakaz/.

149. Про Національну поліцію : Закон України від 2 лип. 2015 р. № 580-VIII. *Відомості Верховної Ради України***.** 2015. № 40–41. Ст. 379. URL: https://zakon.rada.gov.ua/laws/show/580-19.

150. Про оперативно-розшукову діяльність : Закон України від 18 лют. 1992 р. № 2135-XII. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/2135-12#Text.

151. Про основні засади забезпечення кібербезпеки України : Закон України від 05 жовт. 2017 р. **№** 2163-VIII. *Офіційний вісник України***.** 2017 р. № 91. Ст. 2765.

152. Про Раду національної безпеки і оборони України : Закон України від 05 берез. 1998 р. № 183/98-ВР**.** *Відомості Верховної Ради України.* 1998. № 35. Ст. 237.

153. Про рішення Ради національної безпеки і оборони України від 27 січня 2016 року «Про Стратегію кібербезпеки України» : указ Президента України від 15 берез. 2016 р. № 96/2016. *Офіційний вісник України*. 2016 р. № 23. Ст. 899.

154. Про розмежування повноважень щодо здійснення прокурорського нагляду за додержанням законів міжрегіональними територіальними органами Національної поліції при провадженні оперативно-розшукової діяльності : наказ Генеральної прокуратури України від 23 серп. 2016 р. № 305. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/rada/show/v0305900-16?lang=en.

155. Про утворення територіального органу Національної поліції : постанова Кабінету Міністрів України від 13 жовт. 2015 р. № 831. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/831-2015-%D0%BF.

156. Проект безопасное детство. *Министерство юстиции США* : [сайт]. URL: https://www.justice.gov/psc.

157. Проневич О. С. Завдання поліції (міліції) у юридичній поліцеїстиці. *Вісник Харківського національного університету внутрішніх справ*. 2010. № 4 (51). С. 191–205.

158. Проневич О. С. Функції поліції (міліції): нормативнодоктринальна інтерпретація. *Право і Безпека*. 2010. № 4 (36). С. 141–146. URL: http://pb.univd.edu.ua/?controller=service&action=download&download=18544

159. Профилактика в школе. *Stopbullying.gov* : [сайт]. URL: https://www.stopbullying.gov/prevention/at-school.

160. Рабінович П. М. Основи загальної теорії права і держави : підручник для студентів спеціальності «Правознавство». Київ, 1994. 236 с.

161. Рабінович П. М. Основи загальної теорії права та держави : навч. посіб. Львів : Край, 2008. 224 с.

162. Розенфельд В. Г., Старилов Ю. Н. К вопросу о понятии и правовом статусе должностного лица. *Правовая наука и реформа юридического образования*. Воронеж, 1995. Вып.1. С. 84–86.

163. Світличний В. А. Вдосконалення підготовки курсантів вищих навчальних закладів із специфічними умовами навчання як фахівців з кібербезпеки. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : зб. матеріалів Всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2018 р.) / МВС України ; Харків. нац. ун-т внутр. справ ; Координатор проектів ОБСЄ в Україні. Харків, 2018. С. 357–360.

164. Сенчук І. І. Гарантії професійної діяльності поліцейських в сучасних умовах. *Форум права* : електрон. наук. фахове вид. 2018. № 3. С. 88–95.

165. Сиренко В. Ф. Реальность прав советских граждан. Киев : Наук. думка, 1983. 139 с.

166. Скакун О. Ф. Теорія держави і права : підручник. Харків : Консум, 2006. 656 с.

167. Скакун О. Ф. Теорія права і держави : підручник. [3-те вид.]. Київ : Алерта ; ЦУЛ, 2011. 524 с.

168. Скакун. О. Ф. Теория государства и права : підручник. Харьков : Консум ; Ун-т внутр. дел, 2008. 704 с.

169. Сквірський І. О. Теорія і практика громадського контролю у публічному управлінні: адміністративно-правове дослідження : монографія. Харків : Диса плюс, 2013. 428 с.

170. Словарь современного русского литературного языка / под ред. В. И. Чернышёва. Ленинград : АН СССР, 1959. Т. 8. 583 с.

171. Словарь-справочник по праву / [сост. А. Ф. Никитин]. М. : Акалис, 1995. 140 с.

172. Словник іншомовних слів / [уклад.: С. М. Морозов, Л. М. Шкарапута]. Київ : Наук. думка, 2000. 680 с.

173. Словник української мови : [в 11 т.] / за ред. І. К. Білодіда ; АН УРСР ; Ін-т мовознавства ім. О. О. Потебні. Київ : Наукова думка, 1971. Т. 2. Г–Ж. 550 с.

174. Смирнов О. В. Природа и сущность права на труд. М. : Юрид. лит., 1964. 186 с.

175. Старилов Ю. Н. Курс общего административного права : в 3 т. М. : НОРМА ; НОРМА–ИНФРА-М, 2002. Т. I. История. Наука. Предмет. Нормы. Субъекты. 728 с.

176. Статус поліції: міжнародні стандарти і зарубіжне законодавство / за заг. ред. О. А. Банчука. Київ : Москаленко О. М., 2013. 588 с.

177. Стахура Б. І. Роль органів державної влади у забезпеченні прав людини і громадянина в демократичному суспільстві: теоретико-правовий вимір : дис. … канд. юрид. наук : 12.00.01. Львів, 2016. 180 с.

178. Степанов В. Ю. Державна інформаційна політика: проблеми та перспективи : монографія. Харків : С. А. М., 2011. 548 с.

179. Стратегія розвитку органів системи Міністерства внутрішніх справ на період до 2020 року : схв. розпорядженням Кабінету Міністрів

України від 15 листоп. 2017 р. № 1023-р. *Верховна Рада України* : [сайт]. URL: https://zakon.rada.gov.ua/laws/show/1023-2017-%D1%80.

180. Строгович М. С. Основные вопросы советской социалистической законности. М. : Наука, 1966. 271 с.

181. Структура Національної поліції. *Національна поліція України* : [сайт]. URL: https://www.npu.gov.ua/about/struktura/struktura/.

182. Судові та правоохоронні органи України. *Національна академія внутрішніх справ* : [сайт]. URL: https://arm.naiau.kiev.ua/books/spou_2019/info/lec5.html.

183. Теория государства и права : курс лекций / под ред. Н. И. Матузова, А. В. Малько. М. : Юристь, 1997. 672 с.

184. Теория государства и права : учебник для юрид. вузов и факультетов / под ред. В. М. Корельского, В. Д. Перевалова. М. : Норма – Инфра-М, 1998. 570 с.

185. Теорія держави і права. Академічний курс : підручник / за ред. О. В. Зайчука, Н. М. Оніщенко. Київ : Юрінком Інтер, 2006. 688 с.

186. Ткач Т. В. Особливості територіальної юрисдикції підрозділів департаменту кіберполіції національної поліції України. *Науковий вісник Ужгородського національного університету.* Серія : Право. 2018. Вип. 50, т. 4. С. 134–139.

187. Ткач Т. В. Понятие и структура административно-правового статуса Департамента киберполиции Национальной полиции Украины. *Право и политика*. 2019. № 1. С. 191–196. (Кыргызская Республика).

188. Ткач Т. В. Департамент киберполиции Национальной полиции Украины как субъект обеспечения кибербезопасности. *Право и Закон*. 2019. № 3. С. 184–189. (Кыргызская Республика).

189. Ткач Т. В. Юридичні гарантії діяльності департаменту кіберполіції національної поліції України. *Науковий вісник публічного та приватного права*. 2019. Вип. 6. С. 161–166.

190. Ткач Т. В. Органи національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень*. 2019. № 11. С. 113–117.

191. Ткач Т. В. Забезпечення кібербезпеки як частина адміністративно-правового статусу Національної поліції. *Сучасні правові системи світу в умовах глобалізації: реалії та перспективи* : Міжнар. наук.-практ. конф. (м. Київ, 9–10 берез. 2018 р.). Київ, 2018. С. 60–63.

192. Ткач Т. В. Завдання департаменту кіберполіції національної поліції України у сфері забезпечення кібербезпеки. *Актуальні проблеми реформування системи законодавства України* : матеріали міжнар. наук.-практ. конф. (м. Запоріжжя, 25–26 січ. 2019 р.). Запоріжжя, 2019. С. 91–94.

193. Толстой Ю. К. К теории правоотношения. Ленинград : Ленингр. ун-т, 1959. 87 с.

194. Транзитне бюро : [сайт]. URL: https://www1.nyc.gov/site/nypd/bureaus/transit-housing/transit.page.

195. Троян В. А. Гарантії публічно-сервісної діяльності Національної поліції України. *Науковий Вісник публічного та приватного права*. 2017. Вип. 5, т. 2. С. 176–180.

196. Троян В. А. Завдання та функції Національної поліції України як складова реалізації її публічно-сервісної діяльності. *Вісник Харківського національного університету внутрішніх справ.* 2016. № 4 (75). С. 12–18.

197. Трудове право України. Академічний курс : підручник для студентів вищ. навч. закл. / [П. Д. Пилипенко, В. Я. Бурак, З. Я. Козак та ін.] ; ра ред. П. Д. Пилипенка. [3-тє вид., перероб. і допов.]. Київ : Ін Юре, 2007. 536 с.

198. Уебстер Ф. Основи промышленного маркетинга. М. : Изд. дом Гребенникова, 2005. 416 с.

199. Україна та США обговорили спільну протидію кіберзлочинності. *Новини. Інформаційне агентство Українські національні новини* : [сайт]. URL: https://www.unn.com.ua/uk/news/1849243-ukrayina-ta-ssha-obgovorili-spilnu-protidiyu-kiberzlochinnosti.

200. Уржинский К. П. Гарантии права на труд. М. : Юрид. лит., 1984. 200 с.

201. Философский энциклопедический словарь. М. : ИНФРА-М, 2012. 576 с.

202. Функції Департаменту кіберполіції Національної поліції України. *База знань* : [сайт]. URL: https://wiki.1551.gov.ua/pages/viewpage.action?pageId=18842098#id-%D0%94%D0%B5%D0%BF%D0%B0%D1%80%D1%82%D0%B0%D0%BC%D0%B5%D0%BD%D1%82%D0%BA%D1%96%D0%B1%D0%B5%D1%80%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%97%D0%BD%D0%B0%D1%86%D1%96%D0%BE%D0%BD%D0%B0%D0%BB%D1%8C%D0%BD%D0%BE%D1%97%D0%BF%D0%BE%D0%BB%D1%96%D1%86%D1%96%D1%97-%D0%A4%D1%83%D0%BD%D0%BA%D1%86%D1%96%D1%97.

203. Харенко О. О. Адміністративно-правовий статус центрального органу виконавчої влади: проблема змісту. *Актуальні проблеми держави і права.* 2011. Вип. 60. С. 325–330.

204. Хеффе О. Политика. Право. Справедливость. Основоположения критической философии права и государства. М. : Гнозис, 1994. 319 с.

205. Цебинога В. Ю., Чумак В. В. Досвід зарубіжних країн щодо протидії кібербуллінгу та можливість його використання в Україні. *Актуальні питання протидії кіберзлочинності та торгівлі людьми* : матеріали всеукр. наук.-практ. конф. (м. Харків, 23 листоп. 2017 р.). Харків., 2017. С. 394–397.

206. Чечот Д. М. Субъективное право и формы его защиты. Ленинград : Ленингр. ун-т, 1968. 71 с.

207. Чумак В. В. Департамент муніципальної поліції Естонської Республіки як суб’єкт реалізації правоохоронної функції держави. *Науковий вісник Дніпропетровського державного університету внутрішніх справ.* 2017. № 4. С. 138–142.

208. Чумак В. В. Досвід країн Балтії та Грузії щодо протидії корупції в органах внутрішніх справ та можливість його використання в Україні. *Право і безпека.* 2014. № 4 (55). С. 149–154.

209. Чумак В. В. Європейський досвід реформування правоохоронних органів (на прикладі Естонії). *Підготовка охоронців правопорядку в Харкові (1917–2017 рр.)* : зб. наук. статей та тез допов. на наук.-практ. конф. до 100-річчя підготовки охоронців правопорядку в Харкові (м. Харків, 25 листоп. 2017 р.) / МВС України ; Харків. нац. ун-т внутр. справ. Харків, 2017. С. 310–312. URL: http://univd.edu.ua/general/publishing/konf/25_11_2017/pdf/171.pdf.

210. Чумак В. В. Завдання поліції в поліцейському праві сучасних держав. *Вісник Луганського державного університету внутрішніх справ.* 2016. № 2. С. 220–228.

211. Чумак В. В. Зарубіжний досвід протидії торгівлі людьми (на прикладі країн Балтії). *Протидія незаконній міграції та торгівлі людьми* : матеріали міжнар. наук.-практ. симпозіуму (Івано-Франківськ, 11–12 берез. 2016 р.). Івано-Франківськ, 2016. С. 151–153.

212. Чумак В. В. Організаційно-правові засади діяльності KNAB Латвії та ДБР України: порівняльний аналіз. *Роль та місце правоохоронних органів у розбудові демократичної правової держави* : матеріали XI міжнар. наук.-практ. інтернет-конф, (м. Одеса, 25 берез. 2019 р.). Одесса, 2018. С. 60–61.

213. Чумак В. В. Основні напрями та особливості організації діяльності поліції Латвії. *Проблеми застосування інформаційних технологій, спеціальних технічних засобів у діяльності ОВС та навчальному процесі* : матеріали наук.-практ. конф. (Львів, 17 груд. 2015 р.) / МВС України ; Львів. держ. ун-т внутр. справ. Львів, 2015. С. 146–149.

214. Шахов В. Д. К вопросу о понятии юридических гарантий в трудовом праве. *Сборник ученых трудов Свердловского юридического института*. Свердловск, 1974. Вып. 35. Новая кодификация законодательства и развитие трудового права. С. 78–83.

215. Шевчук Г. В. Особливості діяльності Департаменту кіберполіції Національної поліції України. *Науковий вісник публічного і приватного права*. 2019. Вип. 3, т. 1. С. 244–249.

216. Шевчук Г. Принципи та завдання діяльності Національної поліції України. *Підприємництво, господарство і право.* 2019. № 7. С. 120–124.

217. Шиленко М. В. Адміністративно-правовий статус суб'єктів публічної адміністрації, що здійснюють охорону природних ресурсів. *Інформація і право.* 2014. № 2. С. 97–101.

218. Шило С. М. Поняття та зміст правових гарантій законності у сфері адміністративної діяльності міліції. *Вісник Луганського державного університету внутрішніх справ імені Е. О. Дідоренка.* 2013. № 4. С. 283–292.

219. Щербина В. І. Функції трудового права : дис. … канд. юрид. наук : 12.00.05. Дніпро, 2008. 423 с.

220. Энциклопедический юридический словарь / под ред. В. Е. Крутских. М. : Инфра-М, 1998. 368 с.

221. Эстония, Польша, Хорватия, Нидерланды, Румыния и Литва создали общие кибернетические войска. *Tadviser* : [сайт]. URL: https://www.tadviser.ru/index.php/%D0%A1%D1%82%D0%B0%D1%82%D1%8C%D1%8F:%D0%9A%D0%B8%D0%B1%D0%B5%D1%80%D0%BF%D1%80%D0%B5%D1%81%D1%82%D1%83%D0%BF%D0%BD%D0%BE%D1%81%D1%82%D1%8C_%D0%B8_%D0%BA%D0%B8%D0%B1%D0%B5%D1%80%D0%BA%D0%BE%D0%BD%D1%84%D0%BB%D0%B8%D0%BA%D1%82%D1%8B_:_%D0%95%D0%B2%D1%80%D0%BE%D0%BF%D0%B0#.D0.AD.D1.81.D1.82.D0.BE.D0.BD.D0.B8.D1.8F.2C_.D0.9F.D0.BE.D0.BB.D1.8C.D1.88.D0.B0.2C_.D0.A5.D0.BE.D1.80.D0.B2.D0.B0.D1.82.D0.B8.D1.8F.2C_.D0.9D.D0.B8.D0.B4.D0.B5.D1.80.D0.BB.D0.B0.D0.BD.D0.B4.D1.8B.2C_.D0.A0.D1.83.D0.BC.D1.8B.D0.BD.D0.B8.D1.8F_.D0.B8_.D0.9B.D0.B8.D1.82.D0.B2.D0.B0_.D1.81.D0.BE.D0.B7.D0.B4.D0.B0.D0.BB.D0.B8_.D0.BE.D0.B1.D1.89.D0.B8.D0.B5_.D0.BA.D0.B8.D0.B1.D0.B5.D1.80.D0.BD.D0.B5.D1.82.D0.B8.D1.87.D0.B5.D1.81.D0.BA.D0.B8.D0.B5_.D0.B2.D0.BE.D0.B9.D1.81.D0.BA.D0.B0.

222. Юридична енциклопедія : в 6 т. / [редкол.: Ю. С. Шемшученко та ін.]. Київ : Укр. енцикл., 1998. Т. 1. А–Г. 672 с.

223. Юрисдикція. *Вікіпедія – вільна енциклопедія* : [сайт]. URL: https://uk.wikipedia.org/wiki/%D0%AE%D1%80%D0%B8%D1%81%D0%B4%D0%B8%D0%BA%D1%86%D1%96%D1%8F.

224. Юхимюк О. Юридична відповідальність в структурі правового статусу суду як органу державної влади: теоретичний аспект. *Актуальні питання реформування правової системи України* : зб. матеріалів XIII Міжнар. наук.-практ. конф. (м. Луцьк, 24–25 черв. 2016 р.) / [уклад. Л. М. Джурак] ; Східноєвропейський національний університет імені Лесі Українки ; Юрид. фак.-т. Луцьк, 2016. С. 80–82.

225. Ющик А. И. Диалектика права : в 2 кн. Киев : Ін Юре, 2013. Кн. 1, ч. 1. Общее учение о праве (Критический анализ общеправовых понятий). 456 с.

226. Янюк Н. В. Адміністративно – правовий статус посадової особи : автореф. дис. … канд. юрид. наук : 12.00.07. Київ, 2003. 20 с.

227. Cybersecurity National Action Plan. URL: https://obamawhitehouse.archives.gov/the-pressoffice/2016/02/09/fact-sheet-cybersecurity-national-action-plan.

228. Estonia, 5 more EU member states set up Lithuanian-led EU cyber force.
URL: https://www.baltictimes.com/estonia__5_more_eu_member_states_set_up_lithuanian-led_eu_cyber_force/.

229. EU International Cyberspace Policy : [сайт]. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm.

230. Garner B. A., ed. Black`S Law Dictionary. 9th ed. St. Paul: West Group, 2009.

231. Grant J. P., Barker J. C., ed. Encyclopaedic Dictionary of International Law. 3rd ed. New York: Oxford University Press, 2009.

232. Hanqin Xue. Jurisdiction of the International Court of Justice. Vol. 10, Leiden: Brill Nijhoff, 2017.

233. iGuardian. Индустриально-ориентированная платформа отчетности о кибер-вторжениях ФБР. *ФБР* : [сайт.] URL: https://www.fbi.gov/resources/law-enforcement/iguardian.

234. Jellinek G. System der subjectiven offentlichen Rechte. Freiburg : B. Mohr., 1892. 346 s.

235. Presidential Policy Directive-41. URL: https://obamawhitehouse.archives.gov/the-pressoffice/2016/07/26/presidential-policy-directive-united-statescyber-incident.

ДОДАТКИ

Додаток А

Список публікацій здобувача за темою дисертації

1. Ткач Т. В. Особливості територіальної юрисдикції підрозділів Департаменту кіберполіції Національної поліції України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2018. Випуск 50. Т. 4. С. 134-139.

2. Ткач Т. В. Понятие и структура административно-правового статуса Департамента киберполиции Национальной полиции Украины. *Право и политика*. 2019. № 1. С. 191-196. (Кыргызская Республика).

3. Ткач Т. В. Департамент киберполиции Национальной полиции Украины как субъект обеспечения кибербезопасности. *Право и Закон*. 2019. № 3. С. 184-189. (Кыргызская Республика).

4. Ткач Т. В. Юридичні гарантії діяльності Департаменту кіберполіції Національної поліції України. *Науковий вісник публічного та приватного права*. 2019. Випуск 6. С. 161-166.

5. Ткач Т. В. Органи Національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень*. 2019. № 11. С. 113-117.

6. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96-102.

7. Білобров Т. В. Роль та місце Департаменту кіберполіції Національної поліції України у системі суб'єктів забезпечення кібербезпеки держави. *Правові новели*. 2020. № 11. С. 122-128.

8. Ткач Т. В. Забезпечення кібербезпеки як частина адміністративно-правового статусу Національної поліції. Сучасні правові системи світу в умовах глобалізації: реалії та перспективи: Міжнародна науково-практична конференція, м. Київ, 9–10 березня 2018 р. – К.: Центр правових наукових досліджень, 2018. С. 60-63.

9. Ткач Т. В. Завдання департаменту кіберполіції Національної поліції України у сфері забезпечення кібербезпеки. Актуальні проблеми реформування системи законодавства України: Матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 25-26 січня 2019 р. Запоріжжя : Запорізька міська громадська організація «Істина», 2019. С. 91-94.

10. Білобров Т. В. Сучасний стан та перспективи забезпечення кібербезпеки в Україні Національною поліцією. Юридична наука України: історія, сучасність, майбутнє : міжнародна науково-практична конференція, м. Харків, 1–2 листопада 2019 р. Харків : Східноукраїнська наукова юридична організація, 2019. С. 78–80.

11. Білобров Т. В. Права та обов’язки Департаменту кіберполіції Національної поліції України

як елемент адміністративно-правового статусу. Право як ефективний суспільний регулятор : матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 лютого 2020 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2020. С. 45–47.

Додаток Б
Акти впровадження

ЗАТВЕРДЖУЮ
Перший проректор Національної академії внутрішніх справ, доктор юридичних наук, професор
С.Д. Гусарєв
17.01.2020

АКТ
про впровадження результатів дисертаційного дослідження здобувача кафедри поліцейського права Білобров Тетяни Віталіївни на тему: «Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України» в освітній процес Національної академії внутрішніх справ

Комісія у складі завідувача кафедри поліцейського права, кандидата юридичних наук, доцента Кулікова В.А., завідувача кафедри публічного управління та адміністрування, кандидата юридичних наук, доцента Пастуха І.Д. та доцента кафедри поліцейського права, кандидата юридичних наук, доцента Білика В.М., склала цей акт про те, що результати дисертаційного дослідження «Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України» здобувача кафедри поліцейського права Білобров Тетяни Віталіївни, зокрема:

1. Ткач Т. В. Особливості територіальної юрисдикції підрозділів департаменту кіберполіції національної поліції України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2018. Випуск 50. Т. 4. С. 134-139.
2. Ткач Т. В. Понятие и структура административно-правового статуса Департамента киберполиции Национальной полиции Украины. *Право и политика*. 2019. № 1. С. 191-196. (Кыргызская Республика).
3. Ткач Т. В. Департамент киберполиции Национальной полиции Украины как субъект обеспечения кибербезопасности. *Право и Закон*. 2019. № 3. С. 184-189. (Кыргызская Республика).
4. Ткач Т. В. Юридичні гарантії діяльності департаменту кіберполіції національної поліції України. *Науковий вісник публічного та приватного права*. 2019. Випуск 6. С. 161-166.
5. Ткач Т. В. Органи національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень*. 2019. № 11. С. 113-117
6. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96-102.
7. Білобров Т. В. Роль та місце департаменту кіберполіції національної поліції України у системі суб'єктів забезпечення кібербезпеки держави. *Правові новели*. 2020. № 11. С. 122-128.

8. Ткач Т. В. Забезпечення кібербезпеки як частина адміністративно-правового статусу Національної поліції. Сучасні правові системи світу в умовах глобалізації: реалії та перспективи: Міжнародна науково-практична конференція, м. Київ, 9–10 березня 2018 р. – К.: Центр правових наукових досліджень, 2018. С. 60-63.

9. Ткач Т. В. Завдання департаменту кіберполіції національної поліції України у сфері забезпечення кібербезпеки. Актуальні проблеми реформування системи законодавства України: Матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 25-26 січня 2019 р. Запоріжжя : Запорізька міська громадська організація «Істина», 2019. С. 91-94.

10. Білобров Т. В. Сучасний стан та перспективи забезпечення кібербезпеки в Україні Національною поліцією. Юридична наука України: історія, сучасність, майбутнє : міжнародна науково-практична конференція, м. Харків, 1–2 листопада 2019 р. Харків : Східноукраїнська наукова юридична організація, 2019. С. 78–80.

11. Білобров Т. В. Права та обов'язки департаменту кіберполіції національної поліції України як елемент адміністративно-правового статусу. Право як ефективний суспільний регулятор : матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 лютого 2020 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2020. С. 45–47.

використовуються в освітньому процесі Національної академії внутрішніх справ під час проведення семінарських і практичних занять зі здобувачами вищої освіти при вивченні наступних навчальних дисциплін: «Адміністративна діяльність», «Поліцейська діяльність», «Адміністративне право і процес», «Адміністративна реформа в Україні», «Сучасні аспекти адміністративного права», «Державне управління», «Актуальні проблеми адміністративного права і процесу».

Члени комісії:

Завідувач кафедри
поліцейського права
кандидат юридичних наук, доцент — В.А. Куліков

Завідувач кафедри
публічного управління та адміністрування
кандидат юридичних наук, доцент — І.Д. Пастух

Доцент кафедри
поліцейського права
кандидат юридичних наук, доцент — В.М. Білик

ЗАТВЕРДЖУЮ
Проректор Національної
академії внутрішніх справ
доктор юридичних наук,
професор
С.С. Чернявський
16.01.2020

АКТ

про впровадження результатів дисертаційного дослідження здобувача кафедри поліцейського права Білобров Тетяни Віталіївни на тему: «Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України» у науково-дослідну сферу Національної академії внутрішніх справ

Комісія у складі завідувача наукової лабораторії з проблем протидії злочинності ННІ № 1, доктора юридичних наук, доцента Вознюка А.А.; заступника начальника відділу організації наукової діяльності та захисту прав інтелектуальної власності кандидата юридичних наук, старшого наукового співробітника Калиновського О.В. та начальника відділу докторантури та ад'юнктури, доктора юридичних наук, доцента Дрозда О.Ю. склала цей акт про те, що результати дисертаційного дослідження «Адміністративно-правовий статус Департаменту кіберполіції Національної поліції України» здобувача кафедри поліцейського права Білобров Тетяни Віталіївни, зокрема:

1. Ткач Т. В. Особливості територіальної юрисдикції підрозділів департаменту кіберполіції національної поліції України. *Науковий вісник Ужгородського національного університету. Серія «Право»*. 2018. Випуск 50. Т. 4. С. 134-139.

2. Ткач Т. В. Понятие и структура административно-правового статуса Департамента киберполиции Национальной полиции Украины. *Право и политика*. 2019. № 1. С. 191-196. (Кыргызская Республика).

3. Ткач Т. В. Департамент киберполиции Национальной полиции Украины как субъект обеспечения кибербезопасности. *Право и Закон*. 2019. № 3. С. 184-189. (Кыргызская Республика).

4. Ткач Т. В. Юридичні гарантії діяльності департаменту кіберполіції національної поліції України. *Науковий вісник публічного та приватного права*. 2019. Випуск 6. С. 161-166.

5. Ткач Т. В. Органи національної поліції України в національній системі кібербезпеки. *Юридичний бюлетень*. 2019. № 11. С. 113-117

6. Білобров Т. В. Міжнародний досвід протидії кіберзлочинності органами кіберполіції. *Право і суспільство*. 2020. № 3. С. 96-102.

7. Білобров Т. В. Роль та місце департаменту кіберполіції національної поліції України у системі суб'єктів забезпечення кібербезпеки держави. *Правові новели*. 2020. № 11. С. 122-128.

8. Ткач Т. В. Забезпечення кібербезпеки як частина адміністративно-правового статусу Національної поліції. Сучасні правові системи світу в умовах глобалізації: реалії та перспективи: Міжнародна науково-практична конференція, м. Київ, 9–10 березня 2018 р. – К.: Центр правових наукових досліджень, 2018. С. 60-63.

9. Ткач Т. В. Завдання департаменту кіберполіції національної поліції України у сфері забезпечення кібербезпеки. Актуальні проблеми реформування системи законодавства України: Матеріали міжнародної науково-практичної конференції, м. Запоріжжя, 25-26 січня 2019 р. Запоріжжя : Запорізька міська громадська організація «Істина», 2019. С. 91-94.

10. Білобров Т. В. Сучасний стан та перспективи забезпечення кібербезпеки в Україні Національною поліцією. Юридична наука України: історія, сучасність, майбутнє : міжнародна науково-практична конференція, м. Харків, 1–2 листопада 2019 р. Харків : Східноукраїнська наукова юридична організація, 2019. С. 78–80.

11. Білобров Т. В. Права та обов'язки департаменту кіберполіції національної поліції України як елемент адміністративно-правового статусу. Право як ефективний суспільний регулятор : матеріали міжнародної науково-практичної конференції, м. Львів, 14–15 лютого 2020 р. – Львів: Західноукраїнська організація «Центр правничих ініціатив», 2020. С. 45–47.

використовуються у науково-дослідній сфері Національної академії внутрішніх справ під час виконання плану науково-дослідних і дослідно-конструкторських робіт на 2020 рік.

Члени комісії:

Завідувач наукової лабораторії з
проблем протидії злочинності ННІ № 1
доктор юридичних наук, доцент А.А. Вознюк

Заступник начальника відділу
організації наукової діяльності та
захисту прав інтелектуальної власності
кандидат юридичних наук,
старший науковий співробітник О.В. Калиновський

Начальник відділу
докторантури та ад'юнктури
доктор юридичних наук, доцент О.Ю. Дрозд

Додаток В

СТРУКТУРА ДЕПАРТАМЕНТУ КІБЕРПОЛІЦІЇ НАЦІОНАЛЬНОЇ ПОЛІЦІЇ УКРАЇНИ

Департамент кіберполіції (у складі кримінальної поліції)

Апарат

Керівництво

1-е управління

2-е управління

3-є управління

1-й відділ

2-й відділ

3-й відділ

4-й відділ

5-й відділ

Відділ фінансового забезпечення та бухгалтерського обліку

Режимно-секретний відділ

Сектор правового забезпечення

Територіальні (відокремлені) підрозділи

Відділ протидії кіберзлочинам у Вінницькій області

Відділ протидії кіберзлочинам у Волинській області

Управління протидії кіберзлочинам в Дніпропетровській області

Відділ протидії кіберзлочинам в Донецькій області

Відділ протидії кіберзлочинам в Житомирській області

Відділ протидії кіберзлочинам в Закарпатській області

Відділ протидії кіберзлочинам в Запорізькій області

Відділ протидії кіберзлочинам в Івано-Франківській області

Відділ протидії кіберзлочинам в Київській області

Управління протидії кіберзлочинам в місті Києві

Відділ протидії кіберзлочинам в Кіровоградській області

Відділ протидії кіберзлочинам в Луганській області

Управління протидії кіберзлочинам у Львівській області

Відділ протидії кіберзлочинам в Миколаївській області

Управління протидії кіберзлочинам в Одеській області

Відділ протидії кіберзлочинам в Полтавській області

Відділ протидії кіберзлочинам в Рівненській області

Відділ протидії кіберзлочинам в Сумській області

Відділ протидії кіберзлочинам в Тернопільській області

Управління протидії кіберзлочинам в Харківській області

Відділ протидії кіберзлочинам в Херсонській області

Відділ протидії кіберзлочинам в Хмельницькій області

Відділ протидії кіберзлочинам в Черкаській області

Відділ протидії кіберзлочинам в Чернівецькій області

Відділ протидії кіберзлочинам в Чернігівській області

Відділ протидії кіберзлочинам в Автономній Республіці Крим та м. Севастополі