Список використаних джерел:

1. Конвенція про права дитини в редакції зі змінами, схваленими резолюцією 50/155 Генеральної Асамблеї ООН від 21 грудня 1995 року. Ратифіковано Постановою ВР № 789-XII від 27.02.91
2. Сімейний кодекс України: Закон України від 10 січня 2001 р. (станом на 02 квітня 2020 р.) / Верховна Рада України. *Відомості Верховної Ради України*. 2002, № 21-22, ст. 135.
3. Андрущенко В., Губернський Л. Культура. Ідеологія. Особистість: Методолого-світоглядний аналіз. Київ : Знання України. (2007) с. 66–67.
4. Офіційний сайт Державної служби статистики України. URL: http:// www.ukrstat.gov.ua/operativ/operativ2019/prav_zloch/ arh_adm_prp_u.htm.
5. Судова влада України. Огляд даних про стан здійснення правосуддя у 2018 році. URL: http://www.court.gov.ua/ userfiles/media/media/ogl_2018.pdf.
6. Судова влада України. Звіт про осіб, притягнутих до кримінальної відповідальності, та види кримінального покарання за 2019 рік. URL: https://www.court.gov.ua/inshe/ sudova_statystyka/rik_2019.
7. Судова влада України. Звіт судів першої інстанції щодо розгляду справ про адміністративні правопорушення за 2019 рік. URL: https://www.court.gov.ua/userfiles/media/dsa_ pres_slujba_2019/ dsa_pres_slujba_2020/11_2019.xlsx.
8. Энциклопедический словарь Брокгауза и Ефрона Санкт-Петербург : Издательское дело, 1990. Т. XXIX. С. 469. URL: http://dlib.rsl.ru/viewer/01003924202#?page=11.

БІЛОБРОВА Т. В.,
аспірант кафедри поліцейського права
(Національна академія внутрішніх справ)

УДК [341.456:004]:[343.346.8:004]
DOI https://doi.org/10.32842/2078-3736/2020.3.18

МІЖНАРОДНИЙ ДОСВІД ПРОТИДІЇ КІБЕРЗЛОЧИННОСТІ ОРГАНАМИ КІБЕРПОЛІЦІЇ

У статті досліджено успішний міжнародний досвід протидії кіберзлочинності органами поліції. Встановлено, що дослідження діяльності органів поліції зазначених держав та їх національного законодавства є сьогодні вельми актуальним та своєчасним в умовах удосконалення адміністративно-правового статусу Департаменту кіберполіції Національної поліції України. З'ясовано, що належний рівень функціонування органів поліції, які здійснюють заходи щодо боротьби з кіберзлочинністю, залежить від належного рівня їх правового регулювання, що в США є достатньо сильною основою для ефективного здійснення національної політики в галузі кібербезпеки. Визначено, що у США ФБР спільно з іншими урядовими установами створило ряд бюро та робочих груп з питань боротьби з кіберзлочинністю з різними категоріями громадян та відповідно до їх соціального статусу. На нашу думку, досвід вирішення питання забезпечення кібербезпеки дітей в Інтернет-просторі та боротьби з кібержорстокістю має особливу цінність. Підкреслюється, що для забезпечення кібербезпеки держави у Франції створена відповідна нормативна база для функціонування органів, уповнова-

жених забезпечити кібербезпеку держави. Водночас захист кіберпростору та боротьба з кіберзлочинністю вважаються пріоритетними для національної безпеки Франції і здійснюються не лише поліцією (жандармерією), а й на рівні Міністерства оборони та спеціально створених органів. Наголошено, що 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 зі Стратегією була розроблена та прийнята законодавча пропозиція про посилення безпеки інформаційних систем ЄС. Зроблено висновок, 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.

Ключові слова: *міжнародний досвід, протидія кіберзлочинності, органи поліції, США, Франція, країни Європейського Союзу.*

Bilobrova T. V. International experience in combating cybercrime by cyberpolice bodies

The article examines the successful international experience in combating cybercrime by police. It is established that the study of the activities of the police bodies of these states and their national legislation is very relevant and timely today in terms of improving the administrative and legal status of the Cyber Police Department of the National Police of Ukraine. It has been established that the proper level of functioning of police bodies carrying out measures to combat cybercrime depends on the proper level of their legal regulation, which in the United States is a strong enough basis for effective implementation of national cybersecurity policy. It is determined that in the United States, the FBI, together with other government agencies, has established a number of bureaus and working groups on combating cybercrime with different categories of citizens and in accordance with their social status. In our opinion, the experience in resolving the issue of ensuring children's cybersecurity in the Internet space and combating cyberbullying is of special value. It was emphasized that in order to ensure the cybersecurity of the state in France, an appropriate regulatory framework for the functioning of the bodies authorized to ensure the cybersecurity of the state has been created. At the same time, the protection of cyberspace and the fight against cybercrime are considered a priority for the national security of France and are carried out not only by the police (gendarmerie), but also at the level of the Ministry of Defense and specially created bodies. It is emphasized that the EU Cyber Security Strategy was adopted in 2013. Its peculiarity is that the strategy covered various aspects of cyberspace, in particular, the internal market, justice, domestic and foreign policy. Together with the Strategy, a legislative proposal on strengthening the security of EU information systems was developed and adopted. It is concluded that an important condition for the successful operation of the Cyber Police Department of the National Police of Ukraine is to take into account the specifics of various activities of the authorities to ensure cybersecurity abroad, as well as the choice of optimal forms and methods of combating cybercrime based on international principles and standards.

Key words: *international experience, fight against cybercrime, police bodies, USA, France, European Union countries.*

Актуальність теми дослідження. 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 внутрішнього складника безпеки держави, так і 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 пострадянського простору (Латвія, Литва. Естонія та деякі інші).

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

Метою статті є дослідження позитивного міжнародного досвіду протидії кіберзлочинності органами поліції.

Аналіз останніх досліджень та публікацій. 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. 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. Водночас 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 цим 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 зумовлюють наукові дослідження успішного зарубіжного досвіду діяльності уповноважених державних та міжнародних органів у сфері забезпечення кібербезпеки держави та протидії кіберзлочинності.

Виклад основного матеріалу. Сьогодні у багатьох зарубіжних країнах налагоджена система співробітництва, що зумовлюється 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 [1, 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 та однієї з провідних в Європейському Союзі держав, як Сполучені Штати Америки (далі – США). Оскільки саме вказана держава стала однією з перших, хто визначив на національному рівні та прийняв низку законів та нормативно-правових актів у сфері протидії кіберзлочинності та забезпечення кібербезпеки держави. Причинами такого оперативного затвердження концепцій та 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, Бюро спеціальних операцій, Транзитне бюро, Бюро по боротьбі з тероризмом, Бюро по боротьбі зі злочинністю, Бюро детективів та інші.

Окрему увагу слід приділити функціонуванню Бюро по боротьбі з тероризмом [2], оскільки його діяльність спрямована на захист штату від внутрішніх та міжнародних (зовнішніх) загроз терористичного характеру, у тому числі кіберзагроз. На території штату діє так звана «Команда критичного реагування», що здійснює: прогноз можливих кіберзагроз та загроз тероризму; розробку новаторської та довгострокової політики та механізмів захисту від кібератак, інформаційних та комп'ютерних злочинів; готує до оперативного втручання служби первинного реагування та спеціальні підрозділи; нарощує потенціал розвідувальних спроможностей для виявлення та протидії кібератакам та терористичним загрозам. При цьому слід вказати, що діяльність Команди критичного реагування здійснюється відповідно до національного та федерального законодавства, 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 із 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 контртерористичні розгортання на критично важливих об'єктах інфраструктури по всьому штату Нью-Йорк.

Водночас 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 кібербезпеки держави.

Так, на державному рівні в США прийняті такі важливі програмні документи, що створюють фундамент для боротьби з кіберзлочинністю: 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) [1, с. 55].

В США при ФБР функціонує проєкт «Безпечне дитинство», що реалізується спільно з Міністерством юстиції США. Зазначений проєкт – 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 проєкту «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 рятування жертв [3]. В рамках зазначеного проєкту 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 здійсню-

ються систематичні заходи в школах та інших освітніх закладах, щоб допомогти учням дізнатися про профілактику кібербулінгу.

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

Поряд з США активну боротьбу з кіберзлочинністю проводять і в країнах Європейського Союзу (далі – ЄС). У ЄС створений необхідний нормативно-правовий фундамент з питань захисту кіберпростору [1, 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 [4, 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 тією ж мірою, 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 [5].

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 напрямів роботи:

– забезпечення державного суверенітету;

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

– інформування широкої громадськості;

– перетворення інформаційної безпеки на конкурентну перевагу французьких підприємств;

– підвищення впливу Франції на міжнародній арені.

Цю стратегію доповнили:

1) Міжнародна стратегія Франції в сфері інформаційних технологій була представлена міністром Європи і закордонних справ у грудні 2017 року. У ній узагальнені всі стратегічні цілі, які Франція підтримує в сфері інформаційних технологій, зокрема у трьох основних: 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 у лютому 2018 року. У ньому визначається доктрина управління кіберкризами. Огляд також роз'яснює цілі національної стратегії в області кіберзахисту, підтверджує ефективність французької моделі і покладає основну відповідальність у цій галузі на державу [7, с. 316].

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 здійснюються не лише органами поліції (жандармерії), але й також на рівні Міністерства оборони та спеціально створених органів.

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 цифрової продукції і послуг, що випускаються в ЄС. Сьогодні зазначене агентство успішно функціонує на території країн – членів ЄС.

Агентство ЄС з кібербезпеки відповідно до Стратегії ЄС керується у своїй діяльності також прийнятою Директивою ЄС з інформаційної безпеки [7]. У 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.

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.

Висновки. 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 наявні 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.

Список використаних джерел:

1. Петровський О.М., Лівчук С.Ю. Проблеми боротьби з кіберзлочинністю: міжнародний досвід та українські реалії. Молодий вчений. № 12.1 (76.1). 2019. С. 55–59.

2. Бюро по боротьбі з тероризмом : сайт. URL: https://www1.nyc.gov/site/nypd/bureaus/investigative/counterterrorism.page (дата звернення: 20.05.2020).

3. Проект безопасное детство // Министерство юстиции США : сайт. URL: https://www.justice.gov/psc (дата звернення: 20.05.2020).

4. 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 : Івано-Франків. ун-т права ім. Короля Данила Галицького, 2016. С. 151–153.

5. EU International Cyberspace Policy : сайт. URL: http://www.eeas.europa.eu/policies/eu-cyber-security/index_en.htm (дата звернення: 20.05.2020).

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

7. 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. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj (дата звернення: 20.05.2020).