ФП 2020-2
ISSN 1995-6134

УДК *342.52(477)*
DOI: http://doi.org/10.5281/zenodo.3883823

С.Г. ПЕТРОВ,
співробітник Служби безпеки України, кандидат юридичних наук,
м. Київ, Україна; e-mail: kibpetrov@gmail.com;
ORCID: https://orcid.org/0000-0001-7786-4657

ОРГАНІЗАЦІЙНО-ПРАВОВІ ОСНОВИ ПРОТИДІЇ КІБЕРПОСЯГАННЯМ В ІНОЗЕМНИХ ДЕРЖАВАХ: АКТУАЛЬНІ ПРИКЛАДИ ДЛЯ УКРАЇНИ

S.G. PETROV,
Employee of the Security Service of Ukraine, Ph.D. in Law, Kyiv, Ukraine;
e-mail: kibpetrov@gmail.com;
ORCID: https://orcid.org/0000-0001-7786-4657

ORGANIZATIONAL AND LEGAL BASIS FOR COMBATING CYBER ATTACKS IN FOREIGN COUNTRIES: ACTUAL EXAMPLES FOR UKRAINE

АНОТАЦІЇ (ABSTRACTS), КЛЮЧОВІ СЛОВА (KEY WORDS)

Постановка проблеми. Для України важливо розбудовувати Національну систему кібербезпеки з урахуванням найкращих напрацювань у зарубіжних державах, зокрема щодо розбудови інституційних передумов, а також формування відповідної правової бази. Адже порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, насамперед, державних, отримання несанкціонованого доступу до таких ресурсів, порушення безпеки, сталого функціонування комунікаційних та/або технологічних систем, використання засобів електронних комунікацій для здійснення кібератак на інші об'єкти створюють як економічні, так і репутаційні ризики для України. **Метою роботи** є розкриття актуальних для України прикладів формування організаційно-правових основ протидії кіберпосяганням у окремих зарубіжних державах. **Використані методи** – логіко-семантичний при дослідженні понять, що використовуються у законодавстві України та зарубіжних країн. Структурно-логічний – при аналізі особливостей правового регулювання відповідних інформаційних і адміністративних відносин. З використанням формально-юридичного методу наукового пізнання визначені можливості застосування в Україні досвіду зарубіжних країн. **Результат**. У аналізованих зарубіжних державах увага приділяється питанням безпеки об'єктів критичної інфраструктури, вимогам до уповноважених постачальників Інтернет послуг (провайдерів), розробці концептуальних документів щодо протидії кіберпосяганням. Система органів управління відповідними процесами має різну ступінь централізації. **Висновки.** Сформульовані прийнятні для України пропозиції щодо врахування в Україні елементів правової регламентації: вимог до уповноважених постачальників Інтернет послуг (провайдерів) у Республіці Бєларусь з дотриманням демократичних принципів впровадження механізмів правового регулювання; концептуальних основ для розбудови системи кібербезпеки ("Кіберщит Казахстану") у частині здійснення ревізії навчальних програм та професійних стандартів тощо; створення Агентства з кібербезпеки, на прикладі Сінгапуру, з метою нагляду за операційною і освітньою діяльністю, розвитком екосистем у цій сфері тощо.

Ключові слова: *кібербезпека; об'єкти критичної інформаційної інфраструктури; правове регулювання*

***

Problem statement. It is important for Ukraine to build the National Cybersecurity System, taking into account the best practices of foreign countries, in particular with regard to building institutional prerequisites, as well as the formation of an appropriate legal framework. Breach of confidentiality, integrity, accessibility of electronic information resources, first of all, state ones, obtaining unauthorized access to such resources, breach of security, stable functioning of communication and/or technological systems, use of electronic communications for cyber-attacks on other objects create economic, and reputational risks for Ukraine. The **methods** used are logical and semantic while studying concepts implemented in the legislation of Ukraine and foreign countries. Structural and logical – in the analysis of the peculiarities of legal regulation of relevant information and administrative relations. The possibilities of applying the experience of foreign countries in Ukraine were de-

termined using the formal-legal method of scientific knowledge. The **purpose** of this paper is to disclose relevant examples of the organizational and legal foundations formation for counteraction to cyberattacks in some foreign countries. **Results**. In the analyzed foreign countries attention is paid to security issues of critical infrastructure facilities, requirements to authorized internet service providers, development of conceptual documents on counteraction to cyber-attacks. The systems of managing the relevant processes have a different degree of centralization. **Conclusions**. Acceptable for Ukraine proposals have been formulated to take into account in legal regulation in Ukraine: requirements for authorized Internet service providers in the Republic of Belarus in compliance with democratic principles of the legal regulation mechanisms implementation; conceptual bases for building a cybersecurity system ("Cyber Shield of Kazakhstan") in terms of auditing curricula and professional standards, etc.; the establishment of Cyber security Agency, following the example of Singapore, to oversee operational and educational activities, the development of ecosystems in this area.

Key words: *cyber security; critical information infrastructure; legal regulation*

Постановка проблеми

Україна поряд з іншими державами світу останніми роками стає об'єктом протиправних посягань у кіберпросторі. Більшість із них – це навмисні дії в кіберпросторі, які здійснюються за допомогою інформаційно-комунікаційних технологій, програмно-апаратних засобів, іншого технічного та технологічного обладнання. Метою подібних атак є порушення конфіденційності, цілісності, доступності електронних інформаційних ресурсів, насамперед, державних.

Саме тому для України важливо розбудовувати Національну систему кібербезпеки з урахуванням найкращих напрацювань у зарубіжних державах, зокрема, у частині розбудови інституційних передумов, а також формування відповідної правової бази.

Можна за цим науковим напрямком зазначити певні напрацювання – зокрема, Р.В. Лук'янчука щодо досвіду країн-учасниць НАТО у сфері забезпечення кібербезпеки, який визначив етапи взаємодії між Україною та Альянсом у межах функціонування Трастового фонду НАТО з кібербезпеки та обґрунтував доцільність прискорення процесу приєднання України до НАТО з метою входження до системи колективної безпеки, у тому числі й у форматі забезпечення кібербезпеки [1]. Важливою є робота А.І. Марущака з європейського досвіду боротьби з правопорушеннями в інформаційній сфері [2]; Т. Мур (Moore T., 2010) – із багатоаспектності механізмів протидії протиправним кіберпосяганням у контексті відповідних витрат на захист об'єктів критичної інформаційної інфраструктури [3]; С. Шукла (Shukla, S.K., 2016) – із кіберзагроз та протидії їм [4]. До того ж, в цих роботах переважно йдеться про розробку відповідних "політик" для діяльності органів державної влади у тісній взаємодії із приватним сектором.

Актуальними також визначені дослідження О. Гатевей (Hathaway O.A., 2016), Р. Крутоф (Crootof R., 2016), П. Левіц (Levitz P., 2016) із співавторами щодо права кібер-атак, зокрема, міжнародних механізмів правового регулювання та їх імплементації у національні правові системи [5]; Дж. Фарвел (Farwell J. P., 2011) й Р. Рогозінскі (Rohozinski R., 2011) – із питань майбутніх кібервійн [6]; Ф. Бізогні (Bisogni F., 2016) – із випадків правового регулювання повідомлень про розкриття державної інформації [7], Мільтон Мюелер і Андреас Куен (Milton Mueller, Andreas Kuehn, 2013) щодо технологій нагляду, кібербезпеки і відповідних організаційних змін [8]. При цьому, поза дослідженнями залишились питання напрацювання ефективних організаційно-правових основ протидії кіберпосяганням, що могли би бути використані як в цих державах, так і в Україні.

Саме тому в попередніх дослідженнях автора увага була сконцентрована переважно на міжнародному досвіді протидії протиправних посягань на державні електронні інформаційні ресурси США [9] та країн Європейського Союзу [10]. Разом із тим, є деякі країни, що за рівнем розвитку, економічним станом і менталітетом наближені до України. Серед них, наприклад, Бєларусь, що входить до ініціативи Європейського Союзу "Східне партнерство" поряд із Україною, Азербайджаном, Грузією, Вірменію, Молдовою [11]. Казахстан має більш "авторитарну" систему управління відповідними процесами, Сінгапур, навпаки, має одну з найбільш розвинених систем кібербезпеки і кіберзахисту. Їх досвід протидії протиправним кіберпосяганням враховують провідні практики ЄС і є цікавим для врахування в Україні.

Тому метою статті є формування актуальних для України рекомендацій стосовно організаційно-правових основ протидії кіберпосяганням на прикладах Республік Бєларусь, Казахстан і Сінгапуру. Її новизна полягає в тому, що в Україні можуть бути враховані запропоновані автором елементи правової регламентації: вимог до уповноважених постачальників Інтернет послуг

ISSN 1995-6134

(провайдерів) у Республіці Бєларусь з дотриманням демократичних принципів впровадження механізмів правового регулювання; концептуальних основ для розбудови системи кібербезпеки ("Кіберщит Казахстану") у частині здійснення ревізії навчальних програм та професійних стандартів тощо; створення Агентства з кібербезпеки, на прикладі Сінгапуру. Завданням статті є розкриття правових засад систем протидії протиправним кіберпосяганням у Республіках Бєларусь і Казахстан, а також Сінгапуру; формулювання прийнятних для України прикладів для удосконалення відповідних організаційно-правових основ.

Розвиток системи протидії протиправним кіберпосяганням у Республіці Бєларусь

У Республіці Бєларусь (далі – РБ) розроблено правові основи для створення систем інформаційної безпеки, сертифікації засобів інформаційної безпеки, ліцензування окремих видів робіт та послуг щодо кібербезпеки, а також встановлені державні стандарти в інформаційній сфері щодо антивірусного обладнання, роутерів, файерволів тощо. Як і в Україні та більшості країн світу, передбачена адміністративна та кримінальна відповідальність за протиправні кіберпосягання. Важливо відзначити, що в РБ заборонено використовувати на її території програмне забезпечення або технічне обладнання, яке не відповідає вимогам встановлених у цій країні стандартів.

Значна увага в РБ приділяється питанням безпеки об’єктів критичної інфраструктури, основні положення якої викладені в Указі Президента РБ від 16.04.2013 року № 196 "Про деякі заходи з удосконалення захисту інформації". Цим указом затверджено Положення про порядок віднесення об'єктів інформатизації до критично важливих (викладено в новій редакції відповідно до Указу Президента РБ від 09.12.2019 р. № 449), яким встановлено, що об'єкт інформатизації підлягає віднесенню до критично важливих за умови його відповідності встановленим критеріям і показникам рівня можливої шкоди національним інтересам Республіки Бєларусь в політичній, економічній, соціальній, інформаційній, екологічній та інших сферах (далі – показники рівня можливої шкоди) в разі створення загроз інформаційної безпеки або в результаті виникнення ризиків інформаційної безпеки щодо об'єкта інформатизації (його складових елементів), затверджених оперативно-аналітичним центром при Президентові РБ (далі – ОАЦ) за погодженням із зацікавленими державними органами. Критеріями віднесення об'єктів інформатизації до критично важливих у РБ є: соціальної значущості, економічної значущості, екологічної та інформаційної значущості [12].

Подібні критерії можуть бути враховані при удосконаленні критеріїв віднесення об’єктів до критичної інфраструктури в Україні, що частково закріплені у ст.6 Закону України "Про основні засади забезпечення кібербезпеки України" [13]. За змістом поняття "критично важливий об’єкт інформатизації" є тотожним поняттю "об’єкт критичної інформаційної інфраструктури", яке застосовується у вітчизняному законодавстві.

Крім того, Указом Президента РБ від 15.03.2016 року № 98 "Про удосконалення порядку передачі повідомлень електрозв’язку" створено систему протидії порушенням порядку пропуску трафіку в мережах електрозв’язку, що є сукупністю програмно-технічних засобів, інформаційних ресурсів та інформаційних технологій, а також заходів правового, організаційно-технічного та економічного характеру, що спрямовані на попередження, виявлення та припинення порушень порядку пропуску трафіку [14].

Організаційно в РБ регулювання діяльності із забезпечення захисту інформації, яка становить державну таємницю РБ, від витоку технічними каналами та несанкціонованих впливів, а також захист безпеки КВОІ, організацій та фізичних осіб покладено на ОАЦ, який було створено у 2008 році. Захист критично важливих об’єктів та їх сукупності або критичної інфраструктури вважається одним із найбільш важливих завдань національної безпеки країни, а тому у цій сфері ОАЦ здійснює:

– координацію державних органів та інших організацій із забезпечення технічного захисту інформації, що обробляється на КВОІ;

– формування та ведення Державного реєстру КВОІ, а також надання відомостей з нього;

– в межах своєї компетенції – контроль за діяльністю із забезпечення технічного захисту інформації, що обробляється на КВОІ;

– прийняття нормативно-правових актів з питань віднесення об’єктів інформатизації до КВОІ та забезпечення їх безпеки;

– визначення вимог, які висуваються до уповноважених постачальників Інтернет-послуг (провайдерів).

Як видно, зазначений орган має окремі повноваження, що в Україні реалізує Держспецзв'язку України, а також підрозділи СБ України.

ISSN 1995-6134

Відповідно до наказу ОАЦ від 02.08.2010 року № 60 (зі змінами), визначено перелік вимог, які висуваються до уповноважених постачальників Інтернет послуг (провайдерів):

– здійснювати ідентифікацію абонентських пристроїв при наданні інтернет-послуг, облік і зберігання відомостей про абонентські пристрої, надані інтернет-послуги;

– усувати різні види неправомірних дій, про наявність яких стало відомо постачальнику інтернет-послуг, які призводять до порушення конфіденційності, цілісності, автентичності, доступності, збереженості інформації, спрямованих на користувачів інтернет-послуг і (або) походять від них;

– здійснювати з 01.01.2020 р при наданні послуг з розміщення в мережі Інтернет інформаційних систем і (або) інформаційних ресурсів адресацію за технологією, яка передбачає повну підтримку інтернет-протоколів версій 4 і 6 мережевими пристроями;

– забезпечувати з 01.01.2020 р надання інтернет-послуг за технологією, яка передбачає повну підтримку інтернет-протоколу версії 6 мережевими пристроями [15].

Безумовно, вимоги до Інтернет-провайдерів щодо надання послуг значно вищі, ніж в Україні, однак деякі елементи правового регулювання можуть бути застосовані і в нашій державі, з огляду на характер і інтенсивність кібератак та кіберінцидентів.

Розвиток системи протидії протиправним кіберпосяганням у Республіці Казахстан

У Республіці Казахстан (далі – РК) створена досить розгалужена система суб'єктів системи кібербезпеки РК. Управління інформаційною безпекою, а також забезпечення кібербезпеки держави покладено на Міністерство оборонної та аерокосмічної промисловості РК (далі – МОАП РК), створене Указом Президента РК від 06.10.2016 року № 350 [16]. У складі МОАП РК було створено Республіканський державний заклад – Комітет з інформаційної безпеки (наказ МОАП РК від 04.07.2017 року № 125/НК) [17]. Фактично, зі створенням зазначеного органу, було засновано уповноважений регулятор РК з питань розробки державної політики в сфері національної інформаційної безпеки.

Основним суб'єктом забезпечення кібербезпеки в РК є Комітет національної безпеки РК (далі – КНБ РК), до складу якого включено Державну технічну службу (ДТС) РК. Остання здійснює діяльність в сфері інформатизації, електронного документу та електронного цифрового підпису, в галузі зв'язку та телерадіомовлення. Основними функціями ДТС є: моніторинг забезпечення захисту об'єктів "електронного уряду", технічне супроводження системи централізованого управління мережами телекомунікацій РК, супроводження єдиного шлюзу доступу до Інтернету та єдиного шлюзу електронної пошти "електронного уряду", технічне супроводження робіт з відбору частот для телерадіомовлення, радіочастот (радіочастотних каналів) тощо.

До складу ДТС КНБ РК входять:

– Служба реагування на комп'ютерні інциденти (KZ-CERT) – надає консультативні та технічну підтримку користувачам з питань попередження загроз комп'ютерній безпеці, забезпечує збирання та аналіз інформації про комп'ютерні інциденти;

– Національний засвідчувальний центр – надає засоби цифрового електронного підпису фізичним та юридичним особам;

– Центр засвідчення державних органів – відповідає за побудову електронного документообігу між державними органами з використанням технологій електронного цифрового підпису, який використовується також і в Інтернет-порталі державних органів та відомчих системах електронного документообігу держаних установ [18].

У РК 30.06.2017 року затверджена Концепція кібербезпеки ("Кіберщит Казахстану") (далі – Концепція) [19], яка має на меті забезпечувати безпеку електронних інформаційних ресурсів, інформаційних систем та інформаційно-комунікаційної інфраструктури від зовнішніх та внутрішніх загроз для створення умов сталого розвитку РК в умовах глобальної конкурентоздатності. Концепцією визначено основні напрямки реалізації державної політики в сфері захисту електронних інформаційних ресурсів, інформаційних систем та мереж телекомунікацій, забезпечення безпечного використання ІКТ. У Концепції викладена оцінка поточної обстановки в сфері інформатизації державних органів РК, автоматизації держаних послуг, перспектив розвитку "цифрової" економіки, системи "електронний уряд", технологічної модернізації виробничих процесів в промисловості, розширення галузі надання інформаційно-комунікаційних послуг, створення та функціонування національної Служби реагування на комп'ютерні інциденти KZ-CERT тощо.

Постановою Уряду РК від 28.10.2017 року затверджено "План заходів з реалізації Концепції кібербезпеки ("Кіберщит Казахстану") до 2022 року" (далі – План), який охоплює органі-

ISSN 1995-6134

заційно-правові та технічні заходи, а також заходи з управління людським потенціалом та популяризації методів безпечного використання ІКТ [20]. Виконання Плану розподілено на два етапи, перший з яких вже завершено, а другий реалізується у 2019–2022 роках.

Оскільки на першому етапі було заплановано здійснення ревізії навчальних програм та професійних стандартів, збільшення кількості та якості підготовлених фахівців в сфері інформаційної безпеки, а також підвищення кваліфікації діючих співробітників, зайнятих у зазначеній сфері, то для України питання освіти має також стати одним із пріоритетів розвитку Національної системи кібербезпеки. Крім того, зазначеним Планом на першому етапі передбачено збудувати ефективну систему взаємодії та кооперації між промисловістю та наукою в створенні казахських розробок, що закладе основу для розвитку національного та галузевих оперативних центрів інформаційної безпеки.

Саме цей напрям розвитку системи протидії кіберпосяганням в Україні варто врахувати при удосконаленні організаційно-правової основи для розбудови системи протидії кіберпосяганням на електронні ресурси.

Другий етап реалізації Концепції кібербезпеки передбачає ключову участь казахських IT-компаній у забезпеченні національної ІКТ системами інформаційної безпеки, а також забезпечення вітчизняних підприємств електронної промисловості замовленнями на придбання державними органами та квазідержавним сектором телекомунікаційного обладнання, яке вироблено та пройшло процедуру сертифікації на відповідність вимогам інформаційної безпеки на території РК.

Протидія протиправним кіберпосяганням у Сінгапурі

В Сінгапурі впроваджено Національну програму з кібербезпеки (The National Cybersecurity R&D Programme) [21], спрямовану на підвищення стійкості кіберінфраструктури держави. До неї включені такі державні установи, як: Координаційний центр національної безпеки (NSCS) Сінгапуру, Національний науково-дослідний фонд (NRF) Сінгапуру, Національне агентство кібербезпеки Сінгапуру (CSA), Міністерство оборони (MINDEF), Міністерство внутрішніх справ (МНА), Адміністрація розвитку інформаційних комунікацій Сінгапуру (IDA) та Рада з економічного розвитку (EDB), що сприяють поглибленню співпраці між установами, науковими установами, науково-дослідними інститутами та приватним сектором в сфері кібербезпеки.

Для координації діяльності в сфері кібербезпеки у 2015 році було створено Агентство з кібербезпеки Сінгапуру (Cyber Security Agency of Singapore, CSA [22]), яке входить до складу Офісу Прем'єр-міністра та керується Міністерством зв'язку та інформації Сінгапуру, має функцією розробку стратегії кібербезпеки, нагляд за операційною і освітньою діяльністю, розвитком екосистем у цій сфері. CSA виконує наступні основні функції: планування та розвитку (з питань кібернетичної екосистеми, технологічних питань, захисту критичної інформаційної інфраструктури); міжнародного співробітництва (питання взаємодії, стратегії, планування та партнерства); операційний (Національний центр аналізу кіберзагроз, Національний центр моніторингу кіберзагроз та Національний центр реагування на кіберінциденти). Головною метою Національного центру моніторингу кіберзагроз є попередження операторів об’єктів критичної інформаційної інфраструктури про можливе виникнення кібернетичних загроз, характерних для їх операційного середовища, що сприяє своєчасному зменшенню впливу кібератак. Національний центр аналізу кіберзагроз проводить дослідження та аналіз джерел кіберзагроз та перспективні напрямки вчинення кіберзлочинів проти Сінгапуру, а Національний центр реагування на кіберінциденти впроваджує спеціальні заходи з метою пом’якшення наслідків кіберінцидентів на національному рівні та здійснює управління Командою реагування на кіберінциденти Сінгапуру (SingCERT).

CSA була розроблена Національна стратегія кібербезпеки Сінгапуру, яка серед іншого включає питання посилення стійкості об’єктів критичної інформаційної інфраструктури Сінгапуру. У цьому напрямку, зокрема, передбачається забезпечити співпрацю уряду з операторами об’єктів критичної інформаційної інфраструктури та представниками зі сфери забезпечення кібербезпеки щодо посилення обізнаності суспільства та проведення регулярних навчань в сфері боротьби з кіберзагрозами із залученням приватного та державного секторів, розширення більшої кількості Національних груп реагування на кіберінциденти (NCIRT), виділення 8 % усіх витрат уряду на IT сферу для забезпечення кібербезпеки.

Висновки

1. Значна увага в Республіці Бєларусь приділяється питанням безпеки об’єктів критичної інфраструктури, поняття "критично важливий об’єкт інформатизації" є тотожним із поняттям

ISSN 1995-6134

"об'єкт критичної інформаційної інфраструктури", яке застосовується у вітчизняному законодавстві. У РБ заборонено використовувати на її території програмне забезпечення або технічне обладнання, яке не відповідає вимогам встановлених у цій країні стандартів, а захист критично важливих об'єктів та їх сукупності або критичної інфраструктури вважається одним із найбільш важливих завдань національної безпеки країни. У РБ перелік вимог, які висуваються до уповноважених постачальників Інтернет послуг (провайдерів), значно вищі, ніж в Україні, однак деякі елементи правового регулювання можуть бути застосовані і в нашій державі, з огляду на характер і інтенсивність кібератак та кіберінцидентів, звичайно з дотриманням демократичних принципів впровадження механізмів правового регулювання.

2. У Республіці Казахстан функціонує централізована система протидії кіберпосяганням. Правову основу для розбудови відповідної системи закладає Концепція кібербезпеки ("Кіберщит Казахстану"), якою зокрема заплановано здійснення ревізії навчальних програм та професійних стандартів, збільшення кількості та якості підготовлених фахівців в сфері інформаційної безпеки, а також підвищення кваліфікації діючих співробітників, зайнятих у зазначеній сфері, а також розбудова ефективної системи взаємодії та кооперації між промисловістю та наукою в створенні казахських розробок для розвитку національного та галузевих оперативних центрів інформаційної безпеки. Відповідні питання розвитку системи протидії кіберпосяганням визнано актуальними для України.

3. Прийнятною для України є система координації діяльності в сфері кібербезпеки Сінгапуру у частині створення Агентства з кібербезпеки, яке входить до складу Офісу Прем'єр-міністра та керується Міністерством зв'язку та інформації, і має функцією розробку стратегії кібербезпеки, нагляд за операційною і освітньою діяльністю, розвитком екосистем у цій сфері тощо.

Перспективами подальших наукових пошуків визначаємо питання удосконалення Національної системи кібербезпеки в Україні.

Конфлікт інтересів

Автор статі повідомляє про відсутність конфлікту інтересів.

Вираз вдячності

Дослідження не отримало будь-якої фінансової підтримки з боку юридичних чи фізичних осіб.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Лук'янчук Р. В. Міжнародне співробітництво у сфері забезпечення кібернетичної безпеки: державні пріоритети. *Вісник Національної академії державного управління при Президентові України*. 2015. № 4. С. 50–56.
2. Марущак А. І. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. *Безпека інформації*. 2019. Том 25. № 1. С. 13–17. DOI: 10.18372/2225-5036.25.13665.
3. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *The International Journal of Critical Infrastructure Protection*, 393(4), 103–117.
4. Shukla, S. K. (2016). Cyber security of cyber physical systems: Cyber threats and defense of critical infrastructures. *In Proceedings of the 29th International Conference on VLSI Design*.
5. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885.
6. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40.
7. Bisogni, F. (2016). Proving limits of state data breach notification laws: Is a federal law the most adequate solution? *Journal of Information Policy*, 6, 514–205.
8. Milton Mueller, Andreas Kuehn. Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change. URL: https://www.econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf.
9. Петров С. Г. Міжнародний досвід з протидії протиправним посяганням на державні електронні інформаційні ресурси. *Інформаційна безпека людини, суспільства, держави*. 2019. № 2(26). С. 15–21.
10. Петров С. Г. Організаційні і правові основи вирішення проблем протидії кіберпосяганням у Європейському Союзі. *Інформація і право*. 2020. № 1. С. 99–105.
11. Eastern Partnership. URL: http://ukraine-eu.old.mfa.gov.ua/en/ukraine-eu/eu-policy/east-partnership.
12. Положение о порядке отнесения объектов информатизации к критически важным объектам информатизации, в редакции Указа Президента Республики Беларусь от 09.12.2019 р. № 449. URL: https://oac.gov.by/public/content/files/files/law/decrees-rb/2019%20-%20449.pdf.

ISSN 1995-6134

13. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163–VIII. *Відомості Верховної Ради України.* 2017. № 45. Ст. 403.
14. О совершенствовании порядка передачи сообщений электросвязи: Указ Президента Республики Беларусь от 15.03.2016 № 98. URL: https://oac.gov.by/public/content/files/files/law/decrees-rb/2016-98.pdf.
15. О мерах по совершенствованию использования национального сегмента сети Интернет: Указ Президента Республики Беларусь от 01.02.2010 № 60. URL: https://oac.gov.by/public/content/files/files/law/decrees-rb/2010-60.pdf.
16. Об образовании Министерства оборонной и аэрокосмической промышленности Республики Казахстан: Указ Президента РК от 06.10.2016 № 350. URL: http://www.akorda.kz/ru/events/akorda_news/akorda_other_events/ob-obrazovanii-ministerstva-oboronnoi-i-aerokosmicheskoi-promyshlennosti-respubliki-kazahstan.
17. О внесении изменений в приказ МОАП РК от 17 ноября 2016 года № 5/НК "Об утверждении Положения республиканского государственного учреждения "Комитет по информационной безопасности МОАП РК: Приказ МОАП РК от 04.07.2017 № 125/НК. URL: http://mdai.gov.kz/ru/kategorii/polozhenie-16.
18. Государственная техническая служба Комитета национальной безопасности Республики Казахстан. URL: https://www.gov.kz/memleket/entities/knb/press/article/details/727?lang=ru.
19. Об утверждении Концепции кибербезопасности ("Киберщит Казахстан")": Постановление Правительства Республики Казахстан от 30.06.2017 № 407. URL: https://online.zakon.kz/Document/?doc_id=39754354#pos=0;251.
20. Утвержден План мероприятий по реализации Концепции кибербезопасности ("Киберщит Казахстана") до 2022 года. URL: https://www.zakon.kz/4886464-utverzhden-plan-meropriyatiy-po.html.
21. The National Cybersecurity R&D Programme. URL: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme.
22. Our Organisation, Cyber Security Agency of Singapore. URL: https://www.csa.gov.sg/who-we-are/our-organisation.

REFERENCES

1. Luk'yanchuk, R. V. (2015). Mizhnarodne spivrobitnytstvo u sferi zabezpechennya kibernetychnoyi bezpeky: derzhavni priorytety [International cooperation in the field of cyber security: state priorities]. *Visnyk Natsional'noyi akademiyi derzhavnoho upravlinnya pry Prezydentovi Ukrayiny,* (4). 50–56 (in Ukr.).
2. Marushchak, A. I. (2019). Yevropeys'kyy dosvid z pytan' borot'by z pravoporushennyamy v informatsiyniy sferi [European experience in combating information offenses]. *Bezpeka informatsiyi,* 25(1). 13–17. DOI: 10.18372/2225-5036.25.13665 (in Ukr.).
3. Moore, T. (2010). The economics of cybersecurity: Principles and policy options. *The International Journal of Critical Infrastructure Protection*, 393(4), 103–117.
4. Shukla, S. K. (2016). Cyber security of cyber physical systems: Cyber threats and defense of critical infrastructures. *In Proceedings of the 29th International Conference on VLSI Design*.
5. Hathaway, O. A., Crootof, R., Levitz, P., Nix, H., Nowlan, A., Perdue, W., & Spiegel, J. (2012). The law of cyber-attack. *California Law Review*, 100(4), 817–885.
6. Farwell, J. P., & Rohozinski, R. (2011). Stuxnet and the future of cyber war. *Survival*, 53(1), 23–40.
7. Bisogni, F. (2016). Proving limits of state data breach notification laws: Is a federal law the most adequate solution? *Journal of Information Policy*, 6, 514–205.
8. Mueller, Milton, & Kuehn, Andreas. Einstein on the Breach: Surveillance Technology, Cybersecurity and Organizational Change. Retrieved from: https://www.econinfosec.org/archive/weis2013/papers/MuellerKuehnWEIS2013.pdf.
9. Petrov, S. H. (2019). Mizhnarodnyy dosvid z protydiyi protypravnym posyahannyam na derzhavni elektronni informatsiyni resursy [International experience in combating unlawful encroachment on state electronic information resources]. *Informatsiyna bezpeka lyudyny, suspil'stva, derzhavy,* 2(26). 15–21 (in Ukr.).
10. Petrov, S. H. (2020). Orhanizatsiyni i pravovi osnovy vyrishennya problem protydiyi kiberposyahannyam u Yevropeys'komu Soyuzi [Organizational and legal bases for solving the problems of combating cyber-encroachment in the European Union]. *Informatsiya i pravo,* (1). 99–105 (in Ukr.).
11. Eastern Partnership. Retrieved from: http://ukraine-eu.old.mfa.gov.ua/en/ukraine-eu/eu-policy/east-partnership.

12. *Polozheniye o poryadke otneseniya ob"yektov informatizatsii k kriticheski vazhnym ob'yektam informatizatsii* [Regulations on the procedure for classifying objects of informatization as critical objects of informatization]. V redaktsii Ukaza Prezidenta Respubliki Belarus' (09.12.2019 No 449). Retrieved from: https://oac.gov.by/public/content/files/files/law/decrees-rb/2019%20-%20449.pdf (in Russ.).
13. Pro osnovni zasady zabezpechennya kiberbezpeky Ukrayiny [On the basic principles of cybersecurity in Ukraine]. Zakon Ukrayiny (05.10.2017 No 2163–8). *Vidomosti Verkhovnoyi Rady Ukrayiny,* (45). 403 (in Ukr.).
14. *O sovershenstvovanii poryadka peredachi soobshcheniy elektrosvyazi* [On improving the procedure for transmitting telecommunication messages]. Ukaz Prezidenta Respubliki Belarus' (15.03.2016 No 98). Retrieved from: https://oac.gov.by/public/content/files/files/law/decrees-rb/2016-98.pdf (in Russ.).
15. *O merakh po sovershenstvovaniyu ispol'zovaniya natsional'nogo segmenta seti Internet* [On measures to improve the use of the national segment of the Internet]. Ukaz Prezidenta Respubliki Belarus' (01.02.2010 No 60). Retrieved from: https://oac.gov.by/public/content/files/files/law/decrees-rb/2010-60.pdf (in Russ.).
16. *Ob obrazovanii Ministerstva oboronnoy i aerokosmicheskoy promyshlennosti Respubliki Kazakhstan* [On the establishment of the Ministry of Defense and Aerospace Industry of the Republic of Kazakhstan]. Ukaz Prezidenta RK (06.10.2016 No 350). Retrieved from: http://www.akorda.kz/ru/events/akorda_news/akorda_other_events/ob-obrazovanii-ministerstva-oboronnoi-i-aerokosmicheskoi-promyshlennosti-respubliki-kazahstan (in Russ.).
17. *O vnesenii izmeneniy v prikaz MOAP RK ot 17 noyabrya 2016 goda № 5/NK "Ob utverzhdenii Polozheniya respublikanskogo gosudarstvennogo uchrezhdeniya "Komitet po informatsionnoy bezopasnosti MOAP RK* [On amendments to the order of the IOAP of the Republic of Kazakhstan dated November 17, 2016 No. 5 / NK "On approval of the Regulations of the Republican State Institution" Information Security Committee of the IOAP of the RK]. Prikaz MOAP RK (04.07.2017 No 125/HK). Retrieved from: http://mdai.gov.kz/ru/kategorii/polozhenie-16 (in Russ.).
18. *Gosudarstvennaya tekhnicheskaya sluzhba Komiteta natsional'noy bezopasnosti Respubliki Kazakhstan* [State Technical Service of the National Security Committee of the Republic of Kazakhstan]. Retrieved from: https://www.gov.kz/memleket/entities/knb/press/article/details/727?lang=ru (in Russ.).
19. *Ob utverzhdenii Kontseptsii kiberbezopasnosti ("Kibershchit Kazakhstan")"* [On approval of the Concept of cybersecurity ("Cyber shield Kazakhstan")"]. Postanovleniye Pravitel'stva Respubliki Kazakhstan (30.06.2017 No 407). Retrieved from: https://online.zakon.kz/Document/?doc_id=39754354#pos=0;251 (in Russ.).
20. *Utverzhden Plan meropriyatiy po realizatsii Kontseptsii kiberbezopasnosti ("Kibershchit Kazakhstana") do 2022 goda* [The Action Plan for the Implementation of the Cybersecurity Concept ("Cyber Defense of Kazakhstan") until 2022 was approved]. Retrieved from: https://www.zakon.kz/4886464-utverzhden-plan-meropriyatiy-po.html (in Russ.).
21. The National Cybersecurity R&D Programme. Retrieved from: https://www.nrf.gov.sg/programmes/national-cybersecurity-r-d-programme.
22. Our Organisation, Cyber Security Agency of Singapore. Retrieved from: https://www.csa.gov.sg/who-we-are/our-organisation.

ІНФОРМАЦІЯ ПРО СТАТТЮ (ARTICLE INFO)

Published in:
Форум права: 61 pp. 114–121.

Related identifiers:
10.5281/zenodo.3883823
http://forumprava.pp.ua/files/114-121-2020-2-FP-Petrov_12.pdf
http://nbuv.gov.ua/UJRN/FP_index.htm_2020_2_12.pdf

Received: 30.04.2020
Accepted: 26.05.2020
Published: 03.06.2020

Cite as:

Петров, С. Г. (2020). Організаційно-правові основи протидії кіберпосяганням в іноземних державах: актуальні приклади для України. *Форум Права,* 61(2). 114–121. DOI: http://doi.org/10.5281/zenodo.3883823.

Petrov, S. G. (2020). Orhanizatsiyno-pravovi osnovy protydiyi kiberposyahannyam v inozemnykh derzhavakh: aktual'ni pryklady dlya Ukrayiny [Organizational and Legal Basis for Combating Cyber Attacks in Foreign Countries: Actual Examples for Ukraine]. *Forum Prava,* 61(2). 114–121. DOI: http://doi.org/10.5281/zenodo.3883823.