

інформаційної підтримки внутрішнього ринку, активне рекламування і пропагування природно-ресурсного та економічного потенціалів території.

Список використаних джерел:

1. Про передачу об'єктів права державної та комунальної власності: Закон України від 03.03.1998 р. Відомості Верховної Ради України. 1998. Ст. 228.
2. Про концесії: Закон України від 16.07.1999 р. Відомості Верховної Ради України. 1999. №41. С. 372.
3. Про державно-приватне партнерство: Закон України від 01.07.2010 р. Урядовий кур'єр. 2010. № 160. С. 9–11.
4. Про внесення змін до деяких законів України з метою стимулювання концесійної діяльності: Закон України від 03.02.2004 р. Відомості Верховної Ради України. 2004. №19. Ст. 254.
5. Инвестиционный Кодекс Республики Беларусь. URL. www.minsk.by/law/invest.html
6. Вдовенко В.С. Приватно-державне партнерство в автодорожній сфері. Чернігів: ЧДТУ, 2009. 197 с.
7. Джабраїлов Р.А. Господарська правосуб'єктність міста: теорія і практика : [монографія] / Р.А. Джабраїлов; НАН України. Ін-т економіко-правових досліджень. Донецьк : «Ноулідж», 2010. 455 с.

ІНФОРМАЦІЙНА БЕЗПЕКА: ІМПЛЕМЕНТАЦІЯ ЗАКОНІВ ЄВРОСОЮЗУ В ЗАКОНОДАВСТВО УКРАЇНИ

Манелюк Ю.М., доцент кафедри
політичних технологій ДВНЗ
«Київський національний
економічний університет імені Вадима
Гетьмана» канд. політ. наук,

Створення та реформування сфери кібербезпеки в Україні на сьогодні неможливо без вивчення законодавства ЄС. Разом із цим, неможливо Україні здійснити імплементацію законодавства відповідно до Угоди про Асоціацію без врахування сучасних

тенденцій та механізмів кіберзахисту, закріплених у сучасному законодавстві ЄС.

Тому вкрай важливим є вивчення та врахування в роботі основних документів ЄС із питань кібербезпеки, а також досвіду країн-членів ЄС лідерів із цього важливого питання. Сама ідеологія побудови безпечного «електронного суспільства» та створення «єдиного цифрового ринку» в країнах ЄС вимагає постійного моніторингу ситуації та реформування законодавства.

6 липня 2016 року Європейський парламент та Рада Європейського Союзу прийняли Директиву (ЄС) №2016/1148, що отримала назву «Безпека мереж та інформації» (Network and Information Security, або NIS) (далі Директива NIS) та фактично набрала чинності з 09.05.2018 р [1].

Директива NIS спрямована покращити можливості кібербезпеки на національному рівні та сприяти кращому спілкуванню між країнами-членами ЄС. Це передбачає, що кожна держава-член прийме національну стратегію щодо досягнення високого рівня кібербезпеки для мереж та інформаційних систем по основних службах [2].

Метою директиви NIS є запобігання сценаріїв порушення інформаційної безпеки (хакерство), які часто є популярними епізодами у багатьох фільмах, але вони також стають все більш поширеними у реальному житті.

Наступна директива GDPR (General Data Protection Regulation/Загальний регламент по захисту даних) вступила в дію з травня 2018 року. Відповідно до неї принципи та правила захисту фізичних осіб стосовно обробки їх персональних даних повинні здійснюватися незалежно від громадянства або місця проживання осіб, при цьому, поважаючи їх основні права і свободи, зокрема їх право на захист персональних даних [3].

Проблемам аналізу та вдосконалення (реформування) законодавства в сфері забезпечення інформаційної безпеки присвячено поодинокі наукові праці, що розкривають окремі питання правового регулювання інформаційних правовідносин (В. Б. Авер'янов, А. Б. Агапов, І. В. Арістова, О. М. Бандурка, О. А. Баранов, Ю. М. Батурін, В. В. Костицький, В. К. Колпаков та ін.).

Українське законодавство вже має низку нормативно-правових документів та законів, що описують проблеми забезпечення кібербезпеки держави та шлях подолання цих проблем [4, 5].

Одним із найважливіших кроків на шляху розбудови системи кібербезпеки України є «Стратегія Кібербезпеки України» (далі Стратегія), затверджена 15 березня 2016 року указом Президента України. Новий закон в першу чергу спрямований на формування загальної державної політики у галузі кібербезпеки, а також розподіл ролей між різними державними інституціями. Зокрема, він регулює повноваження спецслужб для здійснення кіберзахисту країни [4].

На даний момент триває активна реалізація низки спільних проєктів між Україною та іншими державами щодо кібербезпеки. Серед них — допомога американського уряду з підготовки українських фахівців з кіберзахисту, консультації з іноземними радниками, постачання технічного обладнання для Центру оперативного реагування на кіберзагрози тощо. [6]

Верховною Радою України ухвалено «Закон про захист персональних даних», введений в дію з 1 січня 2014 року. Цей закон накладає на Україну ряд зобов'язань. А саме: забезпечити дотримання прав і свобод людини, зокрема права на недоторканність приватного життя. Відповідно до закону будь-які відомості, які дають змогу ідентифікувати конкретну фізичну особу, можна віднести до персональних даних. Така інформація є конфіденційною і може оброблятися тільки за згодою цієї фізичної особи. [5] Серед головних нововведень — повноваження з контролю за додержанням цього закону покладено на омбудсмена країни.

Згідно з дослідженням «Глобальний індекс кібербезпеки» (Global Cybersecurity Index), який щорічно проводиться Міжнародним союзом електрозв'язку (ITU), в 2017 році Україна зайняла «почесне» 59 місце в рейтингу з 193 можливих [7].

За спостереженням закордонних та українських науковців, всі запроваджені законодавчі ініціативи відповідають загальноприйнятим демократичним вимогам [8]. У розроблених документах все правильно написано, визначені актуальні та потенційні загрози інформаційної безпеки. Проте виконавча частина законодавства в частині інформаційної безпеки залишається слабкою, адже для того, щоб ті чи інші позиції законів виконувались, необхідна належна фінансова підтримка.

Підтвердженням цього є результати дослідження GCI, де чітко визначено, що реалізація цього законодавства на практиці не є достатньою (червона зона).

Серед проблем можна виокремити такі:

- Недостача профільованих актуальних стандартів та методологій;
- Недостатній рівень імплементацій мір кіберзахисту в ІТ-інфраструктурах;
- Недостатньо агітаційно-активний процес навчання та підвищення рівня обізнаності в питаннях кібербезпеки;
- Недостатньо високий ступінь інтеграції України в міжнародну співпрацю з питань забезпечення кібербезпеки.

Незважаючи на деякі проблеми з погляду юридичного забезпечення інформаційної безпеки, в Україні активно пропагандується інформаційна безпека і до цього докладають зусиль не тільки активісти, а й уряд.

Наприклад, «білі хакери» з КІП імені Ігоря Сікорського зайняли 1-е місце у світі за підсумками змагань «Capture the Flag», обійшовши 12 000 «білих» хакерських груп з усього світу [9].

В Україні стартує програма для стартапів з призовим фондом у 1 000 000 дол. Програма буде керуватися 1991 Open Data Incubator, співпрацюючи з Cyber Guard (проект державного концерну «Укроборонпром») і групою підприємств Hacken [10].

Розуміючи, що приведення українського законодавства у відповідність до європейських стандартів неможливе без відповідного інституційного механізму, на базі Центру європейського та порівняльного права, відповідно до Постанови КМУ від 24 грудня 2004 року, був створений Державний департамент адаптації законодавства. Основними завданнями якого є:

1. Організація роботи з реалізації державної політики у сфері адаптації законодавства України до законодавства Європейського Союзу.

2. Участь у межах своєї компетенції в координації роботи, пов'язаної з виконанням Загальнодержавної програми адаптації законодавства України до законодавства ЄС.

3. Організація науково-експертного, аналітичного, інформаційного та методологічного забезпечення євроінтеграції.

4. Проведення експертизи щодо відповідності проектів законів України та інших нормативно-правових актів, що за предметом правового регулювання належать до сфер, правовідносини в яких регулюються правом Європейського Союзу, *acquis communautaire*.

5. Узагальнення інформації про стан адаптації законодавства України до законодавства ЄС.

Прагнення України стати членом ЄС обумовило необхідність обов'язкового прийняття *acquis communautaire* — сукупності цілей, принципів і норм спільної політики та законодавства ЄС, а також юридичних та інституційних механізмів їхнього впровадження [11].

Кіберпростір є важливим аспектом в житті будь-якої людини та суспільства. Але гострим постає питання забезпечення інформаційної безпеки на всіх рівнях від звичайного користувача до держави. За останні роки Україна зробила прогресивні кроки у створенні ефективної національної системи кібербезпеки. Проте законодавча база поки що лише частково охоплює елементи, які потрібні для ефективної та швидкої протидії кіберзагрозам. Вже ні в кого не викликає сумнів, що законодавство країни у галузі інформаційної безпеки має відповідати міжнародним стандартам і цей процес має відбуватися динамічно.

Список використаної літератури:

1. Вадим Баранов: Кібербезпека у 2018 році: новий виклик для бізнесу, необхідність чи побажання? URL. <http://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/kiberbezpeka-u-2018-roci-noviy-viklik-dlya-biznesu-neobhidnist-chi-pobazhannya.html>

2. 10 Things to Know About the Network and Information Security Directive. URL. <https://www.tripwire.com/state-of-security/security-data-protection/10-things-to-know-about-the-network-and-information-security-directive/>

3. GDPR — нові правила обробки персональних даних в Європі для міжнародного IT-ринку. URL. <https://m.habr.com/company/digitalrightscenter/blog/344064/>

4. Указ Президента України «Стратегія кібербезпеки України» від 15 березня 2016 року № 96/2016. URL. <http://zakon.rada.gov.ua/laws/show/96/2016>

5. Закон України «Про захист персональних даних» від 1 червня 2010 року №2297-VI. URL. <http://zakon.rada.gov.ua/laws/show/2297-17>

6. Кібербезпека: виклики та завдання. URL. <https://blogs.pravda.com.ua/authors/popova/5aa639aaa527c/>

7. ITU Global Cybersecurity Index (GCI) 2017: Глобальний індекс кібербезпеки. URL. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf

8. Інформаційна безпека в Україні: зрада чи перемога? URL. <http://porogy.zp.ua/2017/11/informatsijna-bezpeka-v-ukrayini-zrada-chy-peremoga/>

9. Діана Овсепян: Кіберприкриття: інформаційною безпекою України займуться США, Чилі, Канада і Туреччина. URL. <https://ru.rt.com/8bbh>

10. В Україні запускають програму для стартапів в кібербезпеки з призовим фондом \$1млн. URL. <https://delo.ua/special/v-ukraine-zapuskajut-programmu-dlja-startapov-v-sfere-kiberbezop-334849/>

11. В. А. Ліпкан, Ю. Є. Максименко, В. М. Желіховський Інформаційна безпека України в умовах євроінтеграції: Навчальний посібник. К.: КНТ, 2006. 280 с.

ПРОБЛЕМНІ ПИТАННЯ ЗАСТОСУВАННЯ ВАЛЮТНОГО ЗАКОНОДАВСТВА УКРАЇНИ ДЛЯ ЗАБЕЗПЕЧЕННЯ ВІЛЬНОГО РУХУ КАПІТАЛІВ

Нечипоренко О.Ю., доцент кафедри фінансового права ДВНЗ «Київський національний економічний університет імені Вадима Гетьмана», кандидат економічних наук, доцент

З прийняттям Закону України «Про валюту і валютні операції» від 21.06.2018 р. № 2473-VIII (далі — Закон про валюту) [1] Україною здійснено один з етапів адаптації національного законодавства із законодавством Європейського Союзу.

Із набуттям чинності Закону про валюту було взято курс на лібералізацію валютного ринку, що має на меті поступове скасування більшості обмежень, які були визначені Декретом Кабінету Міністрів України «Про систему валютного регулювання і валютного контролю» [2], в тому числі і для вільного руху капіталів в контексті реалізації Угоди про асоціацію з ЄС.

Для реалізації Угоди про асоціацію з ЄС вкрай необхідною є адаптація валютного законодавства України під Директиву Ради ЄС