ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ

Збірник тез доповідей V Міжнародної науково-практичної конференції ІБІТ 2024

27 листопада 2024 року

Міністерство освіти і науки України
Державна служба України з надзвичайних ситуацій
Львівський державний університет безпеки життєдіяльності
Національний університет “Львівська політехніка”

ІНФОРМАЦІЙНА БЕЗПЕКА ТА ІНФОРМАЦІЙНІ ТЕХНОЛОГІЇ ІБІТ 2024

Збірник доповідей
V Міжнародної науково-практичної конференції

27 листопада 2024 року

Львів – 2024

ББК 32.81+78.362

*Інформаційна безпека та інформаційні технології: з*бірник доповідей V Міжнародної науково-практичної конференції, ІБІТ 2024, м. Львів, 27 листопада 2024 року. Львів, ЛДУ БЖД, 2024, 661 с.

Ольга МЕНЬШИКОВА – к.ф.-м.н., доцент, заступник начальника факультету цивільного захисту Львівського державного університету безпеки життєдіяльності з навчально-наукової роботи;

Андрій ІВАНУСА – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валентина ЯЩУК – к.е.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Орест ПОЛОТАЙ – к.т.н., доцент, доцент кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Валерія БАЛАЦЬКА – викладач кафедри управління інформаційною безпекою Львівського державного університету безпеки життєдіяльності;

Ігор МАЛЕЦЬ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Назарій БУРАК – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Ольга СМОТР – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Юрій БОРЗОВ – к.т.н., доцент, доцент кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Роман ГОЛОВАТИЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності;

Олександр ХЛЕВНОЙ – к.т.н., старший викладач кафедри інформаційних технологій та систем електронних комунікацій Львівського державного університету безпеки життєдіяльності.

УДК 351.81

ПЕРСПЕКТИВИ ІМПЛЕМЕНТАЦІЇ ЗАКОНОДАВСТВА ЄС ДЛЯ ЕФЕКТИВНОГО ЗАХИСТУ КРИТИЧНОЇ ІНФРАСТРУКТУРИ ФІНАНСОВОГО СЕКТОРУ

Ірина БЕРДИЧЕНКО[1]
Ярослав ДОРОГИЙ[2]
Олена ДОРОГА-ІВАНЮК

[1]Донецький національний технічний Університет, Дрогобич, Україна

[2]Донецький національний технічний Університет, Дрогобич, Україна

[3]Пологівський ліцей Ковалівської територіального громади с. Пологи, Білоцерківський район, Київська обл., Україна

Abstract. *Last year, a historic event took place – the European Council agreed to start negotiations on Ukraine's accession to the EU. This process involves a set of systemic reforms, among the key ones – further adaptation of Ukrainian legislation to EU law. The financial sector is not left out of this activity. The priority areas are further implementation into national legislation of the provisions of Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (DORA) [1] and alignment with the provisions of Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC [2].*

Keywords: *critical infrastructure, EU legislation, financial sector, critical infrastructure protection.*

Анотація. *У минулому році відбулася історична подія – Європейська Рада дала згоду розпочати перемовини про вступ України до ЄС. Цей процес передбачає комплекс системних реформ, серед ключових – подальша адаптація українського законодавства до права Євросоюзу. Фінансовий сектор не залишається осторонь у цій діяльності. Пріоритетними напрямками є подальша імплементація у національне законодавство положень Регламенту (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) [1] та узгодження з нормами Директиви (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих суб'єктів і скасування Директиви Ради 2008/114/ЕС [2].*

Ключові слова: *критична інфраструктура, законодавство ЄС, фінансовий сектор, захист критичної інфраструктури.*

Вступ. Поточний стан національного законодавства свідчить про позитивні кроки, які відбулись впродовж останніх років у напряму підвищення ефективного забезпечення кібербезпеки та стійкості критичної інфраструк-

тури, що було обумовлено, перш за все, гармонізацією з європейським законодавством.

Імплементація положень вищезгаданих правових актів ЄС знайшла своє відображення у таких законах нашої країні: «Про основні засади забезпечення кібербезпеки України» [3], «Про критичну інфраструктуру» [4], «Про захист інформації в інформаційно-комунікаційних системах» [5], «Про платіжні послуги» [6], «Про фінансові послуги та фінансові компанії» [7], а також низки рішень Уряду, серед іншого Стратегії кібербезпеки України [8].

Шляхи імплементації законодавства ЄС. Національний банк України, як регулятор банківської системи в Україні, а з 1 липня 2020 року – регулятор ринку небанківських фінансових послуг: страхових, лізингових, факторингових компаній, кредитних спілок, ломбардів та інших фінансових компаній, не залишається осторонь від євроінтеграційних процесів.

НБУ відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» є основним суб'єктом національної системи кібербезпеки України та організовує заходи із забезпечення кібербезпеки у фінансовому секторі, серед іншого, визначає порядок, вимоги та заходи із забезпечення кіберзахисту та інформаційної безпеки банками, іншими особами, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням; створює центр кіберзахисту Національного банку України, забезпечує функціонування системи кіберзахисту для банків, інших осіб, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг; забезпечує проведення оцінювання стану кіберзахисту та аудиту інформаційної безпеки на об'єктах критичної інфраструктури в банках, інших особах, що здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк України, операторах платіжних систем та/або учасниках платіжних систем, технологічних операторах платіжних послуг.

НБУ є одним із органів, який здійснює управління національною системою захисту критичної інфраструктури на загальнодержавному рівні та, водночас, виконує функції секторального органу у сфері захисту критичної інфраструктури фінансового сектору, і відповідно, наділений широким колом повноважень, визначених статтею 19 Закону України «Про критичну інфраструктуру».

Національним банком України забезпечено комплексний підхід до нормативно-правового врегулювання питань стосовно особливостей функціонування фінансового сектору, у тому числі, в умовах військової агресії ро-

сійської федерації, забезпечення кіберстійкості та протидії кіберзагрозам, безперервності функціонування фінансового сектору, управління ризиками, що знайшло своє відображення не лише у вище перелічених законах, а і низці нормативно-правових актів НБУ, тут слід згадати про такі постанови Правління Національного банку: від 27.09.2017 № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі» [9], від 11.06.2018 № 64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах» [10], від 12.08.2022 № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» [11] та інші.

Напрямок імплементації європейського законодавства у сфері забезпечення захисту критичної інфраструктури має високий рівень пріоритетності. На сьогоднішній день, законодавство України у цій сфері в значній мірі відповідає основним стандартам законодавства ЄС. Однак поряд з низкою позитивних змін існують деякі невирішені питання. Перш за все, необхідно передбачити впровадження європейського підходу до розуміння критично важливого суб'єкта та критичної інфраструктури.

Так, Директива 2022/2557 оперує поняттям критично важливого суб'єкту: а) суб'єкт господарювання надає одну або декілька основних послуг; б) суб'єкт господарювання здійснює діяльність і його критична інфраструктура розташована на території цієї держави-члена; і с) інцидент міг би мати значні руйнівні наслідки, як визначено відповідно до частини 1 статті 7, на надання суб'єктом господарювання однієї чи кількох основних послуг або надання інших основних послуг у секторах, викладених у Додатку, які залежать від тієї чи тих основних послуг (стаття 6). Тоді як критична інфраструктура – означає актив, об'єкт, обладнання, мережу чи систему або частину активу, об'єкта, обладнання, мережі чи системи, які необхідні для надання основних послуг (стаття 2(4)).

У той же час, у національному законодавстві врегульовується захист об'єктів критичної інфраструктури, на відміну від європейського законодавства, у якому акцент на стійкість критично важливих суб'єктів.

Наступне, це імплементація положень статті 8 Директиви (ЄС) 2022/2557 стосовно критичних суб'єктів у банківській справі та інфраструктурі фінансового ринку (пункт 3 та 4 таблиці у Додатку до Директиви (ЄС) 2022/2557).

Стаття 8 визначає, що Держави-члени повинні гарантувати, що стаття 11 та розділи III, IV та VI не застосовуються до критичних суб'єктів, які вони визначили у секторах, зазначених у пунктах 3 та 4 таблиці у Додатку. Держави-члени можуть приймати або зберігати положення національного законодавства для досягнення більш високого рівня стійкості для цих кри-

тичних суб'єктів, за умови, що ці положення відповідають чинному законодавству Союзу.

Отже, виходячи із положень цієї статті, мова йде про питання, присвячені співробітництву між державами-членами (стаття 11), стійкості критичних об’єктів (розділ 3), у тому числі оцінці ризиків критично важливих суб'єктів (стаття 12 розділу 3) та заходів щодо підвищення стійкості критичних об'єктів (стаття 13, розділ 3), а також стосовно критичних суб'єктів, що мають особливе європейське значення (розділ IV), а саме виявлення критичних суб'єктів, що мають особливе європейське значення (стаття 17) – ті, що надають ті ж чи аналогічні основні послуги шести або більше державам-членам, і нарешті стосовно питань організації перевірок компетентними органами критичної інфраструктури (розділ VI).

Водночас, стаття 9 цієї Директиви визначає, що кожна держава-член призначає або засновує один або більше компетентних органів, відповідальних за правильне застосування та, у разі необхідності, виконання правил, викладених у цій Директиві, на національному рівні. Що стосується критично важливих суб’єктів у секторах, зазначених у пунктах 3 та 4 таблиці у Додатку до цієї Директиви, компетентними органами, в принципі, є компетентні органи, зазначені у статті 46 Регламенту (ЄС) 2022/2554. Держави-члени можуть призначити інший компетентний орган для секторів, зазначених у пунктах 3 та 4 таблиці в Додатку до цієї Директиви відповідно до існуючих національних рамок.

Отже, виходячи із зазначеного, норм статей 8 та 9 Директиви (ЄС) 2022/2557 доцільно імплементувати в частині визначення регуляторів фінансового ринку України, як компетентних органів в розумінні європейського законодавства.

Висновки. Імплементація положень Регламенту (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) та узгодження з нормами Директиви (ЄС) 2022/2557 Європейського парламенту та Ради про стійкість критично важливих суб’єктів і скасування Директиви Ради 2008/114/ЕС дозволить забезпечити комплексний підхід до забезпечення захисту критичної інфраструктури фінансового сектору та створити ефективну вітчизняну систему моніторингу й оцінки, яка відповідає європейським традиціям у сфері захисту критичної інфраструктури, що в свою чергу, потребуватиме змін до Закону України «Про критичну інфраструктуру» та окремих кореспондуючих змін до таких законів, як: «Про основні засади забезпечення кібербезпеки України», «Про банки і банківську діяльність», «Про фінансові послуги та фінансові компанії», «Про Національний банк України».

Інформаційні джерела

1. Регламент (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) (онлайн) URL: http://surl.li/efowfn (дата звернення: 16 листопада 2024).

2. Директива (ЄС) 2022/2557 Європейського парламенту та Ради від 14 грудня 2022 року про стійкість критично важливих суб'єктів і скасування Директиви Ради 2008/114/ЕС (онлайн) URL: http://surl.li/rkfxey (дата звернення: 15 листопада 2024).

3. Про основні засади забезпечення кібербезпеки України: Закон України, 5 жовтня 2017 року, № 2163-VIII / Верховна Рада України (онлайн) URL: http://surl.li/ouqbyp (дата звернення: 15 листопада 2024).

4. Про критичну інфраструктуру: Закон України, 16 листопада 2021 року, № 1882-IX / Верховна Рада України (онлайн) URL: http://surl.li/daxfsm (дата звернення: 15 листопада 2024).

5. «Про захист інформації в інформаційно-комунікаційних системах»: Закон України, 5 липня 1994 року, № 80/94-ВР / Верховна Рада України (онлайн) URL: http://surl.li/jeioai (дата звернення: 16 листопада 2024).

6. «Про платіжні послуги»: Закон України, 30 червня 2021 року, № 1591-IX/ Верховна Рада України (онлайн) URL: http://surl.li/nhzsye (дата звернення: 15 листопада 2024).

7. «Про фінансові послуги та фінансові компанії» Закон України, 14 грудня 2021 року, № 1953-IX / Верховна Рада України (онлайн) URL: http://surl.li/yrieuc (дата звернення: 16 листопада 2024).

8. Указ Президента України Про рішення Ради національної безпеки і оборони України від 14 травня 2021 року "Про Стратегію кібербезпеки України" (онлайн) URL: http://surl.li/cbyycs (дата звернення: 15 листопада 2024).

9. Постанова Правління Національного банку України від 27.09.2017 № 95 «Про затвердження Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі» (онлайн) URL: http://surl.li/xyjkbp (дата звернення: 15 листопада 2024).

10. Постанова Правління Національного банку України від 11.06.2018 № 64 «Про затвердження Положення про організацію системи управління ризиками в банках України та банківських групах» (онлайн) URL: http://surl.li/xhfnpy (дата звернення: 15 листопада 2024).

11. Постанова Правління Національного банку України від 12.08.2022 № 178 «Про затвердження Положення про організацію кіберзахисту в банківській системі України та внесення змін до Положення про визначення об'єктів критичної інфраструктури в банківській системі України» (онлайн) URL: http://surl.li/tmlkke (дата звернення: 15 листопада 2024).