Міністерство освіти і науки України

Державний вищий навчальний заклад
«Донецький національний технічний університет»

Кафедра автоматики і телекомунікацій

Донецький науковий центр НАН України і МОН України

«ТАК»

Телекомунікації, автоматизація, комп'ютерно-інтегровані та інформаційні технології

Збірка доповідей Всеукраїнської науково-практичної конференції молодих учених
(Дрогобич, 12 грудня 2024 р.)

Дрогобич
ДВНЗ «ДонНТУ»
2024

УДК 621.39+681+004
Т 15

Т 15 **«ТАК»**: телекомунікації, автоматика, комп'ютерно-інтегровані технології: зб. доповідей Всеукр. наук.-практ. конф. молодих вчених, 12 грудня 2024 р. / ДВНЗ «ДонНТУ; відп. ред. Г.В. Ступак. – Дрогобич: ДВНЗ «ДонНТУ», 2024. – 215 с.

До збірника увійшли матеріали доповідей, представлених на Всеукраїнській науково-практичній конференції молодих учених «ТАК»: телекомунікації, автоматика, комп'ютерно-інтегровані технології. Конференція проводилася кафедрой автоматики та телекомунікацій (АТ) ДВНЗ «Донецький національний технічний університет».

У збірнику представлені результати досліджень та розробок молодих вчених із технічних вузів та наукових закладів України.

Збірник призначений для викладачів, аспірантів і студентів вищих технічних навчальних закладів, а також фахівців з телекомунікацій, автоматизації, інформаційних та комп'ютерно-інтегрованих технологій, електротехніки та електромеханіки.

УДК 621.39+681+004

КІБЕРБЕЗПЕКА ФІНАНСОВОГО СЕКТОРУ: ПОДАЛЬШІ ШЛЯХИ ЄВРОІНТЕГРАЦІЇ

Бердиченко І.О.[1] , кандидат юридичних наук, irinaberdychenko@gmail.com;
Дорогий Я.Ю.[2] , доктор технічних наук, доцент, yaroslav.dorohyi@donntu.edu.ua
[1] Чорноморський національний університет ім. Петра Могили, Миколаїв, Україна
[2] Донецький національний технічний університет, Дрогобич, Україна

Вступ

На сьогодні, Національний банк унормував питання організації і забезпечення кіберзахисту в банківській системі України та визначив основні засади функціонування системи кіберзахисту; принципи забезпечення інформаційного обміну між Центром кіберзахисту Національного банку і банками України; вимоги щодо заходів із забезпечення кіберзахисту об'єктів критичної інформаційної інфраструктури; вимоги щодо проведення незалежного аудиту інформаційної безпеки банків [1].

Шляхи імплементації законодавства ЄС

Національний банк України 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, операторами платіжних систем та/або учасниками платіжних систем, технологічними операторами платіжних послуг, здійснює контроль за їх виконанням, утворює центр кіберзахисту Національного банку, забезпечує функціонування системи кіберзахисту для банків, інших осіб, які здійснюють діяльність на ринках фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг [2]. Крім того, Національний банк України формує вимоги та забезпечує функціонування системи аудиту інформаційної безпеки на об'єктах критичної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, державне регулювання та нагляд за діяльністю яких здійснює Національний банк, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг, і також забезпечує формування та забезпечення функціонування реєстру об'єктів критичної інформаційної інфраструктури у банківській системі України та на ринках небанківських фінансових послуг, регулювання та нагляд

за діяльністю на яких здійснює Національний банк України, операторів платіжних систем та/або учасників платіжних систем, технологічних операторів платіжних послуг [3].

Участь в організації заходів щодо забезпечення кіберзахисту критичної інфраструктури банків здійснює Центр кіберзахисту Національного банку України. Також у банківській системі України функціонує команда реагування на кіберінциденти CSIRT-NBU Центру кіберзахисту Національного банку України, яка приєдналася до міжнародної робочої групи команд реагування на інциденти безпеки TF-CSIRT (Computer Security Incident Response Teams) та отримала статус «ACCREDITED», що є показником відповідності вимогам міжнародних стандартів у цій сфері та показником визнання з боку інших міжнародних команд CERT/CSIRT.

Отже, Національним банком України проведено широкомасштабну роботу для забезпечення цифрової стійкості банківської системи. Разом з тим, враховуючи євроінтеграційні процеси, що активно проводяться в державі, актуальним є питання імплементації положень Регламенту (ЄС) 2022/2554 Європейського парламенту та Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектора та про внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909 /2014 та (ЄС) 2016/1011 [4].

Як зазначено у статті 1 цього Регламенту, з метою досягнення високого загального рівня цифрової операційної стійкості цей Регламент встановлює єдині вимоги щодо безпеки мережевих та інформаційних систем, що підтримують бізнес-процеси фінансових організацій, а саме: вимоги до фінансових організацій щодо управління ризиками у сфері інформаційно-комунікаційних технологій (ІКТ); інформування про значні інциденти, пов'язані з ІКТ, та добровільне повідомлення компетентних органів про суттєві кіберзагрози; надання фінансовими організаціями, зазначеними у статті 2 (1), пунктах (a) – (d), компетентним органам інформації про значні операційні інциденти або інциденти, пов'язані з платежами щодо забезпечення безпеки; тестування сталості цифрових операцій; обмін інформацією та розвідданими щодо кіберзагроз та вразливостей; заходи щодо раціонального управління ризиками третіх осіб у сфері ІКТ; вимоги щодо договірних відносин, укладених між сторонніми постачальниками послуг ІКТ та фінансовими організаціями; правила створення та ведення системи нагляду за критично важливими сторонніми постачальниками послуг ІКТ під час надання послуг фінансовим організаціям; правила співробітництва між компетентними органами, а також правила нагляду та забезпечення дотримання з боку компетентних органів щодо всіх питань, що охоплюються цим Регламентом.

Відповідно до статті 2 цього Регламенту, його дія розповсюджується, серед іншого на такі фінансові установи, як кредитні та платіжні установи. Цей Регламент визначає цифрову операційну стійкість, як здатність фінан-

сової установи створювати, гарантувати та перевіряти свою операційну цілісність та надійність шляхом забезпечення, безпосередньо чи опосередковано, за допомогою використання послуг, що надаються сторонніми постачальниками послуг ІКТ, повного спектра можливостей, пов'язаних з ІКТ, необхідних для забезпечення безпеки мережі та інформаційних систем, які використовує фінансова установа, та які підтримують безперервне надання фінансових послуг та їх якість.

На сьогодні, низка положень цього Регламенту вже знайшла своє втілення в таких Законах нашої держави, як «Про основні засади забезпечення кібербезпеки України» [3], «Про платіжні послуги» [5], «Про критичну інфраструктуру» [6], іншому законодавстві.

Висновки

Враховуючи поточний стан національного законодавства доцільним є здійснення подальших кроків з імплементації положень Регламенту (ЄС) 2022/2554 Європейського парламенту та Ради від 14 грудня 2022 року про цифрову операційну стійкість фінансового сектора та про внесення змін до Регламентів (ЄС) № 1060/2009, (ЄС) № 648/2012, (ЄС) № 600/2014, (ЄС) № 909 /2014 та (ЄС) 2016/1011, стосовно:

- системи управління ризиками ІКТ;
- системи управління інцидентами, пов’язаними з ІКТ, класифікацією інцидентів;
- системи управління ризиками третіх сторін ІКТ;
- заходів впливу за порушення вимог законодавств;
- організації інформаційного обміну щодо таких подій.

Імплементація у національне законодавства вказаних положень Регламенту (ЄС) 2022/2554 дозволить значно підвищити ефективність цифрової операційної стійкості фінансового сектора, а саме банківських та платіжних установ, та створити ефективну вітчизняну систему моніторингу й оцінки, яка відповідає європейським традиціям у зазначеному напрямку функціонування фінансового сектору.

Література

1. Постанова Правління Національного банку України від 12 серпня 2022 року № 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" [Електронний ресурс]. – Режим доступу: https://bank.gov.ua/ua/legislation/Resolution_12082022_178 (дата звернення: 03.12.2024).
2. Про Національний банк України: Закон України від 20 травня 1999 року № 679-XIV / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/679-14 (дата звернення: 03.12.2024).
3. Про основні засади забезпечення кібербезпеки України: Закон України від 5 жовтня 2017 року № 2163-VIII / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/2163-19 (дата звернення: 15.11.2024).

4. Регламент (ЄС) 2022/2554 про цифрову операційну стійкість для фінансового сектору (DORA) [Електронний ресурс]. – Режим доступу: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32022R2554 (дата звернення: 16.11.2024).
5. Про платіжні послуги: Закон України від 30 червня 2021 року № 1591-IX / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1591-20#Text (дата звернення: 03.12.2024).
6. Про критичну інфраструктуру: Закон України від 16 листопада 2021 року № 1882-IX / Верховна Рада України [Електронний ресурс]. – Режим доступу: https://zakon.rada.gov.ua/laws/show/1882-20#Text (дата звернення: 03.12.2024).

Анотація

Діяльність Національного банку України у сфері європейської інтеграції націлена насамперед на імплементацію Угоди про асоціацію між Україною та ЄС, а також інших правових актів ЄС. Реалізація положень європейського законодавства підвищує ефективність ринку фінансових послуг, забезпечує наближення національних норм регулювання і нагляду до правил ЄС та міжнародних стандартів. Це також створює передумови для посилення конкурентоздатності та рівноправної співпраці українських фінансових установ з європейськими, сприяє підвищенню рівня надання фінансових послуг та захисту прав споживачів, і заходи у сфері кібербезпеки та кіберзахисту є невід'ємним елементом такої діяльності.

Ключові слова: кібербезпека, критичні інфраструктура, фінансовий сектор, регулятор, НБУ.

Abstract

The National Bank of Ukraine's activities in the field of European integration are primarily aimed at implementing the Association Agreement between Ukraine and the EU, as well as other EU legal acts. The implementation of European legislation enhances the efficiency of the financial services market, ensures the alignment of national regulatory and supervisory standards with EU rules and international standards. It also creates preconditions for strengthening the competitiveness and equitable cooperation of Ukrainian financial institutions with European counterparts, promotes the improvement of financial service delivery and consumer rights protection. Measures in the field of cybersecurity and cyber defense are an integral part of such activities.

Keywords: cybersecurity, critical infrastructure, financial sector, regulator, National Bank of Ukraine.