Інституційні механізми забезпечення кібербезпеки в Європейському Союзі

https://doi.org/10.31713/MCIT.2024.057

Оксана Кардаш
Національний університет водного господарства та природокористування
м. Рівне, Україна
o.l.kardash@nuwm.edu.ua

Любомир Гладун
Національний університет водного господарства та природокористування
м. Рівне, Україна
l.v.gladun@nuwm.edu.ua

Анотація **– Проведено дослідження інституційних та організаційно-правових механізмів забезпечення кібербезпеки в Європейському Союзі. Здійснено аналіз співпраці Європейського Союзі з Україною і сфері кібербезпеки. Виокремлено основні загрози кіберпростору ЄС та механізми їх подолання.**

Ключові слова **– кібербезпека, кіберзагрози, кіберзлочинність, кібератака, кіберпростір.**

I. Вступ

Сьогоденний прогрес цифрових технологій змінює економіку країн, а також світові тенденції та бізнес. Суспільство залежать від цифрових послуг, як і компанії та державні установи, які залежать від цифрових мереж та інфраструктур для виконання своїх основних завдань.

Саме через цю розгалужену мережу та зростаючу залежність від цифрових послуг зростає вразливість суспільства. Кібератаки та інциденти можуть мати величезний вплив на безпеку країн та їх економіку, порушуючи пропозиції послуг і порушуючи діяльність бізнесу та уряду.

II. Постановка задач

Підвищення цифрової стійкості країн та забезпечення кібербезпеки в цифровому світі в цілому мають велике значення як для процвітання європейських країн, так і для їх безпеки. Тому кібербезпека є одним із головних пріоритетів Європейського Союзу та центральним спільним викликом для держав, бізнесу, науки та суспільства.

Закон ЄС про кібербезпеку визначає ***кібербезпеку*** *як усі дії, необхідні для захисту мережевих та інформаційних систем, користувачів таких систем та інших осіб, які можуть постраждати від кіберзагроз* [1]. Європейський Союз працює на різних фронтах, щоб сприяти кіберстійкості, захистити власні комунікації та дані, а також забезпечити безпеку онлайн-суспільства та економіки.

Основними інституціями ЄС в сфері кібербезпеи є [1], [2]:

- ENISA – це агентство ЄС, яке займається кібербезпекою. Воно надає підтримку державам-членам, інституціям ЄС та підприємствам у ключових сферах.
- ISAC -центри обміну та аналізу інформації, які сприяють співпраці між спільнотою кібербезпеки в різних секторах економіки.
- JRC - спільний дослідницький центр, який активно сприяє кібербезпеці в ЄС. Він займається розробкою таксономії кібербезпеки, узгоджує термінологію, яка використовується в кібербезпеці, формує звіти про поточний ландшафт кібербезпеки ЄС та його історію.
- CSIRT - групи реагування на інциденти комп'ютерної безпеки Ці команди на практиці справляються з інцидентами та ризиками кібербезпеки. Вони співпрацюють один з одним на рівні ЄС, а також співпрацюють з приватним сектором. Усі типи операторів основних послуг і постачальників цифрових послуг мають бути охоплені призначеними CSIRT.

Основними завданнями CSIRT є:

- моніторинг інцидентів на національному рівні;
- надання раннього попередження, попереджень, оголошень та іншої інформації про ризики та інциденти відповідним зацікавленим сторонам;
- реагування на інциденти;
- забезпечення динамічного аналізу ризиків та інцидентів і ситуаційної обізнаності;

- ECSO - Європейська організація з кібербезпеки, яка здійснює діяльність, спрямовану на розбудову економіки та промисловий розвиток на європейському рівні. Більшість із 250 її членів належать або до галузі кібербезпеки, або до науково-дослідних та академічних установ в галузі.
- Women4Cyber – організація жінок ЄС, які працюють у сфері кібербезпеки.
- Платформа «Атлас кібербезпеки» (European Cybersecurity Atlas) - платформа управління знаннями для картографування, класифікації та стимулювання співпраці між європейськими експертами з кібербезпеки на підтримку цифрової стратегії ЄС.
- Європейський промисловий, технологічний і дослідницький центр компетенції в галузі кібербезпеки, який об'єднує досвід і узгоджує європейський розвиток і впровадження технологій кібербезпеки. Він співпрацює з промисловістю, академічним співтовариством та

іншими, щоб виробити спільну програму для інвестицій у кібербезпеку, а також визначити пріоритети фінансування досліджень,

III. Вирішення поставлених задачі

Основні механізми забезпечення кібербезпеки ЄС викладено в:

Стратегія кібербезпеки ЄС - яка має має на меті створити стійкість до кіберзагроз і забезпечити громадянам і підприємствам користь від надійних цифрових технологій. Стратегія зосереджена на розбудові колективних можливостей для реагування на великі кібератаки та співпрацює з партнерами по всьому світу для забезпечення міжнародної безпеки та стабільності в кіберпросторі. Стратегія містить конкретні пропозиції щодо застосування трьох основних інструментів: регуляторних, інвестиційних та політичних ініціатив. Вони стосуватимуться трьох сфер діяльності ЄС:

- стійкість, технологічний суверенітет і лідерство;

- оперативні можливості для запобігання, стримування та реагування;

- співробітництво для розвитку глобального та відкритого кіберпростору.

Нова стратегія кібербезпеки ЄС для Цифрового десятиліття є ключовим компонентом Формування цифрового майбутнього Європи, Плану відновлення Європи Комісії та Стратегії Союзу безпеки на 2020-2025 роки.

Директива NIS2 - директива про безпеку мережевих та інформаційних систем та заходи для високого загального рівня кібербезпеки в ЄС, яка координує діяльність урядових органів країн, обмін інформацією та здійснення спільних операцій. Директива імплементована 18.10. 2024 р.

Закон про захист від кібернетичного середовища (The Cyber Resilience Act) - нормативно-правовий акт щодо вимог до кібербезпеки для продуктів із цифровими елементами, який посилює правила кібербезпеки, щоб забезпечити більш безпечні апаратні та програмні продукти.

Закон про кіберсолідарність (Cyber Solidarity Act) - документ про кіберсолідарність, який включає Європейський щит кібербезпеки та комплексний механізм надзвичайних ситуацій у сфері кібернетичної безпеки для створення кращого методу кіберзахисту.

Система сертифікації ІТ-продуктів та послуг (EU-wide certification framework) - загальна схема сертифікації ІТ продуктів та послуг і відповідність їх стандартам кібербезпеки.

ЄС співпрацює з партнерами, щоб просувати спільні інтереси в політиці кібербезпеки. Дев'ятий Кібердіалог ЄС-США відбувся в Брюсселі в грудні 2023 року. ЄС і США просунулися у співпраці в таких сферах, як кібердипломатія, врегулювання криз, розбудова потенціалу, кібербезпека критичної інфраструктури (включно зі звітуванням про інциденти), кібербезпека апаратного забезпечення та програмні продукти (включаючи спільний план дій щодо кібербезпечних продуктів), а також аспекти кібербезпеки нових технологій, таких як ШІ [3].

З 2021 року ЄС та Україна провели два Кібердіалоги. У 2023 році Агентство ЄС з кібербезпеки ENISA офіційно уклало робочу домовленість з українськими партнерами для сприяння розбудові потенціалу, обміну найкращими практиками та обізнаності про ситуацію. ЄС також запровадив кібердіалоги з Індією, Японією, Республікою Корея та Бразилією. Перший кібердіалог між ЄС і Великобританією відбувся в Брюсселі в грудні 2023 року.

Висновки

Таким чином, процес становлення кіберзаконодавства в країнах-членах ЄС розпочався у 2001 році й досі набирає оберти, створюючи нове законодавство в цій галузі. Однак з позиції системного підходу більшість проблем кібербезпеки виникає через відставання сучасної законодавчої бази від науково-технічного прогресу. За декілька останніх десятиліть відбулася потужна технологічна революція в галузі використання комп'ютерів та телекомунікацій, яка привела до принципових змін та збільшення апаратного парку, суттєвого прискорення швидкості передачі інформації.

ЄС має очолити зусилля щодо безпечної цифровізації. Це має стати рушійною силою для рішень світового рівня та стандартів кібербезпеки для основних послуг і критичної інфраструктури, а також стимулювати розвиток і застосування нових технологій. Уряди, підприємства та громадяни розділять відповідальність за забезпечення кіберзахищеної цифрової трансформації.

Водночас саме стрімкий інформаційний прогрес спричинив проблему захищеності персональних даних через виникнення глобальних лідерів, що призвело до концентрації інформації в руках «великих гравців мережі» та централізації загальної інфраструктури. Це зробило можливими великомасштабні атаки та створило великі ризики значних збитків при критичних пошкодженнях інфраструктури таких систем.

Тому, незважаючи на існуючу сучасну низку документів щодо кібербезпеки, остання досі залишається досить вразливою, незалежно від ступеня розробки і стану законодавства, виявляючи випереджаючі проблемні науково-технічні прогалини щодо підвищення якості та стану кібербезпеки в ЄС загалом

Література

[1] EU cybersecurity initiatives working towards a more secure online environment / European Union [Електронний ресурс]. – Режим доступу : https://clck.ru/FEMKo.

[2] About ENISA / European Union Agency for Network and Information Security [Електронний ресурс]. – Режим доступу : https://www.enisa.europa.eu/about-enisa

[3] Proposal for a regulation of the European Parliament and of the Council on ENISA, the «EU Cybersecurity Agency», and repealing Regulation (EU) 526/2013, and on Information and Communication Technology cybersecurity certification («Cybersecurity Act»)