Савчук С.О.

АРХІТЕКТУРА КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Агентство Європейського Союзу з кібербезпеки – ENISA займає центральне місце в ініціативах ЄС щодо створення послідовної та ефективної структури кібербезпеки [4]. ENISA було засновано в 2004 році та розташовано в Греції. Повноваження Агентсва з часом значно розширилися, в першу чергу з прийняттям Закону про кібербезпеку 2019 року, який надає Агентству розширені права та обов'язки [6]. Як спеціалізована агенція, ENISA зосереджується на зміцненні потенціалу кібербезпеки в державах-членах, координації транскордонного реагування на кіберінциденти та розробці загальних стандартів і практик, які можуть бути прийняті в усьому Союзі.

Роль ENISA передбачає створення мереж співпраці між національними групами реагування на інциденти комп'ютерної безпеки, підтримку розробки та впровадження законодавства, першочергово Директива NIS та NIS2 [1,2], а також сприяння діалогу між державними та приватними заінтересованими сторонами. Координаційна функція поширюється на управління загальноєвропейськими навчаннями з кібербезпеки, розробленими для перевірки колективної готовності та механізмів реагування на інциденти кіберзагроз. Шляхом імітації великомасштабних кібератак ці навчання виявляють вразливі місця та операційні прогалини, які інакше могли б залишитися непоміченими, спонукаючи держави-члени вдосконалювати свої стратегії виявлення, пом'якшення та звітування про загрози.

Ключовою сферою впливу ENISA є створення та розповсюдження найкращих практик і технічної документації. Звіти Агенства про загрози, які публікуються щорічно, відстежують нові вектори атак і зловмисників, надаючи державам-членам, установам ЄС і приватним організаціям консолідований огляд середовища кібербезпеки [3]. Консолідовані оцінки базуються на даних про

інциденти, висновках експертів і транскордонному обміні розвідувальними даними, щоб висвітлити вразливі місця в критичній інфраструктурі, ланцюгах постачання і мережевих системах. Завдяки розвідувальній функції ENISA служить основоположним регулятором та координатором для національних органів влади, зменшуючи дублювання та фрагментацію в зусиллях зі збору інформації та забезпечуючи більш синхронізовану відповідь на нові кіберзагрози.

Запровадження загальноєвропейської системи сертифікації кібербезпеки відповідно до Закону про кібербезпеку ще більше зміцнило роль ENISA. Хоча схеми сертифікації залишаються добровільними в багатьох секторах, ENISA уповноважена розробляти та підтримувати такі схеми у співпраці з національними органами влади та представниками галузі. На практиці це передбачає скликання робочих груп і технічних груп, де експерти обговорюють базові вимоги безпеки для продуктів, процесів і послуг ІКТ. Мета полягає в тому, щоб після прийняття схеми сертифікації вона застосовувалася в усіх державах-членах без необхідності коригування на національному рівні. Ця модель співпраці з ENISA в центрі підкреслює ідею того, що відповідальність за кібербезпеку в контексті ЄС має бути розподілена між стейкхолдерами, від великих транснаціональних компаній до малих і середніх підприємств, а також між різними національними регуляторами.

Іншим аспектом координаційної функції ENISA є підтримка розробки політики протидії кіберзагрозам. Політики в Європейській комісії та Європейському парламенті часто покладаються на досвід ENISA для формулювання пропозицій, пов’язаних з кібербезпекою, наприклад, нові директиви чи оновлення існуючих правових інструментів. ENISA пропонує технічні оцінки та консультації з найсучасніших тем, зокрема безпеки штучного інтелекту, захисту інфраструктури 5G та управління ризиками в ланцюзі поставок. Дорадча роль Агентства впливає на забезпечення того, щоб політичні пропозиції відображали новітні технологічні реалії та щоб нормативні акти могли бути реально запроваджені як на рівні ЄС, так і на національному рівнях.

Незважаючи на розширені повноваження ENISA, Агентство стикається з певними проблемами щодо забезпечення узгодженого рівня зрілості кібербезпеки в державах-членах. Потенціал і ресурси, виділені на кібербезпеку, суттєво відрізняються між різними національними органами, і здатність ENISA формувати цей потенціал частково залежить від бажання держав-членів інвестувати у власні внутрішні системи та приймати рекомендації ENISA. Незважаючи на те, що з часом Агентство набуло більшої оперативної спрямованості, зокрема на координацію кіберінцидентів, воно все ще значною мірою покладається на співпрацю національних команд і організацій приватного сектора для виявлення, аналізу та реагування на загрози. Така система взаємодії призводить до складної багаторівневої динаміки управління, в якій вплив ENISA іноді обмежений різними правовими традиціями, стратегіями кібербезпеки та адміністративною практикою держав-членів.

ENISA продовжує залишатися ключовим суб'єктом державного управління у гармонізації стандартів і практики кібербезпеки в ЄС. Його стратегічне положення дозволяє подолати розриви між національними органами влади, сприяти передачі знань і послідовному застосуванню нормативних актів у різних секторах. Стимулюючи ініціативи з розбудови потенціалу, підтримуючи спільні оперативні дії та розвиваючи спільну культуру безпеки, Агентство допомогло розвинути спільну відповідальність за проблеми кібербезпеки, які виходять за межі національних кордонів. Завдяки цим спільним зусиллям ENISA підтримує ширшу мету підвищення колективної стійкості проти кіберзагроз, відображаючи визнання того, що фрагментований підхід до кібербезпеки зробить критичну інфраструктуру та цифрові послуги вразливими у все більш взаємозалежному Союзі.

Архітектура кібербезпеки Європейського Союзу спирається на тісно взаємопов'язану мережу інституцій, агентств і оперативних груп, які працюють у цивільних, урядових, військових і приватних сферах. На рисунку 3.1 показано, як екосистема прагне об'єднати стратегічний нагляд, оперативне співробітництво та

технічну експертизу в рамках спільної структури, що відображає імператив колективної стійкості у глобально взаємопов'язаному середовищі [5].

У центрі системи знаходиться Агентство Європейського Союзу з кібербезпеки, яке надає рекомендації, програми з розбудови потенціалу та технічну підтримку як державам-членам, так і органам Європейського Союзу. Роль ENISA виходить за рамки консультативних функцій і включає сприяння обміну інформацією та стимулювання гармонізації стандартів кібербезпеки. У співпраці з приватними підприємствами, державними адміністраціями та науковими установами ENISA сприяє впровадженню найкращих практик у сфері управління ризиками, реагування на інциденти та схем сертифікації. Завдяки цій взаємодії з багатьма заінтересованими сторонами Агентство підтримує більшу частину політично-орієнтованої структури ЄС, перетворюючи Директиви NIS/NIS2 та Закон про кібербезпеку у практичні заходи, які можуть бути прийняті як на національному, так і на галузевому рівнях.

Поряд з ENISA Європейська мережа організації зв'язку з кіберкриз (EU-CyCLONe) більш вузько зосереджується на оперативних аспектах кібербезпеки та врегулюванні криз, особливо під час масштабних або транскордонних кіберзагроз. Спираючись на підтримку галузевих центрів обміну та аналізу інформації (ISAC), EU-CyCLONe допомагає координувати відповіді стейкхолдерів, гарантуючи, що приватний сектор, державні органи та спеціалізовані агентства оперативно обмінюються розвідувальною інформацією про загрози та узгоджують свої зусилля зі стримування та пом'якшення. Секторальні ISAC представляють критичні точки взаємодії для таких галузей, як енергетика, фінанси чи транспорт, що дозволяє установам та організаціям у цих сферах обмінюватися спеціальними галузевими даними та найкращими практиками в режимі реального часу. EU-CyCLONe працює під егідою ENISA, але має власний окремий мандат на подолання розриву між політичними рамками та реагуванням на кризи, сприяючи комунікації між національними органами держав-членів, коли кіберінцидент досягає порогу, який ризикує каскадними ефектами через кордони.

Список використаної літератури:

1. Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union. URL: http://data.europa.eu/eli/dir/2016/1148/oj

2. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972. URL: http://data.europa.eu/eli/dir/2022/2555/2022-12-27

3. ENISA Threat Landscape 2024. ENISA. URL: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

4. ENISA. URL: https://www.enisa.europa.eu/.

5. Potentials and challenges for EU cybersecurity cooperation. Institutt for informatikk. Forside. Det matematisk-naturvitenskapelige fakultet. URL: https://www.mn.uio.no/ifi/studier/masteroppgaver/informasjonssikkerhet/potential-and-challenges-for-cybercooperation-in-e.html.

6. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act). URL: http://data.europa.eu/eli/reg/2019/881/oj