Медіафорум : аналітика, прогнози, інформаційний менеджмент : зб. наук. праць. – Чернівці : Чернівецький нац. ун-т, 2019. – Том 7. – С. 27-46

Mediarorum: Analytics, Forecasts, Information Management: Collection of Research Articles. – Chernivtsi: Chernivtsi National University, 2019. – Vol. 7. – pp. 27-46

https://doi.org/10.31861/mediaforum.2019.7.27-46
УДК: 341:004.738

© *Оксана Звоздецька*[1]

КІБЕРБЕЗПЕКА ЄС В УМОВАХ ПОСИЛЕННЯ КІБЕРЗАГРОЗ В СУЧАСНОМУ ГЛОБАЛІЗОВАНОМУ СВІТІ

Стаття присвячена аналізу сучасної політики кібербезпеки Європейському Союзі в умовах посилення кіберзагроз та кібератак в сучасному глобалізованому світі. Дослідниця констатує, що з 2013 р. Європейський Союз почав приділяти проблемам в сфері кіберзахисту все більше уваги. Про це свідчать ряд досліджень, які були проведені в рамках ЄС, а також прийняття важливих нормативно-правових документів, які регулюють дану проблему на внутрішньому ринку.

Окрім цього, ринок кібербезпеки ЄС, один з найбільш швидкозростаючих у секторі ІКТ, що створює величезні економічні можливості. Зміцнення індустрії кібербезпеки дозволить європейським компаніям скористатися цими можливостями та посилити довіру громадян і бізнесу в цифровому світі, сприяючи досягненню цілей стратегії єдиного цифрового ринку.

Стратегічними пріоритетами зміцнення кібербезпеки ЄС є: досягнення кіберстійкості, різке зменшення кіберзлочинності, спільна політика кібербезпеки та оборони, розробка промислових та технологічних ресурсів для забезпечення кібербезпеки, запровадження координаційних механізмів запобігання, виявлення, пом'якшення та реагування на кіберінциденти між національними компетентними органами в сфері мережевої та інформаційної безпеки, поліпшення взаємодії з приватним сектором для сприяння кібербезпеці.

Ключові слова: *Європейський Союз (ЄС), кіберзагрози, кібербезпека, критичні інфраструктури, мережева та інформаційна безпека, ENISA.*

[1] Кандидат історичних наук, доцент кафедри міжнародної інформації Чернівецького національного університету імені Юрія Федьковича, Україна, E-mail: o.zvozdecka@chnu.edu.ua; http://orcid.org/0000-0003-2623-7615

EU Cybersecurity in the Context of Increasing Cyberthreats in the Modern Globalized World

The article is an attempt to analyze the EU's ever-increasing cybersecurity challenges in today's globally digitalized world. The researcher remarks that since 2013 the European Union has been pursuing the policy of developing awareness of cyber-attacks targeting and beefing-up restrictive measures. The author underlines that the European Council has adopted the regulation known as the Cybersecurity Act to become more cyber-proof. This is evidenced by a number of studies carried out within the EU as well as that this legal regulation facilitated imposing targeted restrictive measures to deter and respond to cyber-attacks in EU and abroad.

Furthermore, the EU cybersecurity market is one of the fastest growing in the ICT sector, providing huge economic opportunities. Underpinning the cybersecurity industry will enable European companies to take advantage of these opportunities and increase citizens and businesses' confidence in the digital world, while significantly contributing to the goals of the EU Digital Single Market Strategy.

Broadly speaking, the problem can be addressed by such strategic priorities for enhancing EU cybersecurity as followed: achieving cyber resilience; dramatically reducing cybercrime; elaborating the common cybersecurity and defence policy; developing industrial and technological resources to ensure cybersecurity; establishing coordination mechanisms to prevent, detect, mitigate and respond to cyber bullying and information security as well as improving engagement with the private sector to enhance cybersecurity.

The ultimate goal of the above-mentioned EU strategy appeared to be a Public Private Partnership (cPPP) that was concluded on 5 July, 2016 between the European Commission and the European Cyber Security Organization (ECSO).

The objective of such partnership is to ensure awareness and resilience in an increasingly multifaceted cyber threat environment and to foster collaboration between public and private actors in the early stages of the research and innovation process to enable the EU Internet users to access secured innovative and credible European solutions (ICT products, services and software).

Keywords: *European Union (EU), cyber threats, cybersecurity, critical infrastructures, network and information security, ENISA.*

Постановка проблеми. Практично без винятку, прогнози майбутнього суспільства, економіки та індивідуального життя віддають перевагу цифровим технологіям та Інтернету, які стануть ще більш вбудованими в наше життя, ніж зараз. Ще десять років інвестицій, досліджень, розробок, інновацій і їх впровадження наблизять нас до світової, глобальної цифрової цивілізації, яка може принести позитивну користь для всіх (Bisson, Pascal (Thales), Fabio, Martinelli (CNR) and Raúl, Riesco Granadino (INCIBE), editors, 2015.). «Інтернет речей» вже є реальністю, і до 2020 р. в ЄС очікуються десятки мільярдів підключених цифрових пристроїв.

Однак крім суспільних благ нові технології тягнуть за собою ряд глобальних інформаційних загроз. Сьогодні економіка ЄС страждає від кіберзлочинців, які використовують все більш складні методи вторгнення в інформаційні системи, крадіжки критичних даних. Збільшення економічного шпигунства в кіберпросторі є новою категорією загроз для урядів та компаній ЄС. За оцінками, кібератаки щороку коштують світовій економіці € 400 млрд. (Reform of cybersecurity, 2019). На підставі метаогляду 17 існуючих досліджень, проведених між 2014 та 2015 роками, Європейське агентство з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security – ENISA), визначило, що вартість кібератак може коштувати країнам-членам ЄС приблизно 1,6% їх ВВП або 41,3 млрд. доларів щорічно для ЄС в цілому (Tom, Spring, 2016).

Зіткнувшись із постійно зростаючими викликами кібербезпеки, ЄС прагне підвищити рівень обізнаності щодо кібератак, спрямованих на держави-члени або інституції ЄС. Сьогоднішні системи ІКТ можуть серйозно постраждати від інцидентів безпеки, таких як технічні збої та віруси. Згідно з проведеним у 2017 р. PricewaterhouseCoopers[1] опитуванням, щонайменше 80 % європейських компаній засвідчили, принаймні, про один інцидент протягом останніх трьох років у сфері кібербезпеки (Д. Дубов, 2018, 23).

За даними Європейської Комісії, незважаючи на зростаючу загрозу, поінформованість, знання про кібербезпеку залишаються недостатніми:

- 51% європейських громадян не знають про кіберзагрози;

[1] PricewaterhouseCoopers – міжнародна мережа компаній, що пропонує професійні послуги у сфері консалтингу та аудиту..

- 69% компаній мають базове або взагалі не розуміють своє ставлення до кіберризиків (Reform of cybersecurity in Europe. Last reviewed on 08/01/2019).

Аналіз останніх досліджень та публікацій. З українських дослідників, що висвітлювали окремі аспекти даної проблеми, слід виокремити публікацію відділу інформаційної безпеки та розвитку інформаційного суспільства Національного інституту стратегічних досліджень під керівництвом доктора політичних наук Д.В. Дубова (Дубов, 2018). Аналітична доповідь присвячена питанням формування ефективного державно-приватного партнерства з питань кібербезпеки. В ній проаналізовано теоретичні підходи до державно-приватного партнерства та їх особливості у питаннях кібербезпекової сфери. Досліджено світовий досвід (США, ЄС, Німеччини, Великої Британії, Польщі) із розбудови довіри між державним та приватним сектором з питань безпеки кіберпростору.

Цікавими, на нашу думку, є дослідження українських науковців В.О. Бойко (В.Бойко, 2019) та А.В. Войціховського (А.Войціховський, 2018), в яких подається аналіз ініціативи ЄС щодо державно-приватного партнерства у сфері кібербезпеки, окреслено колізії, складнощі й точкові розбіжності інтересів різних учасників процесу та можливі варіанти співпраці, висвітлено діяльність ENISA.

Метою даної статті є аналіз сучасної політики ЄС в сфері кібербезпеки в умовах посилення кіберзагроз та кібератак в сучасному глобалізованому світі.

Виклад основного матеріалу. На сьогодні ЄС наголошує на важливості глобального, відкритого, вільного, стабільного та безпечного кіберпростору там, де права людини, основні свободи та верховенство права повністю застосовуються для соціального добробуту, економічного зростання, процвітання та цілісності вільного і демократичного суспільства (Council Conclusions, 2018).

Ринок кібербезпеки ЄС, один з найбільш швидкозростаючих ринків у секторі ІКТ, що створює величезні економічні можливості. Зміцнення індустрії кібербезпеки дозволить європейським компаніям скористатися цими можливостями та посилити довіру громадян і бізнесу в цифровому світі, сприяючи досягненню цілей стратегії єдиного цифрового ринку.

Європі потрібні якісні, доступні, сумісні продукти та рішення для кібербезпеки. Проте постачання продуктів та послуг безпеки ІКТ в

рамках єдиного ринку залишається дуже фрагментарним. З одного боку, це ускладнює конкуренцію європейським компаніям на національному, європейському та глобальному рівнях; з іншого, це зменшує вибір життєздатних і корисних технологій для захисту онлайн-діяльності громадян і підприємств.

Всі ці фактори пояснюють, чому уряди в усьому світі почали розробляти стратегії кібербезпеки і розглядати кіберпростір як одне з найважливіших міжнародних питань.

В 2013 р. ЄС також активізував свої дії в цій сфері і прийняв Стратегію ЄС з кібербезпеки «Відкритий, надійний та безпечний кіберпростір» (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace). Цей документ пропонує конкретні заходи, які можуть підвищити загальну ефективність євроспільноти в цій сфері. Стратегія дає наступне визначення поняттю «кібербезпека» – це захист інформаційних систем від потенційних людських помилок, природного лиха, технічних помилок або ж навмисних шкідливих атак (Cybersecurity Strategy, 2013). Бачення ЄС, представлене в цьому документі, сформульовано у п'яти стратегічних пріоритетах, які вирішують вищезгадані проблеми:

- досягнення кіберстійкості;
- різке зменшення кіберзлочинності;
- розвиток кібербезпечної політики та можливостей, пов'язаних із спільною політикою безпеки та оборони (CSDP);
- розробити промислові та технологічні ресурси для забезпечення кібербезпеки;
- здійснити послідовну міжнародну політику у сфері кіберпростору для Європейського Союзу та просувати основні цінності ЄС (Cybersecurity Strategy, 2013).

Ця стратегія супроводжується пропозицією щодо вдосконалення законодавства в сфері інформаційної безпеки, зокрема:

- встановити спільні мінімальні вимоги до мережевої та інформаційної безпеки (NIS) на національному рівні, які зобов'язують держави-члени призначати національні компетентні органи для мережевої та інформаційної безпеки NIS;
- створити добре функціонуючий CERT;
- прийняти національну стратегію «Мережевої та інформаційної безпеки» та національний план співробітництва в сфері мережевої та інформаційної безпеки.

- запровадити координаційні механізми запобігання, виявлення, пом'якшення та реагування, що дозволяють обмін інформацією та взаємодопомогу між національними компетентними органами NIS. Національним компетентним органам NIS буде запропоновано забезпечити відповідну співпрацю на рівні ЄС, зокрема на основі плану співробітництва NIS, розробленого для реагування на кіберінциденти з транскордонним виміром;
- покращити готовність та залучення приватного сектору. Оскільки переважна більшість мережних та інформаційних систем є приватною власністю, вирішальне значення має поліпшення взаємодії з приватним сектором для сприяння кібербезпеці. Приватний сектор повинен розвивати на технічному рівні власні кіберспроможності та співпрацювати з різними секторами.

Одразу після оприлюднення Стратегії кібербезпеки було розпочато роботу над відповідною директивою, яка розроблялася не окремо від інших напрямків, а в якості частини документу «Цифрова стратегія єдиного ринку для Європи» (Digital Single Market Strategy) 2015 р. (Communication from the Commission, 2015).

Директива «Про безпеку мережевих та інформаційних систем» (Network and Information Security Directive, Директива NIS) була прийнята парламентом ЄС ще 6 липня 2016 р. і набрала чинності в серпні 2016 р. (Директива Європейського Парламенту, 2016). Держави-члени повинні були до 9 травня 2018 р. імплементувати її у свої національні законодавства, та у внутрішні статутні документи основних підприємств до 9 листопада 2018 р. Директива, яка стала важливим кроком в Європейському Союзі щодо впровадження правових заходів для посилення кібербезпеки в ЄС, захисту цифрової економіки та суспільства від все більше негативних наслідків кібератак та інших кіберінцидентів. Метою цього документу є також сприяння співпраці між державами-членами в управлінні ризиками, пов'язаними зі зростаючою цифризацією.

Директива NIS застосовується до суб'єктів, що діють у галузях, які є життєво важливими для економіки та суспільства, і в значній мірі покладаються на ІТ-системи, такі як цифрова інфраструктура, постачальники фінансових послуг, енергетика, банківська справа, охорона здоров'я, транспорт та вода. Ці суб'єкти називаються операторами основних послуг (OES) і повинні були бути ідентифіковані окремими державами-членами до 9 листопада 2018 р.

Директива NIS також стосується постачальників цифрових послуг (DSP). DSP – це організація, яка надає хмарні послуги, а також послуги, такі як пошукові системи та ринки онлайн. Держави-члени ЄС повинні визначити критерії для виконання DSP; і саме DSP необхідно визначити, чи повинні вони дотримуватись цієї директиви (Директива Європейського Парламенту, 2016).

Директивою NIS вимагається, щоб установи приймали відповідні рішення та впроваджували заходи безпеки відповідно до ризиків кібербезпеки та можливих негативних наслідків для їхніх клієнтів та суспільства. Керівні принципи щодо політики та заходів у сфері кібербезпеки повинні здійснюватися Європейським агентством мережевої та інформаційної безпеки (ENISA) та Національними центрами кібербезпеки або національними компетентними органами. Регулятори можуть забезпечити розуміння впроваджених заходів безпеки, докази ефективності політики безпеки та результатів перевірок безпеки.

У документі також зазначено, що відповідальність за визначення штрафів за невідповідність покладається на окремі держави-члени, а ці штрафні санкції повинні бути «ефективними, пропорційними і переконливими» (Директива Європейського Парламенту, 2016).

Іншим аспектом Директиви про NIS є процедура інформування про інциденти. Відповідні інциденти, пов'язані з кібербезпекою, повинні повідомлятися відповідним національним органам. У більшості країн це буде Національний центр кібербезпеки (NCSC) або їх команда реагування на інциденти з комп'ютерної безпеки (CSIRT) та галузеві регулятори. Центр також оголошує про формування «групи зі співпраці», завдання якої – зміцнення довіри і обміну інформацією між країнами, обмін передовими методами і створення мережі національних груп комп'ютерної безпеки і реагування на інциденти (групи CSIRT) з метою поліпшення координованого реагування на інциденти (Хопфнер, 2016, 58).

Зростання взаємозв'язку критично важливою інфраструктури в цифровому середовищі і взаємозалежності інфраструктур європейських країн породив потребу в узгодженні цих двох секторів з метою зміцнення безпеки Європи і забезпечення її конкурентоспроможності. Нова Директива NIS має послужити важливою відправною точкою для розвитку гармонізованої програми захисту критично важливої інфраструктури ЄС (Хопфнер, 2016, 59).

Загальна ідея і уявлення про те, що таке критично важлива інфраструктура і як вона визначається, в більшості країн дуже схожі і зводяться до наступного: це інфраструктура, яка забезпечує безперебійне існування суспільства. Однак підходи різних країн розходяться у визначенні того, які саме елементи інфраструктури критично важливі.

З усіх 11 секторів Директива Ради ЄС 2008/114 / ЕС однозначно відносить лише енергетику і транспорт до «Критично важливої загальноєвропейської інфраструктури». Ця Директива є першим кроком поступового підходу до ідентифікації і визначення ЄКІ, а також оцінювання необхідності покращення їх охорони та захисту. Фактично, ця Директива робить основний акцент на енергетичному і транспортному секторах, та вимагає перегляду для оцінки її впливу і необхідності додати до сфери її застосування інші сектори, зокрема, і сектор інформаційно-комунікаційних технологій («ІКТ») (Директива Ради ЄС, 2008).

Згідно Директиви, «європейська критична інфраструктура» або «ЄКІ» означає критичну інфраструктуру, розташовану в державах-членах, пошкодження або знищення якої матиме істотний вплив щонайменше на дві держави-члени. Істотність впливу оцінюється за допомогою наскрізних критеріїв. Вони включають в себе наслідки міжсекторальних залежностей від інфраструктур інших типів (Директива Ради ЄС, 2008).

Створення іншої публічно-приватної платформи NIS було оголошено Стратегією кібербезпеки Європейського Союзу. Вона поділяла ту саму мету, що і Стратегія кібербезпеки та Директива NIS, тобто сприяти стійкості мереж та інформаційних систем, із надання послуг, що здійснюються операторами ринку та державними адміністраціями в Європі. На першому засіданні в червні 2013 р. для реалізації «Платформ NIS» було сформовано три окремі робочі групи:

- РГ1 щодо управління ризиками, включаючи забезпечення інформації, показники ризиків та підвищення обізнаності;
- РГ2 щодо обміну інформацією та координації інцидентів, включаючи повідомлення про випадки та показники ризиків з метою обміну інформацією;
- РГ3 щодо безпечних досліджень та інновацій в галузі ІКТ (Cybersecurity and Privacy, 2019, 37).

Платформа NIS, як пріоритетна, буде спрямована на визначення технологічно нейтральних найкращих практик, включаючи стандарти, для підвищення кібербезпеки та на розвиток стимулів, як з боку попиту, так і з боку пропозиції, дотримуватися цих кращих практик та приймати безпечні рішення ІКТ.

Результатом діяльності Платформи та Робочої групи 3 у третьому кварталі 2015 р. стала Програма стратегічних досліджень «Стратегічний порядок денний дослідження кібербезпеки» (Pascal, Martinelli and Riesco Granadino, 2015) на базі Платформи мережевої та інформаційної безпеки (European Cyber Security, 2016, 102). В цьому звіті європейський ринок кібербезпеки становить близько 25% (тобто близько 17 млрд. євро) світового ринку (оцінюється в 70 млрд. євро в 2015 р.), середній річний приріст трохи перевищує 6%, у той час, коли світовий ринок зростає приблизно на 8% (European Cyber Security, 2016). Це дослідження наголошувало на тому, що Європі загрожує відставання в галузі міжнародної цифрової економіки, тому необхідно терміново посилити зростання в секторі кібербезпеки / ІТ-безпеки. У документі також підкреслюється той факт, що Європа є найбільш надійною територією у світі, коли справа стосується забезпечення високого рівня безпеки даних та конфіденційності, і саме цю конкурентну перевагу потрібно підтримувати та розвивати. Щоби покращити ситуацію, необхідно розширити свої сильні сторони та подолати слабкі, скориставшись багатьма можливостями, які пропонує динамічний цифровий ринок (European Cyber Security, 2016).

З метою реалізації стратегії ЄС у сфері кібербезпеки та стратегії цифрового єдиного ринку Європейська Комісія у своєму повідомленні від 5 липня 2016 р. оголосила про укладення Державно-приватного партнерства з питань кібербезпеки (Public-Private Partnership (cPPP)) між Єврокомісією та Європейською організацією з кібербезпеки (European Cyber Security Organisation (ECSO).

Метою партнерства є сприяння співпраці між державними та приватними учасниками на ранніх етапах дослідницького та інноваційного процесу, щоб дозволити користувачам у Європі отримати доступ до інноваційних та надійних європейських рішень (продукти, послуги та програмне забезпечення ІКТ). Вона також має на меті стимулювати індустрію кібербезпеки, допомагаючи узгоджувати сектори попиту та пропозиції, щоб дозволити промисловості отримати майбутні потреби від кінцевих користувачів, а також секторів,

які є важливими клієнтами рішень у сфері кібербезпеки (наприклад, енергетика, охорона здоров'я, транспорт, фінанси) (Communication from the Commission, 2015).

Європейська організація з кібербезпеки (European Cyber Security Organisation – ECSO) є неприбутковою організацією зі штаб-квартирою в Брюсселі, яку було створеною у червні 2016 р. ECSO представляє галузеву контрактну співпрацю з Європейською Комісією для впровадження договірного державно-приватного партнерства з кібербезпеки (cPPP). Члени ECSO включають широкий спектр зацікавлених сторін, таких як великі компанії, малі, середні підприємства та стартапи, дослідницькі центри, університети, кінцеві користувачі, оператори, кластери та асоціації, а також місцеві, регіональні та національні адміністрації держав-членів Європи, країни, що входять до Європейської економічної зони (European Economic Area (EEA) and H2020 ЄЕЗ), Європейської асоціації вільної торгівлі (European Free Trade Association (EFTA)) та асоційовані країни програми «Горизонт 2020» (H2020) .

Основною метою ECSO є підтримка всіх видів ініціатив або проектів, спрямованих на розвиток, сприяння, заохочення європейської кібербезпеки, і зокрема:

- сприяти і захищати від кіберзагроз європейський цифровий ринок;
- співпрацювати з Європейською Комісією та національними державними адміністраціями для просування досліджень та інновацій у сфері кібербезпеки;
- запропонувати Стратегічну програму досліджень та інновацій (SRIA) та багаторічну дорожню карту з її регулярними оновленнями;
- сприяти підвищенню конкурентоспроможності та зростання індустрії кібербезпеки в Європі, а також кінцевих користувачів / операторів за допомогою інноваційних технологій, додатків, послуг, рішень у сфері кібербезпеки;
- підтримувати найширше та найкраще впровадження інноваційних технологій і послуг у сфері кібербезпеки для професійного та приватного використання.

Сфери інтересу:

- Інфраструктура ІКТ (включаючи хмарні технології, мобільні мережі, мережі тощо).

- Розумні мережі (енергія).
- Перевезення (у тому числі автомобільні / електричні транспортні засоби).
- Розумні будівлі та розумні міста.
- Промислові системи керування (промисловість 4.0).
- Державне управління та Відкритий уряд.
- Охорона здоров'я.
- Фінанси та страхування (European Cybersecurity Organisation (ECSO). Statutes).

13 вересня 2017 р. Європейська комісія представила документ «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» (Joint Communication, 2017), в якому ЄК та Верховний представник запропонували широкий спектр конкретних заходів, які сприятимуть подальшому зміцненню структур і можливостей кібербезпеки ЄС за допомогою ширшого співробітництва між державами-членами та різними зацікавленими структурами ЄС. Ці заходи забезпечать кращу підготовку ЄС до вирішення завдань, що постають у сфері кібербезпеки.

Голова Єврокомісії Жан-Клод Юнкер 13 вересня 2017 р. зазначив, що «кібератаки можуть бути більш небезпечними для стабільності демократій і економік, ніж зброя і танки. […] Кібератаки не знають кордонів і ніхто не застрахований. Саме тому сьогодні Комісія пропонує нові інструменти, включаючи Європейське агентство з кібербезпеки, щоб допомогти захистити нас від таких нападів» (Resilience, Deterrence and Defence, 2017).

Пропонує нові ініціативи для подальшого поліпшення кіберстійкості та реагування ЄС у трьох ключових сферах:

• розбудова стійкості ЄС до кібератак і посилення спроможності ЄС щодо кібербезпеки;

• створення ефективної кримінально-правової відповідальності;

• посилення глобальної стабільності через міжнародне співробітництво.

Для посилення стійкості, стримування та реагування ЄС на кібернапади пропонують:

• створення сильнішого агентства з питань кібербезпеки Європейського Союзу, на основі Агентства мережевої та інформаційної безпеки (ENISA), для надання допомоги державам-членам у боротьбі з кібератаками;

• створення загальноєвропейської схеми сертифікації кібербезпеки, яка збільшить кібербезпеку продуктів і послуг в цифровому світі;

• створення платформи навчання та освіти в сфері кіберзахисту (Resilience, Deterrence and Defence, 2017).

Наступним кроком у зміцненні кібербезпеки ЄС стало схвалення 19 грудня 2018 р. закону «Про кібербезпеку», що дасть змогу запровадити сертифікацію в сфері кібербезпеки в усьому ЄС, а також призведе до створення постійного агентства ЄС з кібербезпеки. Закон набув чинності 27 червня 2019 р. Це перший закон, який спрямований на регулювання внутрішнього ринку ЄС, підвищення безпеки онлайн-послуг і користувачів пристроїв шляхом створення загальноєвропейської системи сертифікації продуктів, послуг та процесів ІКТ (REGULATION (EU), 2019).

На даний час в ЄС існує низка різних схем сертифікації безпеки для продуктів ІКТ. Без єдиних рамок для діючих схем сертифікатів кібербезпеки, що є загальносоюзними, існує ризик фрагментації та бар'єрів на єдиному ринку.

«У цифровому середовищі люди і компанії повинні відчувати себе в безпеці. Для них це єдиний спосіб в повній мірі скористатися перевагами цифрової економіки Європи. Довіра і безпека мають основоположне значення для правильної роботи нашого єдиного цифрового ринку», – заявив заступник голови Єврокомісії по цифрового ринку Андрюс Ансіп (У ЄС дійшли згоди щодо закону про кібербезпеку, 2018).

Загальноєвропейська система сертифікації створює вичерпний набір правил, технічних вимог, стандартів та процедур узгодження кожної схеми. Кожна схема базуватиметься на домовленості на рівні ЄС щодо оцінки властивостей безпеки конкретного продукту чи послуги на основі ІКТ. Цей сертифікат засвідчує, що продукти та послуги ІКТ, які були сертифіковані відповідно до такої схеми, відповідають визначеним вимогам кібербезпеки. Отриманий сертифікат буде визнаний у всіх державах-членах ЄС, що полегшує підприємствам торгувати, а покупцям зрозуміти особливості безпеки товару чи послуги. Використання схем сертифікації буде добровільним, якщо майбутнє законодавство ЄС не встановить сертифікат ЄС як обов'язкову вимогу для задоволення конкретної потреби в кібербезпеці. Однак Європейська Комісія оцінить можливу потребу в обов'язковій сертифікації певних категорій товарів і послуг (EU Cybersecurity Act).

Новий закон вимагатиме від фірм, що здійснюють «основні» послуги, включаючи водні, енергетичні, транспортні, медичні та банківські операції, інформування національних органів влади, якщо вони постраждали від серйозних порушень кібербезпеки. Постачальники послуг хмарних обчислень, пошукові системи та онлайн-ринки також повинні повідомляти про ці інциденти.

Компаніям будуть пред'явлені штрафи, якщо вони не будуть повідомляти про порушення. Поки що лише уряд Великобританії оголосив про рівень своїх штрафів відповідно до закону – до 17 мільйонів фунтів стерлінгів або 19 мільйонів євро. Представник Єврокомісії заявив тоді, що Брюссель очікує, що інші країни запровадять аналогічно високі санкції (First EU cybersecurity law, 2018), що дозволить «поліпшити підтримку держав-членів у протидії загрозам кібербезпеки і кібератак».

Закон також модернізує нинішнє агентство ЄС з питань мережевої та інформаційної безпеки (EU agency for Network and Information Security (ENISA), і надає йому постійний мандат, більше ресурсів та нові завдання. Для того, щоби виконати свій новий мандат, ресурси агентства були подвоєні, збільшившись з 11 до 23 мільйонів євро протягом п'яти років, а кількість працівників збільшиться з 84 до 125 (EU Cybersecurity Act).

Європейське агентство з питань мережевої та інформаційної безпеки (European Union Agency for Network and Information Security – ENISA), як заявлено на його офіційному сайті, «було створено з метою підвищення здатності Європейського союзу, країн-членів ЄС та ділової спільноти запобігати проблемам мережевої та інформаційної безпеки, усувати їх і реагувати на них», є незалежною організацією в рамках Європейського Співтовариства. ENISA – єдине з агентств ЄС, якому було визначено конкретний термін завершення його дії – 2020 р. Агентство функціонує з 1 вересня 2005 р., штаб-квартира знаходиться в м. Іракліон, Крит, (Греція).

ENISA фактично розглядається як «вузол обміну інформацією, передовими методами і знаннями в галузі інформаційної безпеки» і не має реальної керівної влади, за винятком консультування Ради ЄС. Не існує центрального відомства, що має можливість координувати політику і впливати на неї з метою захисту критично важливої інфраструктури. В якості незалежного агентства ENISA визнає проблему зростаючої конвергенції між системами промислового контр-

олю, ІТ та їх функціональними елементами. У зв'язку з цим агентство виробило ряд рекомендацій та принципів для пом'якшення цієї проблеми на технічному і практичному рівнях.

Зокрема, ENISA матиме ключову роль у створенні та підтримці європейської системи сертифікації кібербезпеки, підготувавши технічну базу для конкретних схем сертифікації та інформуючи громадськість про схеми сертифікації, а також видані сертифікати через спеціалізований веб-сайт. ENISA також має повноваження розширювати оперативне співробітництво на рівні ЄС , допомагаючи державам-членам ЄС, які вимагатимуть допомоги, вирішувати їх кіберінциденти, та підтримує координацію ЄС у разі масштабних транскордонних кібератак та криз.

Уповноважений з питань цифрової економіки та суспільства Марія Габріель додала: «Закон про кібербезпеку ЄС продемонстрував необхідність підходу ЄС до реагування на всі виклики, захисту наших громадян та збереження конкурентоспроможності. Для досягнення цієї мети Європа надала постійний мандат Агентству ЄС з питань кібербезпеки» (The EU Cybersecurity Act, 2019).

Крім того, ENISA сприятиме розширенню можливостей кібербезпеки на рівні ЄС та підтримці розбудови потенціалу та готовності. Нарешті, ENISA буде незалежним експертним центром, який сприятиме підвищенню рівня обізнаності громадян та бізнесу, а також допоможе інституціям та державам-членам ЄС у розробці та впровадженні політики.

І наостанок, для посилення кібербезпеки у військовому секторі дев'ять країн-членів Євросоюзу дійшли згоди про створення кібернетичних сил швидкого реагування. Про це повідомив Раймундас Каробліс, міністр оборони Литви – країни, яка була ініціатором такого об'єднання.

25 червня 2018 р. шість країн ЄС підписали Декларацію про наміри щодо створення «Сил швидкого реагування в кіберпросторі ЄС» («EU Cyber Rapid Response Force»). «Мета - створити кібернетичні команди швидкого реагування, ротація яких буде проводитися кожне півріччя», - пояснив Раймундас Каробліс. Ще чотири країни – Бельгія, Греція, Словенія та Німеччина - приєднаються до проекту на правах спостерігачів.

За словами литовського міністра оборони, команди кібернетичних сил швидкого реагування могли б приходити на допомогу держа-

вам-членам Євросоюзу у разі серйозних кібернетичних інцидентів. Буде розглянуто можливість використовувати для цього проекту кошти бюджету ЄС на придбання комп'ютерної техніки і програмного обладнання («Дев'ять країн ЄС створюють кібернетичні «війська», 2018).

Це один із 17 проектів, схвалених державами-членами ЄС наприкінці 2017 р. в рамках так званого «Постійного структурованого співробітництва» (PESCO). PESCO - це абсолютно нова, обов'язкова рамкова програма ЄС для тіснішої співпраці у сфері безпеки та оборони. Кожен такий проект має провідну- країну та різні групи держав-членів ЄС. У цьому випадку шість держав-членів ЄС - Естонія, Хорватія, Румунія, Литва, Іспанія та Нідерланди – об'єдналися для створення кібернетичних сил.

Для тестування та підготовки нової структури передбачається, що восени 2018 р. перші бригади ЄС з питань кіберреагування візьмуть участь у навчанні з кібербезпеки в Литві.

Згідно з даними Литовського національного центру кібербезпеки, кількість кіберінцидентів зростає щороку на одну десяту, в той час як кіберрозслідування виявляють їх зростаючу складність. Сталися серйозні інциденти в критичній енергетичній інфраструктурі, а також IT-системах правоохоронних органів та закордонних справ. Такі інциденти потребують особливо швидкого реагування та нового типу готовності та інструментів (New tool, 2018).

Отже, стратегічними пріоритетами зміцнення кібербезпеки ЄС є: досягнення кіберстійкості, різке зменшення кіберзлочинності, спільна політика кібербезпеки та оборони, розробка промислових та технологічних ресурсів для забезпечення кібербезпеки, запровадження координаційних механізмів запобігання, виявлення, пом'якшення та реагування на кіберінциденти між національними компетентними органами в сфері мережевої та інформаційної безпеки, поліпшення взаємодії з приватним сектором.

Запроваджено сертифікацію в сфері кібербезпеки в усьому ЄС з метою підвищення безпеки онлайн-послуг і користувачів пристроїв шляхом створення загальноєвропейської системи сертифікації продуктів, послуг та процесів ІКТ. Фірми, що надають «основні» послуги, включаючи водні, енергетичні, транспортні, медичні та банківські операції, повинні інформувати національні органи влади, якщо вони постраждали від серйозних порушень кібербезпеки.

Джерела та література:

1. Директива Європейського Парламенту І Ради (ЄС). 2016. «Про заходи для високого спільного рівня безпеки мережевих та інформаційних систем на території Союзу» 2016/1148 від 6 липня. Офіційний вісник Європейського Союзу. 19.07.2016. https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-20161148.pdf

2. Директива Ради ЄС. 2008. «Про ідентифікацію і визначення європейських критичних інфраструктур та оцінювання необхідності покращення їх охорони та захисту» 2008/114/ від 8 грудня. Офіційний вісник Європейського Союзу. https://zakon.rada.gov.ua/laws/show/984_002-08.

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2015. A Digital Single Market Strategy for Europe 6.5.2015 COM(2015) 192 final. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN.

4. Bisson, Pascal (Thales), Fabio, Martinelli (CNR) and Raúl, Riesco Granadino (INCIBE), editors. 2015. Cybersecurity Strategic Research Agenda – SRA Produced by the European Network and Information Security (NIS) Platform Final version v0.96 Last modified: August 2015. https://www.dcypher.nl/sites/default/files/.../NCSRA-III_0.pd.

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. Brussels. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

6. European Cyber Security Strategic Research & Innovation Agenda for a contractual Public-Pravate Rartnership (cPPP). ECSO. 2016. https://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

7. Cybersecurity and Privacy landscape in Europe. 2017 – 2019, 60 p. http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Cybersecurity-and-Privacy-landscape-in-Europe.pdf

8. European Cybersecurity Organisation (ECSO). Statutes. http://ecs-org.eu/documents/ecso-asbl-statutes.pdf

9. Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 13.9.2017. Brussels, JOIN(2017) 450 final https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

10. Council Conclusions on malicious cyber activities. 2018 16 April (OR. en) 7925/18 CYBER 62 COPS 90 JAI 310 COPEN 97 DROIPEN 50

RELEX 313. Brussels. https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf

11. 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) https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

12. «Дев'ять країн ЄС створюють кібернетичні «війська». 2018. Новое время. 22 червня 2018. https://nv.ua/ukr/world/geopolitics/devjat-krajin-jes-stvorjujut-kibernetichni-vijska-2478015.html

13. «У ЄС дійшли згоди щодо закону про кібербезпеку». 2018. День 11 грудня. https://day.kyiv.ua/uk/news/111218-u-yes-diyshly-zgody-shchodo-zakonu-pro-kiberbezpeku

14. Андрій, Войціховський. 2018. «Кібербезпека як важлива складова системи захисту національної безпеки європейських країн». Журнал східноєвропейського права. 53: 26-37. http://easternlaw.com.ua/wp-content/uploads/2018/07/voytsikhovskyy_53.pdf

15. Бенедикт, Хопфнер. 2016. «Как защитить критически важные объекты инфраструктуры в Европе». per Concordiam 4(7): 58-63. http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V7N4_ru.pdf

16. Вікторія, Бойко. 2019. «Європейський досвід державно-приватного партнерства у сфері кібербезпеки: підходи до формування нормативно-правових засад». Стратегічні пріоритети 1: 28-36. http://nbuv.gov.ua/UJRN/

17. Дмитро, Дубов, заг. ред. 2018. Державно-приватне партнерство у сфері кібербезпеки: міжнародний досвід та можливості для України : аналіт. доп. К. : НІСД, 2018. https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

18. «EU Cybersecurity Act - ENISA and the cybersecurity certification framework» Digital Single Market. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-enisa-and-cybersecurity-certification-framework

19. «Resilience, Deterrence and Defence: Building strong cybersecurity in Europe». 2017. Cybersecurity. STATE OF THE UNION. https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

20. European Union Agency for Network and Information Security - ENISA. https://www.enisa.europa.eu/

21. First EU cybersecurity law takes effect—with new fines for misbehaving companies 2018. https://www.euractiv.com/section/cybersecurity/news/first-eu-cybersecurity-law-brings-fines-for-companies-that-fail-to-report-hacks

22. New tool to address cyber threats: the EU's Rapid Response Force. 27/06/2018. About the European External Action Service (EEAS). https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

23. Reform of cybersecurity in Europe. Last reviewed on 08/01/2019. https://www.consilium.europa.eu/en/policies/cyber-security/

24. The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification 26 June 2019. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

25. Tom, Spring. 2016. EU Struggles to Determine Growing Cost of Cyberattacks. https://threatpost.com/eu-struggles-to-determine-growing-cost-of-cyberattacks/119870/

References:

1. Dyrektyva Yevropeiskoho Parlamentu I Rady (IeS). 2016. «Pro zakhody dlia vysokoho spilnoho rivnia bezpeky merezhevykh ta informatsiinykh system na terytorii Soiuzu» 2016/1148 vid 6 lypnia. Ofitsiinyi visnyk Yevropeiskoho Soiuzu.19.07.2016. https://www.kmu.gov.ua/storage/app/media/uploaded-files/es-20161148.pdf

2. Dyrektyva Rady YeS. 2008. «Pro identyfikatsiiu i vyznachennia yevropeiskykh krytychnykh infrastruktur ta otsiniuvannia neobkhidnosti pokrashchennia yikh okhorony ta zakhystu» 2008/114/ vid 8 hrudnia. Ofitsiinyi visnyk Yevropeiskoho Soiuzu. https://zakon.rada.gov.ua/laws/show/984_002-08

3. Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. 2015. A Digital Single Market Strategy for Europe 6.5.2015 COM(2015) 192 final. Brussels. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52015DC0192&from=EN

4. Bisson, Pascal (Thales), Fabio, Martinelli (CNR) and Raúl, Riesco Granadino (INCIBE), editors. 2015. Cybersecurity Strategic Research

Agenda – SRA Produced by the European Network and Information Security (NIS) Platform Final version v0.96 Last modified: August 2015. https://www.dcypher.nl/sites/default/files/.../NCSRA-III_0.pd

5. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. 7.2.2013. Brussels. https://eeas.europa.eu/archives/docs/policies/eu-cyber-security/cybsec_comm_en.pdf

6. European Cyber Security Strategic Research & Innovation Agenda for a contractual Public-Pravate Rartnership (cPPP). ECSO. 2016. https://www.ecs-org.eu/documents/ecs-cppp-sria.pdf

7. Cybersecurity and Privacy landscape in Europe. 2017 – 2019, 60 p. http://aegis-project.org/wp-content/uploads/2019/01/AEGIS-Cybersecurity-and-Privacy-landscape-in-Europe.pdf

8. European Cybersecurity Organisation (ECSO). Statutes. http://ecs-org.eu/documents/ecso-asbl-statutes.pdf

9. Joint Communication to the European Parliament and the Council. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU. 13.9.2017. Brussels, JOIN(2017) 450 final. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52017JC0450&from=en

10. Council Conclusions on malicious cyber activities. 2018 16 April (OR. en) 7925/18 CYBER 62 COPS 90 JAI 310 COPEN 97 DROIPEN 50 RELEX 313 . Brussels. https://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en/pdf

11. 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). https://eur-lex.europa.eu/legalcontent/EN/TXT/HTML/?uri=CELEX:32019R0881&from=EN

12. «Deviat krain YeS stvoriuiut kibernetychni «viiska». 2018. Novoe vremia. 22 chervnia 2018. https://nv.ua/ukr/world/geopolitics/devjat-krajin-jes-stvorjujut-kibernetichni-vijska-2478015.html

13. «U YeS diishly zghody shchodo zakonu pro kiberbezpeku». 2018. Den 11 hrudnia. https://day.kyiv.ua/uk/news/111218-u-yes-diyshly-zgody-shchodo-zakonu-pro-kiberbezpeku

14. Andrii, Voitsikhovskyi. 2018. «Kiberbezpeka yak vazhlyva skladova systemy zakhystu natsionalnoi bezpeky yevropeiskykh krain». Zhurnal skhidnoievropeiskoho prava. 53: 26-37. http://easternlaw.com.ua/wp-content/uploads/2018/07/voytsikhovskyy_53.pdf

15. Benedikt, Khopfner. 2016. «Kak zashchitit kriticheski vazhnye obekty infrastruktury v Yevrope». per Concordiam 4(7): 58-63. http://www.marshallcenter.org/mcpublicweb/mcdocs/files/College/F_Publications/perConcordiam/pC_V7N4_ru.pdf

16. Viktoriia, Boiko. 2019. «Ievropeiskyi dosvid derzhavno-pryvatnoho partnerstva u sferi kiberbezpeky: pidkhody do formuvannia normatyvno-pravovykh zasad». Stratehichni priorytety 1: 28-36. http://nbuv.gov.ua/UJRN/

17. Dmytro, Dubov, zag. red. 2018. Derzhavno-pryvatne partnerstvo u sferi kiberbezpeky: mizhnarodnyj dosvid ta mozhlyvosti dlya Ukrayiny : analit. dop. K. : NISD, 2018. https://niss.gov.ua/sites/default/files/2019-05/Dopovid_Derzhavn-pryvatn_partnerstvo_Ciberbezpeka.pdf

18. «EU Cybersecurity Act - ENISA and the cybersecurity certification framework» Digital Single Market https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-enisa-and-cybersecurity-certification-framework

19. «Resilience, Deterrence and Defence: Building strong cybersecurity in Europe». 2017. Cybersecurity. STATE OF THE UNION. https://www.consilium.europa.eu/media/21480/cybersecurityfactsheet.pdf

20. European Union Agency for Network and Information Security - ENISA. https://www.enisa.europa.eu/

21. First EU cybersecurity law takes effect—with new fines for misbehaving companies 2018. https://www.euractiv.com/section/cybersecurity/news/first-eu-cybersecurity-law-brings-fines-for-companies-that-fail-to-report-hacks

22. New tool to address cyber threats: the EU's Rapid Response Force. 27/06/2018. About the European External Action Service (EEAS). https://eeas.europa.eu/topics/eu-international-cyberspace-policy/47525/new-tool-address-cyber-threats-eus-rapid-response-force_en

23. Reform of cybersecurity in Europe. Last reviewed on 08/01/2019. https://www.consilium.europa.eu/en/policies/cyber-security/

24. The EU Cybersecurity Act brings a strong agency for cybersecurity and EU-wide rules on cybersecurity certification 26 June 2019. https://ec.europa.eu/digital-single-market/en/news/eu-cybersecurity-act-brings-strong-agency-cybersecurity-and-eu-wide-rules-cybersecurity

25. Tom, Spring. 2016. EU Struggles to Determine Growing Cost of Cyberattacks. https://threatpost.com/eu-struggles-to-determine-growing-cost-of-cyberattacks/119870/