УДК 061.1ЄС
DOI: 10.31733/15-03-2024/2/308-310

Андрій ВОЙЦІХОВСЬКИЙ
професор кафедри конституційного
і міжнародного права факультету № 4,
кандидат юридичних наук, доцент

Владислав БЕРНАЦЬКИЙ
курсант факультету № 4
Харківського національного
університету внутрішніх справ

ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ В ЄВРОПЕЙСЬКОМУ СОЮЗІ

У зв'язку зі швидкими темпами розвитку інформаційно-комунікаційних технологій в країнах-членах ЄС, значну увагу у діяльності Євросоюзу набуває проблема забезпечення регіональної інформаційної безпеки.

У 2001 році Європейська комісія оприлюднила перший документ під назвою «Мережева та інформаційна безпека: європейський політичний підхід», в якому висвітлювався європейський погляд на проблему інформаційної безпеки. Документ визначав, що інформаційна безпека стає важливим елементом розвитку інформаційного суспільства. Мережі та інформаційні системи містять конфіденційну та економічно цінну інформацію, що збільшує зацікавленість до вчинення різного роду атак у цифровому просторі [1].

Згідно з рішенням Європейського парламенту та Ради ЄС № 460/2004 від 4 березня 2004 року було утворено Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) [2]. Метою ENISA є покращення рівня інформаційної безпеки в Європейському Союзі, сприяючи розвитку усвідомлення про мережеву та інформаційну безпеку серед громадян, підприємств та громадських організацій. Агентство працює на користь споживачів та підприємств, сприяючи безперебійному функціонуванню внутрішнього ринку ЄС. Водночас воно виступає як центр експертних послуг, надаючи консультації країнам-членам та інституціям ЄС з питань мережевої та інформаційної безпеки.

ENISA здійснює тісну співпрацю з Європейським поліцейським офісом (Європол), Європейським центром боротьби з кіберзлочинністю та іншими спеціалізованими установами Європейського Союзу.

У своїй діяльності Агентство ENISA оперує щорічними робочими планами і програмами, в яких визначаються основні стратегічні пріоритети. Ці пріоритети включають підвищення стійкості європейських інформаційних мереж до зовнішніх загроз, розвиток співпраці між країнами-членами ЄС у сфері мережевої та інформаційної безпеки, а також виявлення нових ризиків у цій сфері та підвищення взаємного довір'я.

Розташовується Європейське агентство з питань мережевої та інформаційної безпеки (ENISA) – м. Іракліон (Греція) [3, с. 513– 514].

Для поліпшення співпраці між судовими, правоохоронними та іншими владними органами у сфері захисту інформаційних систем у 2005 році Рада ЄС ухвалила Рамкове рішення 2005/222/JHA щодо нападу на інформаційні системи [4]. Цей документ встановив мінімальні стандарти для визначення кримінальних злочинів та санкцій, пов'язаних із нападами на інформаційні системи. Рамкове рішення відображає занепокоєння країн-членів ЄС стосовно можливості терористичних атак на інформаційні системи, які є важливою частиною інфраструктури та потребують спеціального захисту.

У 2007 році Європейською комісією представлено документ «На шляху до загальної політики в сфері боротьби з кіберзлочинністю» [5], який надає визначення терміну «кіберзлочинність» та містить основні напрями політики ЄС у протидії цьому явищу. Відповідно до цього документа, кіберзлочинність означає кримінальні дії, які здійснюються за допомогою електронних комунікаційних мереж та інформаційних систем або проти них.

Політика Європейської комісії щодо забезпечення інформаційної безпеки

реалізується у наступних напрямах: активної участі у формуванні законодавства (створення та прийняття нормативно-правових актів у цій галузі), сприяння міжнародному співробітництву правоохоронних органів країн-членів ЄС (організація науково-практичних заходів, конференцій, семінарів, тренінгів тощо), розвитку взаємодії між державним і приватним секторами в сфері інформаційної безпеки, включаючи співпрацю між правоохоронними органами та приватними підприємствами, заохочення підписання країнами-членами ЄС та іншими країнами Конвенції про кіберзлочинність 2001 року [6] тощо.

У 2009 році було опубліковано Повідомлення Європейської комісії під назвою «Захист Європи від широкомасштабних кібератак та руйнувань: посилення рівня підготовленості, безпеки та стійкості» [7], в якому сформульовані головні проблеми, які потребують негайної уваги ЄС, а також передбачені основні заходи для підвищення безпеки та стійкості критичної інформаційної інфраструктури країн-членів Євросоюзу перед зовнішніми загрозами.

Основні виклики в галузі безпеки інформаційної інфраструктури ЄС включають відсутність координації національних підходів до безпеки, яка знижує ефективність національних заходів, відсутність партнерства між державним та приватним секторами на європейському рівні, обмежені можливості ЄС у ранньому виявленні та реагуванні на безпекові інциденти та відсутність міжнародного консенсусу щодо пріоритетів у політиці захисту критичної інформаційної інфраструктури.

У 2013 році Європейська комісія затвердила Стратегію кібербезпеки «Відкритий, надійний та безпечний кіберпростір» [8], яка визначила загальну перспективу ЄС щодо протидії загрозам в інформаційному просторі. Заходи, передбачені у цій стратегії, спрямовані на посилення стійкості інформаційних систем до кібератак, зменшення кількості кіберзлочинів та зміцнення міжнародної політики ЄС з питань інформаційної безпеки.

Невдовзі після опублікування Стратегії кібербезпеки розпочалася робота з розробки Директиви ЄС «Щодо заходів забезпечення високого рівня безпеки мережевих та інформаційних систем у всьому Союзі», яка була прийнята у 2016 році [9]. Документ встановлює єдині правила та вимоги для забезпечення підвищеного рівня безпеки мереж та інформаційних систем у ЄС.

У 2017 році Європейська комісія оприлюднила документ «Стійкість, стримування та захист: створення сильної кібербезпеки для ЄС» [10], у якому було відзначено, що безпека інформації є критично важливою для економічного процвітання та безпеки країн-членів ЄС. Недотримання заходів щодо забезпечення інформаційної безпеки може призвести до збільшення ризику кіберзагроз, оскільки цифрові перетворення можуть посилити цей ризик. Небезпека політично мотивованих атак на цивільні об’єкти та недоліки у військовому кіберзахисті додатково підвищують загальний ризик. Для забезпечення значної кіберстійкості необхідний колективний та всебічний підхід.

Фактором, що заслуговує на увагу, є те, що в Європейському Союзі протягом наступних років очікується збільшення обсягів накопиченої інформації, надання електронних послуг та підключення до мереж більше мільярда пристроїв. Це не лише приносить переваги, але й призводить до зростання кількості, обсягу та різноманітності кіберзагроз. Ураховуючи цей контекст і розуміючи сутність цих загроз, у 2017 році Європейська комісія висунула пропозицію щодо нової архітектури інформаційної безпеки в ЄС та необхідності відповідного правового забезпечення.

Для досягнення цієї мети Європейська комісія пропонує впровадити нові інструменти, серед яких створення Європейського агентства з кібербезпеки (EAC) та Європейського центру досліджень кібербезпеки (ECRCC). Ці заходи призначені допомогти країнам-членам ЄС захистити свої інформаційні системи від кібернападів.

Європейське агентство з кібербезпеки (EAC) планують створити на базі існуючого Європейського агентства з питань мережевої та інформаційної безпеки (ENISA). Нове агентство буде мати постійний мандат та зможе надавати ефективну допомогу країнам-членам ЄС у відповіді на загрози в інформаційному просторі. Це сприятиме підвищенню готовності Євросоюзу реагувати на подібні виклики через організацію річних європейських тренувань та поліпшення обміну інформацією шляхом створення центрів обміну інформацією та аналізу.

Агентство EAC буде сприяти впровадженню єдиного європейського стандарту сертифікації. Ці нові європейські сертифікати з інформаційної безпеки гарантують надійність мільярдів пристроїв, які мають важливе значення для сучасної критичної

інфраструктури, такої як енергетичні та транспортні мережі.

За принципом партнерства між державними та приватними суб'єктами, Європейська комісія висуває ідею створення Мережі з інформаційної безпеки разом з Європейським центром досліджень кібербезпеки (ECRCC). Ця ініціатива передбачає надання підтримки у розробці та впровадженні інструментів та технологій, необхідних для протидії чимраз більшим загрозам у сфері інформаційної безпеки. Мережа буде допомагати збільшити потенціал у цьому напрямі як на рівні Європейського Союзу, так і на національному рівні країн-членів.

Для посилення глобальної інформаційної безпеки Європейський Союз активно здійснює розвиток міжнародного співробітництва з іншими державами. ЄС вже практикує співпрацю з країнами, такими як США, Японія, Індія, Південна Корея, Китай тощо. Крім того, здійснюються тісні консультації з міжнародними організаціями, такими як Організація Північноатлантичного договору (НАТО), Асоціація держав Південно-Східної Азії (АСЕАН), Організація з безпеки і співробітництва в Європі (ОБСЄ), Рада Європи (РЄ), Організація економічного співробітництва і розвитку (ОЕСР) тощо [3, с. 516].

Загальна концепція інформаційної безпеки стає все більш актуальною в контексті швидкого розвитку технологій та зростання залежності суспільства від цифрових ресурсів. У Європейському Союзі, як і в інших регіонах світу, проблема забезпечення інформаційної безпеки стає передумовою для стабільного розвитку економіки, політики та суспільства загалом. Це вимагає систематичного аналізу, розробки та впровадження стратегій, політик та технологій, спрямованих на запобігання кіберзагрозам, захисту конфіденційності, цілісності та доступності інформації. Лише шляхом спільних зусиль уряду, приватного сектору та громадськості Європейський Союз може забезпечити ефективний захист інформаційного простору та зберегти високий рівень довіри громадян та партнерів.

1. Network and Information Security: Proposal for A European Policy Approach : Communication COM (2001) 298 from the Commission to the Council, the European Parliament, the European Economic and Social Committee and the Committee of the Regions of 06 June 2001 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52001DC0298 (дата звернення : 28.02.2024).
2. European Network and Information Security Agency : Regulation (EC) № 460/2004 of the European Parliament and of the Council of 10 March 2004 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32004R0460 (дата звернення : 28.02.2024).
3. Міжнародне право : підручник / А. В. Войціховський ; МВС України, Харків. нац. ун-т внутр. справ. Харків, 2020. 544 с.
4. Attacks against information systems : Council Framework Decision 2005/222/JHA of 24 February 2005 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32005F0222 (дата звернення : 28.02.2024).
5. Towards a general policy on the fight against cyber crime : Communication COM (2007) 267 from the Commission to the European Parliament, the Council and the Committee of the Regions of 22 May 2007 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52007DC0267 (дата звернення : 28.02.2024).
6. Конвенція про кіберзлочинність : міжнародний документ, схвалений Радою Європи від 23.11.2001 // База даних «Законодавство України» / Верховна Рада України. URL : https://zakon.rada.gov.ua/laws/show/994_575 (дата звернення : 28.02.2024).
7. Protecting Europe from large scale cyber-attacks and disruptions: enhancing preparedness, security and resilience : Communication COM (2009) 149 from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions on Critical Information Infrastructure Protection of 30 March 2009 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149 (дата звернення : 28.02.2024).
8. Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace : Joint Communication (2013) 1 to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions of 07 February 2013 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52013JC0001 (дата звернення : 28.02.2024).
9. Concerning measures for a high common level of security of network and information systems across the Union : Communication from the Commission to the European Parliament and the Council Making the most of NIS – towards the effective implementation of Directive (EU) 2016/1148 of 04 October 2017 / EUR-Lex. Access to European Union Law. URL : https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0476 (дата звернення : 28.02.2024).
10. Resilience, Deterrence and Defence: Building strong cybersecurity for the EU : Joint Communication (2017) 450 to the European Parliament and the Council of 13 September 2017 URL : https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX%3A52017JC0450 (дата звернення : 28.02.2024).