

ЦЕНТРАЛІЗАЦІЯ КІБЕРБЕЗПЕКОВИХ ФУНКЦІЙ У ЄВРОПЕЙСЬКОМУ СОЮЗІ: РОЛЬ ENISA В НОВІЙ АРХІТЕКТУРІ УПРАВЛІННЯ КІБЕРРИЗИКАМИ

ПЕТРОВСЬКИЙ Сергій Станіславович - аспірант кафедри міжнародного та європейського права факультету права та міжнародних відносин Національного університету «Київський авіаційний інститут»

ORCID ID: 0009-0001-8993-1092

УДК 341.176:004.056

DOI: <https://doi.org/10.71404/EP.2026.1.34>

У статті здійснено комплексний інституційно-правовий аналіз процесу централізації кібербезпекових функцій у Європейському Союзі крізь призму трансформації мандата та ролі Агентства Європейського Союзу з кібербезпеки (ENISA). Досліджено еволюцію правового статусу Агентства від консультативно-аналітичного органу до суб'єкта з розширеними координаційними та квазі-операційними повноваженнями в межах нової архітектури управління кіберризиками ЄС. Обґрунтовано, що прийняття Регламенту (ЄС) 2019/881 (Cybersecurity Act), а також подальший розвиток нормативної бази, зокрема Директиви (ЄС) 2022/2555 (NIS2), стали визначальними чинниками інституційної модернізації ENISA та посилення її ролі у формуванні інтегрованої моделі колективної кіберстійкості.

У роботі проаналізовано ключові напрями діяльності Агентства, зокрема формування та підтримання Європейської системи сертифікації кібербезпеки для інформаційно-комунікаційних продуктів і послуг, розвиток механізмів оперативної співпраці держав-членів у межах CSIRTs Network та EU-CyCLONe, участь у процедурах кризового реагування в межах IPCR, а також виконання стратегічно-аналітичних функцій, пов'язаних із підготовкою дворічної доповіді про стан кібербезпеки в Союзі та розробленням інструментів оцінювання кіберзрілості, зокрема EU Cybersecurity Index. Визначено, що ENISA дедалі більше виступає інституційним центром координації, інформаційного обміну та вироблення спільних стандартів у сфері кібербез-

пеки. Окрему увагу приділено впливу сучасних геополітичних викликів, насамперед повномасштабної збройної агресії Російської Федерації проти України та супутніх гібридних і кібероперацій, на трансформацію підходів Європейського Союзу до забезпечення цифрової стійкості.

У висновках сформульовано тезу про те, що інституційна еволюція ENISA відображає ширшу тенденцію до поглиблення інтеграції та наднаціоналізації кібербезпекової політики Європейського Союзу, в межах якої національні компетенції держав-членів поєднуються з централізованими механізмами стратегічного моніторингу, кризового управління та регуляторної уніфікації.

Ключові слова: Європейський Союз; ENISA; кібербезпека; кіберстійкість; Cybersecurity Act; NIS2; безпека, кіберкриза.

Постановка проблеми

Стрімка цифровізація суспільних відносин, критична залежність держав і економік від інформаційно-комунікаційної інфраструктури, а також ускладнення характеру кіберзагроз обумовлюють необхідність формування ефективної та стійкої системи забезпечення кібербезпеки в межах Європейського Союзу. Особливої гостроти ця проблема набула в умовах повномасштабної збройної агресії Російської Федерації проти України, яка супроводжується масштабними та системними кібератаками, спрямованими як проти України, так і проти держав-членів ЄС, їхніх критичних інфраструктур,

урядових мереж та стратегічних секторів економіки.

Російська агресія продемонструвала, що кіберпростір став невід'ємним компонентом сучасних воєнних дій і гібридних операцій, у межах яких кіберінструменти використовуються для дестабілізації державних інституцій, підризу довіри до публічної влади, впливу на енергетичні, фінансові та транспортні системи, а також для здійснення інформаційно-психологічного тиску. Вказані обставини засвідчили вразливість як окремих держав, так і інтегрованого цифрового простору Європейського Союзу, що актуалізує потребу в посиленні наднаціональної координації та розбудові спільної архітектури кіберстійкості.

У цьому контексті прийняття Акта ЄС про кібербезпеку та подальший розвиток нормативної бази, зокрема в межах Директиви (ЄС) 2022/2555 (NIS2), відображають прагнення Європейського Союзу перейти від фрагментарної координації до більш інтегрованої моделі управління кіберризиками. Істотне розширення повноважень European Union Agency for Cybersecurity свідчить про посилення ролі наднаціональних інституцій у забезпеченні оперативного реагування, кризового управління та стратегічного моніторингу у сфері кібербезпеки [9].

Водночас у науковій площині залишається відкритим питання щодо характеру цієї трансформації: чи є вона лише інструментом удосконалення координаційних механізмів між державами-членами, чи свідчить про поступове формування централізованої моделі колективної кіберстійкості з розширенням наднаціонального впливу. З огляду на зростаючі транснаціональні загрози, зокрема пов'язані з агресивною кібердіяльністю Російської Федерації, дослідження інституційної еволюції ENISA та її ролі у формуванні європейської моделі безпеки набуває особливої актуальності.

Таким чином, проблематика дослідження полягає у необхідності комплексного осмислення впливу сучасних геополітичних викликів на трансформацію системи забезпечення кібербезпеки Європейського Союзу та визначення місця ENISA в процесі формування інтегрованого механізму про-

тидії кіберзагрозам у воєнних і гібридних умовах.

Аналіз останніх досліджень і публікацій

Сучасні дослідження у сфері кібербезпеки Європейського Союзу зосереджені на розвитку нормативної архітектури, зокрема після ухвалення Акта ЄС про кібербезпеку та Директиви (ЄС) 2022/2555 (NIS2), а також на трансформації інституційного механізму управління кіберризиками. У наукових працях аналізуються питання гармонізації вимог до суб'єктів критичних секторів, запровадження європейської системи сертифікації та удосконалення процедур координації під час транскордонних кіберінцидентів. Окрему увагу приділено інституційній ролі European Union Agency for Cybersecurity у формуванні стандартів, забезпеченні ситуаційної обізнаності та координації оперативних спільнот. Водночас у науковому дискурсі триває обговорення правової природи розширення її повноважень та меж наднаціоналізації кібербезпекових функцій.

З огляду на зростання гібридних загроз і кібероперацій у контексті агресії Російської Федерації проти України, дослідження дедалі більше акцентують на необхідності посилення колективної кіберстійкості ЄС. Проте комплексний аналіз інституційної еволюції ENISA у взаємозв'язку з тенденцією до централізації кібербезпекового управління залишається недостатньо розробленим, що зумовлює актуальність даного дослідження.

Отже, **метою цієї статті** є комплексний аналіз інституційно-правового статусу та функціональної трансформації European Union Agency for Cybersecurity в контексті розвитку нормативної архітектури кібербезпеки Європейського Союзу, а також визначення її ролі у формуванні інтегрованої моделі колективної кіберстійкості ЄС.

Методологічну основу статті становить комплекс загальнонаукових і спеціально-юридичних методів пізнання, застосованих з метою всебічного дослідження інституційно-правового статусу та функціональної еволюції European Union Agency for Cybersecurity у системі забезпечення кібербезпеки Євро-

пейського Союзу. У процесі дослідження використано формально-юридичний метод для аналізу положень Акта ЄС про кібербезпеку, Директиви (ЄС) 2022/2555 (NIS2) та інших нормативно-правових актів ЄС, що визначають мандат і повноваження Агентства. Системно-структурний метод застосовано для з'ясування місця ENISA в інституційній архітектурі ЄС та взаємозв'язку її функцій із механізмами координації, реагування на кіберінциденти та стратегічного моніторингу. Функціональний підхід дозволив дослідити трансформацію ролі Агентства від консультативно-аналітичного органу до суб'єкта з розширеними координаційними та квазі-операційними повноваженнями. Порівняльно-правовий метод використано для оцінки розвитку нормативної моделі кібербезпеки ЄС у динаміці та виявлення тенденцій до централізації відповідних функцій на наднаціональному рівні. Крім того, елементи інституційного та доктринального аналізу застосовано з метою визначення впливу посилення мандата ENISA на формування інтегрованої моделі колективної кіберстійкості Європейського Союзу.

Виклад основного матеріалу

European Union Agency for Cybersecurity (Агентство Європейського Союзу з кібербезпеки, надалі також – Агентство або ENISA) є спеціалізованою інституцією Європейського Союзу, діяльність якої спрямована на формування та забезпечення високого спільного рівня кібербезпеки на всій території ЄС. Засноване у 2004 році та суттєво посилене після ухвалення Акта ЄС про кібербезпеку, European Union Agency for Cybersecurity відіграє ключову роль у реалізації європейської кіберполітики.

Так, Агентство сприяє підвищенню надійності та безпечності інформаційно-комунікаційних продуктів, послуг і процесів шляхом розроблення та впровадження європейських схем сертифікації у сфері кібербезпеки, забезпечує інституційну взаємодію з державами-членами та органами ЄС, а також бере участь у підготовці Союзу до майбутніх кіберзагроз.

Завдяки системному обміну знаннями, розвитку інституційної спроможності та під-

вищенню рівня обізнаності Агентство у тісній співпраці з ключовими заінтересованими сторонами зміцнює довіру до цифрової та взаємопов'язаної економіки, підвищує стійкість критичної інфраструктури Європейського Союзу і в ширшому вимірі сприяє забезпеченню цифрової безпеки європейського суспільства та його громадян [10].

Аналізуючи нормативне регулювання діяльності Агентства, слід зазначити таке. Акт Європейського Союзу про кібербезпеку закріпив якісно нову модель інституційного та нормативного забезпечення кібербезпеки в межах Союзу, істотно посиливши статус і повноваження European Union Agency for Cybersecurity та запровадивши загальноєвропейську систему сертифікації у сфері кібербезпеки для інформаційно-комунікаційних продуктів і послуг. У результаті його ухвалення Агентству надано постійний мандат, розширено ресурсне забезпечення та визначено нові функціональні завдання, що трансформувало ENISA у центральний координаційний орган кібербезпекової політики ЄС.

У межах оновленого мандата Агентство уповноважене на формування та підтримання Європейської системи сертифікації кібербезпеки, зокрема шляхом підготовки технічних і процедурних передумов для розроблення спеціалізованих сертифікаційних схем. Окремим елементом цього мандата є забезпечення публічної доступності інформації щодо чинних схем сертифікації та виданих сертифікатів, що сприяє підвищенню рівня правової визначеності й довіри на внутрішньому ринку Союзу.

Водночас Акт про кібербезпеку істотно розширив повноваження ENISA у сфері оперативної співпраці, закріпивши її роль у підтримці держав-членів під час реагування на кіберінциденти за їх запитом, а також у координації дій Союзу у випадку масштабних транскордонних кібератак або кризових ситуацій. Ці функції логічно випливають із ролі Агентства як секретаріату мережі національних груп реагування на комп'ютерні інциденти (CSIRTs), створеної відповідно до Директиви про безпеку мережевих та інформаційних систем, і спрямовані на посилення узгодженості дій на рівні ЄС [8].

Подальший розвиток цього інституційного підходу відображено у пропозиції Європейської комісії щодо перегляду Акта про кібербезпеку, внесеної у січні 2026 року, яка має на меті зміцнення загальної кіберстійкості та операційних спроможностей Союзу. У межах запропонованих змін передбачається розширення підтримувальної ролі ENISA щодо суб'єктів господарювання та інших заінтересованих сторін, зокрема через запровадження механізмів раннього попередження про кіберзагрози та інциденти. У взаємодії з Europol та мережами CSIRTs Агентство також залучається до підтримки реагування на атаки із застосуванням програм-вимагачів і процесів відновлення після них.

Окремим напрямом діяльності ENISA визначено формування спільної для Європейського Союзу спроможності з управління вразливими елементами системи, включно з наданням відповідних послуг заінтересованим суб'єктам та функціонуванням єдиного пункту подання повідомлень про інциденти, передбаченого ініціативами цифрового регулювання Союзу. У такий спосіб інституційно-правова модель забезпечення кібербезпеки доповнюється елементами централізованої координації та інформаційного обміну.

Переглянутий Акт про кібербезпеку також спрямований на мінімізацію ризиків у ланцюгах постачання інформаційно-комунікаційних технологій, пов'язаних із залученням постачальників із третіх держав, щодо яких існують обґрунтовані застереження у сфері кібербезпеки. З цією метою формується система безпеки ланцюгу постачання інформаційно-комунікаційних технологій, що базується на гармонізованому, пропорційному та ризик-орієнтованому підході, з урахуванням критичної залежності основних послуг та інфраструктур від стабільності таких ланцюгів.

У сфері сертифікації Акт закріпив єдину для Союзу систему сертифікації кібербезпеки інформаційно-комунікаційних продуктів, послуг і процесів, яка забезпечує взаємне визнання сертифікатів на всій території Європейського Союзу та зменшує регуляторне навантаження на суб'єктів господарювання. Запропоновані зміни до Акта мають на меті подальше спрощення та уніфікацію проце-

дур розроблення сертифікаційних схем із чітко визначеними часовими межами [6].

Крім того, у 2023–2025 роках було ухвалено цільові зміни до Акта ЄС про кібербезпеку, спрямовані на створення правових підстав для майбутнього запровадження європейських схем сертифікації керованих послуг безпеки, зокрема у сферах реагування на інциденти, тестування на проникнення, аудитів і консалтингу. Такі зміни відображають прагнення законодавця забезпечити високий рівень якості та надійності послуг, що мають критичне значення для запобігання, виявлення та подолання кіберінцидентів.

Паралельно із цим запропоновані у 2026 році точкові зміни до Директиви NIS2 спрямовані на підвищення правової визначеності та спрощення виконання вимог у сфері кібербезпеки й управління ризиками для суб'єктів, що здійснюють діяльність у межах Європейського Союзу, з особливим урахуванням пропорційності регуляторного навантаження для малих і мікропідприємств.

Варто також зауважити, що одним із ключових завдань Агентства Європейського Союзу з кібербезпеки є забезпечення реагування ЄС на кіберінциденти та управління кіберкризами на наднаціональному рівні.

У межах реалізації цього завдання European Union Agency for Cybersecurity здійснює практичну та безпосередню взаємодію з державами-членами Європейського Союзу, Європейською комісією та іншими агенціями ЄС з метою як запобігання кіберінцидентам, так і забезпечення ефективного реагування на них у разі їх виникнення. У межах свого політико-правового мандата Агентство протягом кількох років послідовно формує та підтримує європейську систему управління кіберінцидентами і кризовими ситуаціями.

Зокрема, діяльність ENISA у цій сфері охоплює забезпечення щоденного функціонування мережі національних груп реагування на комп'ютерні інциденти (CSIRTs Network) та мережі ЄС з організації реагування на масштабні кіберкризи (EU-CyCLONe), проведення кризових симуляційних навчань і спеціалізованих тренінгів, надання підтримки державам-членам у розробленні національних планів і структур управління кіберкризами, а також організацію міжнарод-

них конференцій і підготовку аналітичних досліджень [10].

Як активний учасник скоординованого реагування Європейського Союзу на кіберінциденти та кризові ситуації у сфері кібербезпеки, ENISA надає інституційну підтримку Союзу у разі необхідності, зокрема в межах Механізму інтегрованого політичного реагування на кризи (IPCR). У тісній співпраці з державами-членами Агентство сприяє розробленню процедур управління кіберкризами на рівні ЄС, спрямованих на підвищення ситуаційної обізнаності у випадку транскордонних кіберінцидентів [1].

Крім того, ENISA виконує допоміжну аналітичну та консультативну функцію, підтримуючи як національні, так і європейські органи ухвалення рішень у виборі найбільш доцільних і пропорційних заходів реагування в умовах кіберкриз, що підсилює узгодженість і ефективність дій Європейського Союзу в цій сфері.

Зокрема, European Union Agency for Cybersecurity забезпечує управління кіберкризами на рівні Європейського Союзу через реалізацію комплексу взаємопов'язаних функцій, що формують інституційну основу скоординованого реагування.

Агентство забезпечує операційну спроможність мережі CSIRTs ЄС — Мережі команд реагування на комп'ютерні інциденти держав-членів Європейського Союзу (від англ. Computer Security Incident Response Teams Network) та мережі EU-CyCLONe — Європейська мережа організацій зв'язку у сфері кіберкриз (від англ. European Cyber Crisis Liaison Organisation Network), виконуючи функції секретаріату, надаючи організаційну підтримку, ресурси та спеціалізовану експертизу. Це дозволяє підтримувати безперервну координацію між національними органами реагування та структурами Союзу у сфері кібербезпеки [7].

Важливим елементом мандата ENISA є створення та підтримання захищеної інформаційно-технічної інфраструктури й інструментів, які забезпечують безпечний і оперативний обмін інформацією про кіберінциденти та актуальні загрози між заінтересованими сторонами, насамперед у межах CSIRTs Network та EU-CyCLONe. Така інфраструк-

тура є ключовою передумовою ефективного реагування на динамічні кіберзагрози.

Агентство також бере участь у розробленні та впровадженні операційних процедур, спрямованих на підготовку до масштабних транскордонних кіберінцидентів і кризових ситуацій та реагування на них на рівні Європейського Союзу [5]. Ці процедури забезпечують узгодженість дій держав-членів і інституцій ЄС в умовах підвищеної кіберзагрози.

Окремим напрямом діяльності ENISA є підготовка та проведення спеціалізованих навчань і симуляційних вправ у сфері управління кіберкризами. Такі заходи сприяють перевірці ефективності чинних процедур реагування на європейському та національному рівнях, а також дозволяють своєчасно виявляти інституційні та операційні недоліки.

Значну роль Агентство відіграє у формуванні спільної ситуаційної обізнаності Європейського Союзу, ґрунтуючись на власній діяльності з моніторингу кіберінцидентів і загроз та у межах Програми кіберпартнерства ENISA. Це включає обмін достовірною й оперативною інформацією щодо поточних подій, а також підготовку регулярних поглиблених технічних звітів відповідно до вимог Акта ЄС про кібербезпеку [3].

У цьому контексті ENISA також забезпечує надання релевантної та своєчасної інформації інституціям і органам Європейського Союзу, зокрема Європейській службі зовнішніх дій та відповідним робочим структурам, що дозволяє інтегрувати кібербезпечковий вимір у загальносоюзні механізми політичного та кризового реагування.

Крім того, Агентство надає послуги з підвищення готовності до кіберінцидентів (*ex ante*), а також підтримку реагування і відновлення після них (*ex post*) для життєво важливих, важливих і критичних суб'єктів у межах Європейського Союзу. Така діяльність спрямована на зміцнення загальної кіберстійкості та мінімізацію негативних наслідків кіберкриз для функціонування суспільства, економіки та публічних інституцій.

Діяльність ENISA спрямована на методичну та експертну підтримку національних органів кібербезпеки держав-членів Європейського Союзу у питаннях кризового управління, формування ситуаційної обізна-

ності, міжінституційної координації та ухвалення політичних рішень в умовах кіберзагроз. У цьому контексті Агентство виступає центральним інформаційно-аналітичним вузлом, який забезпечує обмін даними та сприяє узгодженості дій між Мережею команд реагування на комп'ютерні інциденти (CSIRTs Network), Європейською мережею організацій зв'язку у сфері кіберкриз (EU-CyCLONe), а також іншими релевантними інституціями, органами та агентствами Європейського Союзу, зокрема CERT-EU, Європейською службою зовнішніх дій та Eurropol, у період масштабних інцидентів і кризових ситуацій [4].

У межах цієї діяльності ENISA приділяє особливу увагу зміцненню спроможностей щодо підготовки до кіберінцидентів та реагування на них, забезпечуючи розвиток як превентивних, так і оперативних механізмів реагування.

Важливим напрямом є підвищення рівня інституційної зрілості та професійної спроможності оперативних спільнот, включаючи розвиток співпраці з правоохоронними органами, що дозволяє поєднувати технічний і правозастосовний виміри реагування на кіберзагрози.

Окремий акцент робиться на забезпеченні скоординованого реагування та відновлення після масштабних кіберінцидентів, що охоплюють різні секторальні та інституційні спільноти. Такий підхід спрямований на подолання фрагментарності у реагуванні та формування узгодженого міжгалузевого механізму дій.

Водночас ENISA сприяє еволюції спільного реагування Європейського Союзу, забезпечуючи можливість практичного впровадження ініціатив і пропозицій, сформованих на рівні ЄС, що дозволяє поступово інституціоналізувати модель колективної кіберстійкості Союзу.

Логічним продовженням аналізу операційної та координаційної ролі Агентства у сфері реагування на кіберінциденти є розгляд його стратегічної функції — оцінювання загального стану кібербезпеки в Європейському Союзі та формування доказової основи для подальшого розвитку політики у цій сфері.

Відповідно до мандата, визначеного Актом ЄС про кібербезпеку, діяльність European Union Agency for Cybersecurity зосереджена на досягненні високого спільного рівня кібербезпеки в межах Союзу та на підтримці Європейського Союзу і держав-членів у нарощуванні їхніх спроможностей у сфері кібербезпеки. Таким чином, інституційна роль ENISA виходить за межі технічної координації та охоплює стратегічний вимір оцінки та розвитку кіберстійкості.

Останні роки характеризуються інтенсивним формуванням нормативно-політичної архітектури кібербезпеки ЄС, зокрема через ухвалення горизонтальних і секторальних законодавчих актів, спрямованих на підвищення загального рівня захищеності в Союзі. Водночас геополітична динаміка та еволюція кіберзагроз суттєво впливають на поведінку і тактику як державних, так і недержавних суб'єктів, що зумовлює необхідність системного та постійного перегляду підходів до забезпечення кібербезпеки.

У цих умовах комплексне розуміння рівня розвитку кібербезпеки держав-членів набуває принципового значення для досягнення визначених цілей. Послідовний і систематичний моніторинг рівнів кібербезпеки в межах Європейського Союзу є ключовим інструментом оцінювання наявних спроможностей, виявлення структурних прогалин і визначення пріоритетних напрямів удосконалення кіберекосистеми Союзу.

Відповідно до статті 18 Директиви (ЄС) 2022/2555 (NIS2), ENISA уповноважене у співпраці з Європейською комісією та Групою співробітництва готувати та ухвалювати раз на два роки звіт про стан кібербезпеки в Союзі. Перший дворічний звіт про стан кібербезпеки в Європейському Союзі було прийнято та оприлюднено 3 грудня 2024 року. Його метою є надання органам формування політики ЄС доказово обґрунтованого огляду поточного стану кібербезпекового середовища та наявних спроможностей на рівні Союзу, держав-членів і суспільства загалом. Звіт також містить рекомендації щодо усунення виявлених прогалин і слабких місць, що спрямовані на подальше підвищення

рівня кібербезпеки в Європейському Союзі. Прийняття такого звіту ENISA у співпраці з Комісією та Групою співробітництва прямо відповідає вимогам статті 18 Директиви NIS2.

З точки зору фінансового забезпечення кібербезпеки, належне бюджетне та кадрове ресурсування є визначальною умовою підтримання наявних спроможностей і розвитку кіберстійкості. У межах звіту про інвестиції в кібербезпеку за напрямом NIS ENISA аналізує вплив нормативної рамки ЄС у сфері кібербезпеки, зокрема Директиви NIS, на обсяг інвестицій та рівень організаційної зрілості суб'єктів, що підпадають під її дію. Щорічний аналіз дозволяє оцінити, яким чином ключові та важливі суб'єкти критичних секторів реагують на еволюцію регуляторного середовища та сучасні виклики у сфері кібербезпеки, і тим самим формує емпіричну основу для подальшого вдосконалення політики Союзу.

З метою подальшого інституційного посилення зазначеного моніторингового напрямку діяльності European Union Agency for Cybersecurity розробило інструмент під назвою «EU Cybersecurity Index» (EU CSI) — аналітичний механізм, призначений для системного опису та оцінювання кібербезпечного стану держав-членів і Європейського Союзу в цілому [2].

Індекс ґрунтується на максимально повному використанні наявних даних та інформаційних джерел і забезпечує комплексне уявлення про рівень зрілості та спроможностей у сфері кібербезпеки. Його методологія дозволяє не лише фіксувати поточний стан, а й ідентифікувати структурні прогалини, а також потенціал для взаємного навчання між державами-членами та запозичення кращих практик.

Таким чином, EU CSI виступає інструментом вимірювання прогресу у напрямі досягнення вищих стандартів кібербезпеки, співвіднесених із визначеними індикаторами індексу. Це забезпечує об'єктивовану основу для оцінки результативності політики ЄС у сфері кібербезпеки та подальшого вдосконалення нормативних і інституційних механізмів забезпечення кіберстійкості.

Висновки

Інституційна еволюція European Union Agency for Cybersecurity свідчить про поступову трансформацію Агентства з консультативно-аналітичного органу у суб'єкта з розширеними координаційними та квазі-операційними повноваженнями. Закріплення постійного мандата, інтеграція у механізми кризового реагування, формування системи сертифікації та запровадження інструментів стратегічного моніторингу означають інституціоналізацію його ролі як центрального елемента європейської архітектури кібербезпеки. Посилення повноважень ENISA та розвиток спільних процедур реагування засвідчують тенденцію до поглиблення наднаціональної координації у сфері кібербезпеки та поступового формування інтегрованої моделі колективної кіберстійкості Європейського Союзу. Такий розвиток демонструє зміщення від фрагментарної взаємодії держав-членів до більш системної багаторівневої конструкції управління кіберризиками, у межах якої національні компетенції поєднуються з централізованими інструментами стратегічного й операційного впливу. Таким чином, ENISA виступає не лише технічним агентством підтримки, а й ключовим інституційним механізмом реалізації спільної кібербезпечної політики Європейського Союзу, що має визначальне значення для забезпечення його цифрової стійкості в умовах зростаючих глобальних загроз.

Література

1. Council of the European Union. (2018). Council Decision (EU) 2018/1993 of 11 December 2018 on the Integrated Political Crisis Response (IPCR) arrangements. Official Journal of the European Union, L 320, 28–34.
2. European Commission. (2017). Joint communication to the European Parliament and the Council: Resilience, deterrence and defence: Building strong cybersecurity for the EU (JOIN(2017) 450 final).
3. European Commission. (2020). The EU's Cybersecurity Strategy for the Digital Decade (JOIN(2020) 18 final).
4. European Commission. (2026). Proposal for a Regulation amending Regulation (EU) 2019/881 as regards strengthening ENISA and

the Union's cybersecurity resilience (COM(2026) final).

5. European Parliament and Council of the European Union. (2014). Regulation (EU) No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS Regulation). Official Journal of the European Union, L 257, 73–114.

6. European Parliament and Council of the European Union. (2016). Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union (NIS Directive). Official Journal of the European Union, L 194, 1–30.

7. European Parliament and Council of the European Union. (2018). Directive (EU) 2018/1972 establishing the European Electronic Communications Code. Official Journal of the European Union, L 321, 36–214.

8. European Parliament and Council of the European Union. (2019). Regulation (EU) 2019/881 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification (Cybersecurity Act). Official Journal of the European Union, L 151, 15–69.

9. European Parliament and Council of the European Union. (2022). Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union, L 333, 80–152.

10. European Parliament and Council of the European Union. (2022). Regulation (EU) 2022/2554 on digital operational resilience for the financial sector (Digital Operational Resilience Act – DORA). Official Journal of the European Union, L 333, 1–79.

**CENTRALISATION OF
CYBERSECURITY FUNCTIONS IN THE
EUROPEAN UNION: THE ROLE OF ENISA
IN THE NEW CYBER RISK GOVERNANCE
ARCHITECTURE**

The article provides a comprehensive institutional and legal analysis of the process of centralisation of cybersecurity functions within the European Union through the prism of the transformation of the mandate and role of the

European Union Agency for Cybersecurity (ENISA). It examines the evolution of the Agency's legal status from a primarily advisory and analytical body to an entity endowed with expanded coordination and quasi-operational powers within the emerging EU cyber risk management architecture. The study substantiates that the adoption of Regulation (EU) 2019/881 (Cybersecurity Act), as well as the further development of the regulatory framework, in particular Directive (EU) 2022/2555 (NIS2), have become decisive factors in the institutional modernisation of ENISA and in strengthening its role in shaping an integrated model of collective cyber resilience.

The paper analyses the key areas of the Agency's activities, including the establishment and maintenance of the European cybersecurity certification framework for ICT products and services, the development of operational cooperation mechanisms among Member States within the CSIRTs Network and EU-CyCLONe, participation in crisis response procedures under the Integrated Political Crisis Response (IPCR) arrangements, and the performance of strategic and analytical functions related to the preparation of the biennial State of Cybersecurity in the Union report and the development of cybersecurity maturity assessment tools, notably the EU Cybersecurity Index. It is argued that ENISA is increasingly acting as an institutional hub for coordination, information exchange, and the development of common standards in the field of cybersecurity. Particular attention is paid to the impact of contemporary geopolitical challenges, notably the full-scale armed aggression of the Russian Federation against Ukraine and the accompanying hybrid and cyber operations, on the transformation of the European Union's approach to ensuring digital resilience.

The conclusions advance the thesis that the institutional evolution of ENISA reflects a broader trend towards deeper integration and the gradual supranationalisation of EU cybersecurity policy, within which Member States' national competences are combined with centralised mechanisms of strategic monitoring, crisis management, and regulatory harmonisation.

Keywords: European Union; ENISA; cybersecurity; cyber resilience; Cybersecurity Act; NIS2; security; cyber crisis.