МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
ЧЕРНІВЕЦЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ЮРІЯ ФЕДЬКОВИЧА

Факультет історії, політології та міжнародних відносин
Кафедра міжнародних відносин та суспільних комунікацій

Кібербезпека ЄС в умовах повномасштабної російсько-української війни: виклики та рішення

Кваліфікаційна робота

Рівень вищої освіти – другий (магістерський)

Виконав:
студент 6 курсу, 604 групи
Бідоча Антон
Керівник:
кандидат історичних наук,
доцент **Звоздецька О.Я.**

До захисту допущено
на засіданні кафедри
протокол №____ від _____ 2025 р.
Зав. кафедрою _____ проф. Макар. В.Ю.

Чернівці – 2025

Анотація

Магістерська робота присвячена комплексному дослідженню трансформації системи кібербезпеки Європейського Союзу в умовах повномасштабної російсько-української війни. У роботі обґрунтовується, що кіберагресія стала одним із ключових вимірів гібридної стратегії Російської Федерації, спрямованої на дестабілізацію України та вплив на цифрову інфраструктуру країн ЄС. Внаслідок цього кіберпростір перетворився на критичний фронт сучасної війни, що зумовило перегляд політики, інституційної архітектури та практик кіберзахисту в Європейському Союзі.

Ключові слова: кібербезпека, ЄС, російсько-українська війна, кіберагресія, гібридні загрози, критична інфраструктура, кібероборона, NIS2, ENISA, Україна–ЄС.

Summary

This master’s thesis provides a comprehensive analysis of the transformation of the European Union’s cybersecurity system in the context of the full-scale Russian–Ukrainian war. The study argues that cyber aggression has become one of the central dimensions of Russia’s hybrid strategy aimed not only at destabilizing Ukraine but also at influencing the critical digital infrastructure of EU member states. As a result, cyberspace has turned into a pivotal front of contemporary warfare, prompting a re-evaluation of security policies, institutional structures, and operational mechanisms within the European Union.

Keywords: cybersecurity, European Union, Russian–Ukrainian war, cyber aggression, hybrid threats, critical infrastructure, cyber defence, NIS2, ENISA, EU–Ukraine cooperation.

Кваліфікаційна робота містить результати власних досліджень. Використання ідей, результатів і текстів наукових досліджень інших авторів мають посилання на відповідне джерело_____ Бідоча А.І.

(підпис)

ЗМІСТ

ВСТУП 3
РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ 7
1.1. Понятійні та концептуально-теоретичні засади дослідження. 7
1.2. Стан джерельної бази дослідження. 16
РОЗДІЛ II. ВПЛИВ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ НА КІБЕРБЕЗПЕКУ ЄС 25
2.1. Кіберагресія Росії як елемент гібридної війни та її вплив на безпеку ЄС 25
2.2. Кіберзагрози критичній інфраструктурі та цифровій безпеці ЄС. . 38
2.3. Кіберзлочинність як виклик кібербезпеці ЄС. 53
РОЗДІЛ III. ЄВРОПЕЙСЬКІ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У ВОЄННИЙ ЧАС 59
3.1. Правове регулювання кіберпростору в Європейському Союзі. 59
3.2. Інституційна структура та механізми забезпечення кібербезпеки ЄС. 70
3.3. Співпраця України та ЄС у посиленні кіберстійкості держав. 84
ВИСНОВКИ 97
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ 100
SUMMARY 100

ВСТУП

Актуальність дослідження. Повномасштабна війна Російської Федерації проти України, яка розпочалася 24 лютого 2022 року, стала не лише трагедією для українського народу, а й потужним каталізатором масштабних змін у сфері міжнародної та національної безпеки. Одним із найнебезпечніших та водночас найменш видимих фронтів цієї агресії є кіберпростір. Саме в цьому вимірі Росія вже тривалий час здійснює гібридну війну, використовуючи кібератаки як інструмент дестабілізації, впливу та інформаційного тиску. У нових умовах кібербезпека перетворилася на один із ключових елементів не лише для забезпечення стабільного функціонування державних інституцій, але й для захисту критичної інфраструктури, інформаційного простору, цифрової економіки, особистих даних громадян і, зрештою, цифрового суверенітету держав.

Для України війна у кіберпросторі триває паралельно з бойовими діями на фізичному фронті. Під удар потрапляють урядові структури, військові об'єкти, банківські системи, транспортні мережі, енергетичні комплекси, освітні й медичні заклади. Масштаб і системність таких атак свідчать про високий рівень організованості та державної підтримки з боку агресора. Багато з кібератак мали транскордонний ефект, поширюючись за межі України й створюючи загрози для кібербезпеки країн Європейського Союзу. Таким чином, кіберагресія проти України перетворилася на виклик не лише для окремої держави, а й для всієї європейської та євроатлантичної спільноти.

У цьому контексті війна в Україні стала поворотною точкою для Європейського Союзу, спонукаючи його до переосмислення основ безпеки у цифрову епоху. Загроза, що постала перед країнами-членами, продемонструвала нагальну потребу в єдності зусиль, розбудові спільних механізмів кіберзахисту та удосконаленні політик протидії кібератакам. ЄС активізував свою діяльність у цій сфері, розпочавши реформування правових рамок, створення нових інституцій, підвищення спроможності національних кіберцентрів та зміцнення міжнародної співпраці.

Особливої ваги в умовах гібридної війни набула співпраця ЄС з Україною. Україна більше не розглядається лише як об’єкт нападів, а виступає повноправним партнером у розробці нових підходів до кіберстійкості. Європейський Союз визнав досвід України як унікальний і стратегічно важливий, адже саме на прикладі української кібероборони можна моделювати ефективні підходи до захисту цифрових екосистем у період збройних конфліктів. У цьому зв’язку особливого значення набуває обмін інформацією, технічна підтримка, участь українських фахівців у європейських ініціативах, а також інтеграція країни у спільні механізми реагування на інциденти у кіберпросторі.

Формування єдиного європейського простору кібербезпеки сьогодні неможливе без урахування українського чинника. Досвід відбиття кібератак, побудова системи кібероборони у воєнних умовах, а також залучення цифрових технологій до протидії дезінформації є надзвичайно цінними. Таким чином, війна, попри всі свої жахливі наслідки, стала також потужним імпульсом до формування нової архітектури цифрової безпеки Європи, в якій Україна відіграє важливу роль як рівноправний партнер і носій унікального практичного досвіду.

Метою даного дослідження є всебічний аналіз кібербезпеки Європейського Союзу в умовах повномасштабної російсько-української війни, зосереджуючи увагу на головних викликах, загрозах і рішеннях, що були сформовані в цей період.

Завдання дослідження:

- Визначити понятійні та концептуальні основи кібербезпеки в контексті воєнних конфліктів.
- Проаналізувати джерельну базу дослідження проблем кібербезпеки ЄС.
- Розкрити характер та масштаби кіберагресії Росії проти України та її наслідки для ЄС.
- Дослідити вплив війни в Україні на кібербезпеку ЄС та окреслити виклики і перспективи формування спільної кіберполітики.

- Проаналізувати правові та інституційні механізми Європейського Союзу, спрямовані на забезпечення кібербезпеки в умовах збройного конфлікту.
- Оцінити формати співпраці між Україною та ЄС у сфері кібербезпеки та кіберстійкості.

Об'єктом дослідження є система забезпечення кібербезпеки Європейського Союзу.

Предметом дослідження є кібербезпека ЄС в умовах повномасштабної російсько-української війни.

Методи дослідження. Для досягнення цілей роботи використано комплексний підхід, який охоплює кілька взаємодоповнюючих методів. Зокрема, застосовано історичний метод, що дозволяє простежити еволюцію політики кібербезпеки Європейського Союзу у передвоєнний та воєнний періоди, а також виявити, як змінювалися пріоритети та інструменти реагування на кіберзагрози під впливом зовнішніх факторів. Системний аналіз дав змогу розглядати кібербезпеку як багаторівневу систему взаємодії між державами-членами, інституціями ЄС та зовнішніми партнерами, що, у свою чергу, дозволило визначити ключові елементи механізмів координації на європейському рівні. Порівняльний метод використано для аналізу трансформації стратегії кіберзахисту до та після початку повномасштабного вторгнення Росії в Україну, що дало можливість виявити відмінності в підходах до протидії загрозам у мирний і кризовий періоди. Контент-аналіз матеріалів засобів масової інформації, офіційних заяв, звітів Європейської комісії, ENISA, Європолу, НАТО та інших джерел дозволив виявити головні наративи, тренди та зміни в публічному дискурсі щодо кібербезпеки. Крім того, здійснено аналіз документів для вивчення правової та інституційної бази ЄС у сфері кіберзахисту, зокрема таких ключових актів, як Директива NIS2, Стратегія кібербезпеки ЄС 2020 року, Рамкова структура кіберкризового реагування, що дало змогу визначити нормативні підходи до зміцнення кіберстійкості Євросоюзу.

Структура роботи. Магістерська робота складається зі вступу, трьох основних розділів, висновків, списку використаної літератури (понад 150

найменувань). Розділ 1 охоплює аналіз поняття кібербезпеки, гібридної війни, цифрового суверенітету та актуальних підходів до їх дослідження. Розділ 2 розглядає масштаб кібератак, їхні наслідки для ЄС, нові форми кіберзагроз та динаміку адаптації європейської системи безпеки. Розділ 3 аналізує правову й інституційну базу, співпрацю з Україною, нові стратегії ЄС з кібероборони та їх ефективність у кризових умовах

РОЗДІЛ 1. ТЕОРЕТИКО-КОНЦЕПТУАЛЬНІ ЗАСАДИ ДОСЛІДЖЕННЯ КІБЕРБЕЗПЕКИ

1.1. Понятійні та концептуально-теоретичні засади дослідження.

У сучасному безпековому дискурсі поняття «кібербезпека» займає центральне місце, зокрема в умовах масштабної гібридної війни, що триває між Росією та Україною. Європейський Союз, що сприймає цю війну як стратегічну загрозу для власної стабільності, активізував нормативне, інституційне й політичне переосмислення основ кіберзахисту. Відтак, дослідження кібербезпеки в контексті ЄС та України потребує чіткого окреслення понятійних рамок і концептуального апарату. Визначення термінів та концепцій є не лише академічною необхідністю, а й практичною умовою ефективного регулювання та реагування на кіберзагрози, які набули особливої гостроти після 2022 року.

Поняття «кібербезпека» не має універсального визначення, проте найпоширеніші дефініції зосереджуються на забезпеченні цілісності, конфіденційності, доступності та стійкості інформаційних систем, що функціонують у кіберпросторі. Європейське агентство з кібербезпеки (ENISA) визначає кібербезпеку як здатність захищати мережі, пристрої та дані від кіберзагроз і забезпечувати їхню надійну роботу в умовах ризиків. Подібне розуміння пропонується й у Регламенті ЄС 2019/881 (Cybersecurity Act), де акцент зроблено на технологічному й організаційному аспектах кіберзахисту [81].

У Директиві ЄС NIS2, що набула чинності в 2023 році, кібербезпека подається як сукупність заходів, які необхідні для захисту мережевих і інформаційних систем, користувачів та інших осіб від кіберзагроз [69]. Українське законодавство пропонує визначення через призму національної безпеки: відповідно до Закону України «Про основні засади забезпечення кібербезпеки України» (ст. 1), кібербезпека – це захищеність кіберпростору, що забезпечується через правові, організаційні, технічні заходи і є складовою національної безпеки [10]. Таким чином, у всіх правових контекстах поняття

кібербезпеки поєднує технічні (захист систем), організаційні (реагування та управління) та політичні (частина стратегії безпеки) компоненти.

З огляду на складність та міждисциплінарність тематики, важливо розмежовувати суміжні поняття. Під кіберзагрозою слід розуміти потенційне джерело шкідливого впливу на мережеву або інформаційну систему. Це поняття охоплює як технологічні ризики (вразливості), так і суб'єктні джерела (хакерські угруповання, державні актори). Кіберінцидент, у свою чергу, – це подія або серія подій, які мали або могли мати негативний вплив на безпеку мереж чи даних. Зазвичай ідеться про несанкціонований доступ, знищення або порушення роботи системи. Кібератака – це вже цілеспрямована дія, що має на меті спричинити шкоду інформаційній інфраструктурі або отримати несанкціонований доступ до даних. У рамках гібридної війни кібератаки часто мають і інформаційно-психологічний ефект – порушення довіри до державних структур або створення паніки в суспільстві. Кібероборона розглядається як активна частина кібербезпеки, що включає не лише захист, а й можливість реагування, нейтралізації та відновлення. У європейській термінології, особливо в рамках PESCO та ENISA, цей термін набув ширшого змісту, включаючи спільне реагування держав-членів на загрози [62]. Кіберстійкість – це здатність системи протистояти, адаптуватися та швидко відновлюватися після кіберінциденту. Ця категорія особливо важлива в контексті критичної інфраструктури, коли навіть короткострокове порушення може мати катастрофічні наслідки для енергетики, транспорту, медицини. Нарешті, критична інформаційна інфраструктура – це об'єкти, порушення функціонування яких унаслідок кіберзагроз може призвести до порушення функцій держави, життя та здоров'я населення або економічної стабільності. Згідно з Директивою CER ЄС, до критичної інфраструктури включено 11 секторів, у тому числі цифрові, енергетичні та водні системи [38].

Застосування цих понять у науковому дослідженні потребує також аналізу теоретичних підходів, що пояснюють сутність, функції та виклики кібербезпеки в умовах сучасних глобальних загроз. Геополітичний підхід, що бере за основу конкуренцію держав за домінування в кіберпросторі, актуалізується в умовах

агресії РФ проти України. У цьому контексті кіберпростір виступає не лише як технологічне середовище, а як поле реалізації геополітичних інтересів: зокрема, атакування критичної інфраструктури України мало на меті не лише знищення об'єктів, а й політичну дестабілізацію з послабленням підтримки з боку ЄС. В умовах війни кібероперації стали логічним продовженням військових дій з боку Росії, тому їх не можна розглядати у відриві від класичної безпеки.

Системно-функціональний підхід дозволяє розглядати кібербезпеку як невід'ємну складову загального функціонування державного та наддержавного організму. Для ЄС це виявляється в спробі побудови цифрового єдиного ринку, де кібербезпека є умовою забезпечення сталого функціонування економіки, транспорту, енергетики, соціальних послуг. У випадку України системний підхід дозволяє поєднати в дослідженні як національні завдання (захист реєстрів, банківської системи, е-урядування), так і координацію з європейськими структурами (ENISA, CERT-EU).

Інституційно-правовий підхід акцентує на ролі міжнародного та національного правового регулювання, а також інституційного забезпечення кіберзахисту. В ЄС це особливо виражено у впровадженні таких інструментів, як NIS2, CER, Cyber Solidarity Act, що задають правила і обов'язки для суб'єктів цифрової безпеки. Водночас в Україні нормативна база активно адаптується до європейської моделі, що є предметом аналізу в подальших розділах дослідження. У цьому підході важливе значення має також взаємодія інституцій – національних агентств, європейських агентств, силових структур, приватного сектору.

Інфраструктурний підхід дозволяє зосередитись на вразливості цифрових платформ, каналів комунікації, центрів обробки даних. Важливо не лише виявити вразливості, але й оцінити їхній каскадний ефект на загальну стійкість країни чи Союзу. Саме цей підхід використовують під час аналізу ризиків у директивах ЄС, зокрема в CER.

Концепція гібридної війни, яка поєднує військові, політичні, інформаційні та кіберзасоби, є, безумовно, ключовою для розуміння місця кібербезпеки у

конфлікті РФ проти України. За даними ENISA Threat Landscape 2023, РФ залишається основним джерелом кібератак проти України та країн ЄС, що мають не лише технічний, а й стратегічний характер (наприклад, атака на супутникову мережу KA-SAT) [39]. У цьому контексті кіберпростір розглядається як бойове поле, а кіберзагрози – як зброя нового покоління, яка потребує не лише технічної протидії, а й теоретичного осмислення в межах загальної безпекової парадигми.

У рамках наукового аналізу кібербезпеки, особливо в контексті повномасштабної війни в Україні та глобальних трансформацій, постає потреба осмислити цю проблематику не лише з прикладної, а й з теоретичної перспективи. Кіберзагрози дедалі частіше розглядаються не просто як технічні інциденти, а як частина ширших безпекових процесів, що охоплюють політичні, економічні, правові й соціальні виміри. У цьому контексті низка теоретичних парадигм дозволяє більш глибоко інтерпретувати феномен кібербезпеки та взаємодії держав і наднаціональних структур у протидії кіберзагрозам.

Однією з найбільш релевантних теорій є концепція сек'юритизації, або теорія безпеки Копенгагенської школи, сформульована Бузаном, Веєвером та де Вільде. Вона полягається в тому, що безпека є не стільки об'єктивною категорією, скільки результатом дискурсивного акту – процесу, в межах якого певна проблема набуває статусу екзистенційної загрози, що потребує позаурядових і негайних дій. У випадку кібербезпеки цей підхід дозволяє розглядати загрози у цифровому просторі не лише як технічні виклики, а як інструмент політичної мобілізації та зміни порядку денного [91]. Після 2022 року кіберзагрози, пов'язані з агресією Російської Федерації, були сек'юритизовані як в Україні, так і в ЄС. Риторика політичних лідерів, зокрема в заявах Європейської комісії та Ради ЄС, прямо ототожнює кібератаки з елементами гібридної війни, які загрожують суверенітету та політичній стабільності. Таким чином, кіберпростір стає ареною, де відбувається політичне означення загроз, що легітимізує мобілізацію ресурсів, зміну правових режимів і міжнародну кооперацію.

Інша група теоретичних підходів – теорії міжнародних відносин – дозволяє інтерпретувати динаміку співпраці та конфліктів у сфері кібербезпеки. З позиції реалізму, домінуючою логікою є боротьба за вплив і виживання держав у безпековому середовищі, що в кіберпросторі проявляється як змагання за технологічну перевагу, протидія шпигунству та контроль над критичною інфраструктурою. Неореалізм посилює цю парадигму, наголошуючи на структурній анархії міжнародної системи, що стимулює держави до самодопомоги [20]. Водночас ліберальний інституціоналізм пояснює появу міжнародних механізмів співпраці, таких як ENISA, PESCO, CERT-EU, через прагнення до зменшення транзакційних витрат, забезпечення обміну інформацією та підвищення передбачуваності в поведінці акторів. Саме в цій логіці функціонує європейська модель кіберстійкості, яка заснована на багатоактірному підході, участі держав-членів, агенцій, приватного сектору, громадянського суспільства [107].

Теорія мереж та цифрових ризиків дає змогу розглядати кіберпростір як складну, гетерогенну, взаємопов'язану систему, де вразливість однієї ланки може спричинити каскадні наслідки – так звані cascading failures. Такий підхід надзвичайно актуальний для критичної інфраструктури, особливо в енергетичному та транспортному секторах. Прикметним є кейс кібератаки на супутникову мережу KA-SAT у 2022 році: атака, спрямована на Україну, одночасно дестабілізувала інфраструктуру в Німеччині та Польщі. Це підтверджує, що кіберпростір є простором колективної вразливості, де національні інциденти можуть мати транснаціональні наслідки. Мережевий підхід також дозволяє дослідити характер взаємозв'язків між акторами (держави, корпорації, платформи, агентства) та аналізувати ризики через призму структурної топології мережі, на відміну від традиційної ієрархічної моделі безпеки [79].

Європейська концепція кіберстійкості, що дедалі частіше фігурує в документах ЄС (ENISA, NIS2, Cyber Solidarity Act), базується на здатності цифрових систем не лише уникати загроз, а й адаптуватися до них, мінімізувати

збитки та швидко відновлювати функціонування. Це інтегративна парадигма, яка поєднує технічні, організаційні та нормативно-правові елементи. Ключовими елементами є превенція, виявлення, реагування та відновлення. Особливу увагу приділено співпраці – і між державами, і між публічним і приватним секторами. В межах концепції кіберстійкості цифрова автономія розглядається як стратегічна ціль ЄС, а Україна поступово долучається до цього простору через імплементацію NIS2, участь у програмах Digital Europe і доступ до кіберрезерву ЄС [104]. Війна сприяла активації цієї концепції, продемонструвавши, що цифрова стійкість – не теоретичне поняття, а умова виживання функціонуючої держави.

Поряд з теоретичними підходами важливим є визначення методологічних принципів, що використовуються для вивчення кібербезпеки в межах міждисциплінарного дослідження. Системний підхід дозволяє розглядати кібербезпеку як складову цілісної безпекової архітектури ЄС, де взаємодіють політичні інституції, агентства, служби реагування, приватні постачальники IT-послуг. Це дає змогу аналізувати не лише окремі інциденти, а й взаємозв’язки між компонентами системи: від ENISA до національних CSIRTs, від PESCO до CyCLONe [28]. Порівняльно-правовий аналіз дозволяє дослідити нормативну конвергенцію між законодавствами України та ЄС, зокрема у контексті імплементації Директиви NIS2, CER та національного Закону України «Про основні засади забезпечення кібербезпеки». Аналізуються як загальні концепти (захист критичної інфраструктури, обов’язки операторів), так і конкретні механізми (оцінка ризиків, повідомлення про інциденти).

Емпіричний підхід передбачає використання конкретних кейсів кібератак, таких як операція Industroyer2 проти української енергетики, атака на мережу KA-SAT, кібершпіонаж від угруповань APT28 або Sandworm. Аналіз даних, зібраних в рамках цих інцидентів, дозволяє верифікувати гіпотези щодо тактик, технік та процедур (TTPs) супротивника, ефективності заходів реагування, ролі міжнародної допомоги (наприклад, діяльності CRRTs чи CERT-EU). Інституційний аналіз зосереджується на тому, як функціонують основні актори

в політиці кібербезпеки: ENISA як центр знань і координації, CERT-EU як оперативна одиниця реагування, PESCO як інструмент стратегічної оборонної співпраці, CyCLONe як мережа кризового управління. Аналіз їхніх мандатів, ресурсів, функціональних зв'язків із національними структурами дає змогу оцінити ступінь інтегрованості європейської системи кіберзахисту.

Нарешті, міждисциплінарність є невід'ємною складовою методології. Вивчення кібербезпеки вимагає поєднання знань з галузей права, інформаційних технологій, політичної науки, міжнародних відносин, кризового менеджменту. В умовах гібридної війни це особливо важливо, адже кіберзагрози перетинають кордони між секторами: вони одночасно є і технічною атакою, і юридичним інцидентом, і політичним викликом. Лише комплексний підхід, заснований на поєднанні кількох аналітичних перспектив, дозволяє адекватно оцінити природу кіберзагроз, їхню ескалацію та шляхи реагування.

Становлення кібербезпеки як окремого напряму наукового дослідження є відносно новим, проте стрімко розвивається на тлі зростання залежності суспільств від цифрових технологій та загроз, які виникають у результаті їхнього зловживання. Науковий дискурс у цій сфері за останнє десятиліття зазнав якісного перетворення – від досліджень у межах інформаційних технологій до складних міждисциплінарних моделей, які поєднують юридичні, безпекові, геополітичні та соціальні аспекти. У європейській академічній традиції кібербезпека тісно інтегрується в проблематику національної та регіональної безпеки, кібердипломатії, захисту критичної інфраструктури, цифрових прав та свобод.

Окрему увагу варто приділити сучасним європейським програмам з кіберстійкості, які одночасно є предметом політичного управління, правового регулювання та стратегічного дослідження. Прийняття в 2022 році Директиви NIS2 стало вододілом у законодавчому оформленні кібербезпеки в ЄС. Цей документ значно розширив сферу застосування попередньої NIS (2016), зобов'язавши не лише операторів критичної інфраструктури, але й цифрові постачальники, компанії середнього бізнесу та органи місцевого самоврядування

дотримуватися стандартів захисту. У науковому середовищі NIS2 сприймається як прояв нового підходу до кіберрегулювання – не через м'які рекомендації, а через створення обов'язкових юридичних рамок із санкційними механізмами.

Так само програмні документи PESCO, зокрема проєкти CRRTs та кіберкоординаційні центри, потрапляють у фокус уваги європейських дослідників як приклади поступового створення спроможності до колективної кібероборони. Багато аналітиків (наприклад, Савчук С. О.) розглядають Cyber Solidarity Act як наступний етап інституціоналізації: не лише політика й право, але й створення інфраструктури спільного реагування, фінансованої ЄС [12]. У цих дебатах звучить теза про те, що цифрова безпека в ЄС переходить із фази координації до фази інтеграції – і саме це є викликом для країн-партнерів, таких як Україна, які прагнуть долучитися до цього середовища.

Ключовою тенденцією в дослідженнях стає міждисциплінарність. З одного боку, вона дає змогу охопити кібербезпеку в усій її складності – як питання технологічне, політичне, юридичне, безпекове та соціальне. З іншого боку, вона вимагає високої фаховості дослідників у кількох сферах одночасно. В умовах гібридної війни між Україною та Росією межі між технічним інцидентом, інформаційною операцією, юридичним порушенням і військовим актом практично стираються. Це створює потребу у створенні нових міжгалузевих дослідницьких методологій – як у межах академічної науки, так і в рамках аналітичних центрів, таких як RAND, Chatham House, EUISS або український Центр протидії дезінформації.

Попри прогрес, існує низка об'єктивних викликів, які обмежують розвиток наукових досліджень у сфері кібербезпеки. По-перше, це висока швидкість змін: кібертехнології та тактики загроз еволюціонують швидше, ніж з'являються академічні публікації. По-друге, значна частина матеріалів є засекреченою або обмеженою в доступі – як з міркувань національної безпеки, так і через внутрішню закритість IT-сектору. По-третє, багато аспектів кібербезпеки мають наддержавний характер: загрози часто є транскордонними, а відповідальність за реагування розподілена між державами, приватним сектором і міжнародними

організаціями. Це ускладнює вироблення єдиної методології та верифікацію результатів.

Узагальнюючи теоретико-методологічні основи, слід зазначити, що кібербезпека постає як комплексне й поліцентричне явище, що охоплює юридичні категорії, політичні механізми, технологічну динаміку й соціальні наративи. Поняття, які фігурують у дослідженні – кіберзагроза, кібератака, кіберстійкість, критична інформаційна інфраструктура – мають чітко виражений правовий і функціональний зміст у нормативних документах ЄС і України. Їхня теоретична інтерпретація ґрунтується на концепціях сек'юритизації, теоріях міжнародних відносин, мережевих ризиків і європейській парадигмі resilience. Методологічно дослідження базується на системному, порівняльному, емпіричному, інституційному й міждисциплінарному підходах. Вибір цих підходів є виправданим з огляду на комплексність об'єкта дослідження та потребу адекватно відтворити взаємозв'язки між кіберпростором, політикою, правом, війною й транснаціональними процесами. Саме таке розуміння забезпечує глибину аналізу в подальших розділах цієї роботи. Хронологічні межі дослідження охоплюють період з 2014 до 2025 року – від початку гібридної агресії РФ проти України до повномасштабної війни та активної інтеграції України у кіберполітику ЄС. Географічно аналіз охоплює простір Європейського Союзу як спільноти держав із уніфікованою політикою у сфері кібербезпеки, а також Україну як партнера, що поступово адаптує європейську модель і одночасно слугує випробувальним полем для міжнародних механізмів кіберреагування.

1.2. Стан джерельної бази дослідження

Однією з найважливіших особливостей змістовної основи досліджень ЄС у сфері кібербезпеки в контексті конфлікту між Росією та Україною є нормативно-правове та аналітичне забезпечення, яке відповідає реальному політичному, технологічному та інституційному розвитку за останні кілька років. Основу джерельної бази цього дослідження становлять обов'язкові до виконання закони, що визначають правові засади кібербезпеки в ЄС та Україні, а також стратегічні та аналітичні звіти, підготовлені міжнародними агенціями, які здійснюють моніторинг, оцінку та прогнозування кіберзагроз. Ці дві групи джерел дозволяють скласти повну картину того, як розвивається регуляторне середовище і які проблеми виникають у реальному кіберпросторі в умовах військового конфлікту.

За останні п'ять років Європейський Союз значно зміцнив і вдосконалив свою нормативно-правову базу у сфері кібербезпеки. Прийняття Директиви NIS2 (2022/2555) стало знаковою подією, яка замінила попередню Директиву NIS, розширивши сферу її дії на нові сектори (такі як цифрова інфраструктура, управління та охорона здоров'я) та застосувавши принцип пропорційної відповідальності за кіберстійкість критично важливих об'єктів [69]. Національні органи влади держав-членів повинні були проводити систематичну оцінку ризиків, а компанії – повідомляти про кіберінциденти, впроваджувати заходи внутрішнього захисту та навчати персонал. У контексті дослідження воєнних дій ці положення є найбільш застосовними, оскільки критична інфраструктура найчастіше зазнає кібератак.

Не менш важливим є Регламент (ЄС) 2019/881, або Закон про кібербезпеку, який не лише надав постійний характер мандату ENISA, але й створив першу загальноєвропейську схему сертифікації ІКТ-продуктів та послуг. Це дозволяє державам уникнути фрагментації стандарту в національному контексті, забезпечує довіру між державами і сприяє підвищенню загального рівня безпеки у віртуальному світі. Регламент також особливо застосовний в контексті дебатів

щодо спільної з партнерами кіберінфраструктури, зокрема, в енергетичному, транспортному та комунікаційному секторах.

NIS2 був доповнений документом CER, прийнятим у 2022 році (Директива 2022/2557), який окреслює потреби фізичної та технічної стійкості критично важливих об'єктів. Ця директива розширила перелік секторів, в яких держави-члени повинні забезпечити ідентифікацію основних гравців, оцінку ризиків та розгортання наскрізних систем безперервності обслуговування. Компанії повинні здійснювати внутрішнє сканування вразливостей, вживати заходів безпеки після інцидентів та повідомляти про інциденти. Така інтеграція фізичної та кібербезпеки відповідає гібридній природі сучасного конфлікту [34].

Окремої уваги заслуговує новітній інструмент – Акт про кіберсолідарність, робота над яким зараз завершується (Регламент (ЄС) 2025/38). Його положення спрямовані на створення основи для негайного реагування на масові кібератаки: передбачається створення Європейського кіберрезерву (підрозділів швидкого реагування), транскордонної мережі SOC (операційних центрів безпеки) та схеми солідарного фінансування заходів з ліквідації наслідків атак. Цей закон також вносить зміни до Регламенту 2019/881 з метою надання дозволу на створення нових схем сертифікації керованих послуг з кібербезпеки [81].

З української сторони основою правового забезпечення є Закон України «Про основні засади забезпечення кібербезпеки» (2017), який визначає принципи, суб'єкти та механізми гарантування захисту кіберпростору, а також створює Національну координаційну структуру у цій сфері. Його доповнює Постанова Кабінету Міністрів № 563 (2018) про об'єкти критичної інформаційної інфраструктури, яка містить критерії визначення таких об'єктів та вимоги до їх захисту. Ці документи є основою для інкорпорації українського законодавства у правове поле ЄС [10].

Окрім законодавчого контексту, велике значення для цього дослідження мають аналітичні звіти міжнародних організацій. Починаючи з щорічних звітів ENISA, а саме ENISA Threat Landscape 2023, цей звіт надає всебічний огляд активних загроз: від DDoS-атак до програм-вимагачів та загроз для критичної

інфраструктури. ENISA не лише систематизує події, але й прогнозує загрози, що є фундаментальним для стратегічного планування кіберзахисту [39].

Звіти CERT-EU є одним із джерел актуальної інформації про кібератаки, пов'язані з війною в Україні, такі як випадки використання шкідливого програмного забезпечення, фішингові кампанії та атаки на європейські інституції. Зокрема, у 2022-2023 роках CERT-EU відстежував активність таких акторів, як APT28 та Sandworm, які одночасно атакували цілі як в Україні, так і в ЄС [19] [26].

Європейська Комісія виконує політичну координаційну функцію. У своїх комюніке та планах Комісія неодноразово підкреслювала взаємозв'язок між геополітикою та кіберзагрозами. ЄК насамперед зацікавлена у створенні механізмів колективного реагування, підтримці кіберстійкості партнерів і створенні гармонізованої політики.

Центр НАТО з аналізу спільного кіберзахисту забезпечує основу знань з кібербезпеки у військовому контексті. Центр відносить кібератаки до гібридної агресії і визначає загрози «сірої зони конфлікту», коли атаки не перетинають межі відкритого військового протистояння, але серйозно впливають на мережі державного управління.

Вартий уваги також внесок Європолу, який зосередився на взаємозв'язку між кіберзлочинністю та проксі-акторами, що діють від імені держав. Протягом 2022-2023 років Європол відстежував діяльність таких угруповань, як KillNet, які здійснювали DDoS-атаки на європейську інфраструктуру з метою тиску [44] [46] [53].

Стратегічне бачення, представлене у звітах Центру стратегічних і міжнародних досліджень (CSIS), є актуальним, оскільки кібервійна розглядається не лише як технологія, а й як політичний процес, що змінює принципи міжнародної безпеки. Звіти CSIS підкреслюють взаємозалежність країн у кіберпросторі, що робить навіть локальні конфлікти глобальними проблемами [30; 94].

Академічні дослідження в галузі кібербезпеки, особливо після конфлікту в Україні, набули особливої актуальності після 2014 року і особливо після російського тотального вторгнення у 2022 році. В європейській академічній традиції домінують дослідження, які поєднують національну безпеку, інституційну реакцію ЄС та розвиток нормативно-правової бази з питань кіберзахисту. Зокрема, Сметс у роботі «Без коротких шляхів: Чому держави борються за створення військових кібервійськ» досліджує складність розбудови національних кібервійськ, зосереджуючись на відсутності міжгалузевої координації та труднощах перетворення цифрового потенціалу на стійку інституційну безпекову спроможність. Цей підхід відповідає концепції цифрового суверенітету Бергеля. Його аналітичні джерела вказують на те, що кібербезпека ЄС – це не лише питання захисту технічної інфраструктури, а й політика відмежування від зовнішньополітичного впливу, особливо з боку США і Китаю, шляхом створення «цифрових кордонів» в Європі [97].

Крейг та Валеріано у своїй праці «Реалізм та кіберконфлікт: безпека у цифрову еру. Реалізм на практиці» досліджують особливості ведення інформаційних війн у сучасну епоху, коли реалізм стає все більше значущим та практичнішим у сфері вирішення міждержавних та міжрегіональних конфліктів. Цей підхід дослідження дозволяє вказати на те, що потрібно адаптуватись і враховувати нові ризики ведення нових типів війн і як на це необхідно реагувати. Кібербезпека стає питанням не лише захисту інфраструктури держави, а і захисту державних інтересів, суверенітету [27].

У своїй роботі Сантос застосовує теорію сек'юритизації до кібербезпеки, ілюструючи, як інформаційні загрози політизують політичну мову, перетворюючи кіберподії на історії про загальноєвропейську загрозу, що вимагає інституціоналізованої відповіді [91].

Українські академічні дослідження в основному зосереджені на прикладних і правових питаннях. Роботи Гнатюка, Савчука та Давимуки досліджують сферу національної кіберполітики, спроби її регулювання з 2017 року, а також роль України як лабораторії для тестування гібридних операцій,

що покладає на неї відповідальність стати «цифровим щитом» для Європи. Іншим важливим елементом української джерельної бази є діяльність Національного інституту стратегічних досліджень, Ради національної безпеки і оборони та Центру протидії дезінформації, які визначають оперативні наслідки російських кібератак, окреслюючи їх вплив на політичну стабільність, енергетичну безпеку та цифрову економіку. [3] [4] [12] [13]

З 2022 року досвід реальних кібератак в Україні став сферою емпіричних спостережень для дослідників, переводячи прикладний етап досліджень у теоретичні рамки. Компанія Microsoft зробила важливий внесок у цю сферу у своєму звіті «Захищаючи Україну: Перші уроки кібервійни» [65], в якому вони задокументували такі відомі атаки, як FoxBlade, Industroyer2 та Prestige. Ці кібероперації, спрямовані на дестабілізацію уряду, продемонстрували безпрецедентний рівень координації між російськими кібератаками та політичним і військовим керівництвом Росії. Атака Industroyer2 у квітні 2022 року на українські електропідстанції стала одним з перших подібних інцидентів у світі, коли код у цифровій сфері був використаний в активному збройному конфлікті, синхронізованому з обстрілом об’єкта. [54] [89]

Групи APT – APT28 (Fancy Bear), APT29 (Cozy Bear) та Sandworm – згадуються в різних дослідженнях як найпоширеніші державні хакерські групи, які атакували урядові та інфраструктурні об’єкти в Україні, а згодом і в ЄС. Вони були причетні до вторгнення в комп’ютерні системи, а також до використання вразливостей нульового дня, за допомогою яких їм вдавалося непомітно проникати у високозахищені системи.

Однією з найвідоміших атак стала атака на супутникову мережу KA-SAT ввечері 24 лютого 2022 року. Ця атака набуває все більшого значення не лише як кібератака, але і як доказ того, що кібератака синхронізувалася з початком вторгнення, демонструючи новий ступінь інтеграції військової та кібервійни [96].

Кіберполітики та програми Європейського Союзу лише нещодавно зазнали величезних змін – від риторичної політики до реальних оперативних

інструментів втручання, фінансування та співпраці по всьому світу. Перед обличчям зростаючої загрози з боку держав-агресорів, головним з яких є Російська Федерація, та в умовах посилення цифрового взаємозв'язку з країнами-партнерами ЄС випереджаючими темпами розбудовує інституційну спроможність за допомогою спеціально розроблених програм та інструментів. Однією з таких пріоритетних ініціатив є Постійна структурована співпраця у сфері оборони (PESCO), яка передбачає розробку спільних проектів для посилення спроможностей країн-членів, в тому числі у сфері кіберзахисту [57] [62]. Саме в такому контексті були організовані Кібернетичні групи швидкого реагування (Cyber Rapid Response Teams, CRRT) – групи швидкого кібернетичного реагування, які можуть бути швидко розгорнуті для реагування на атаки країн-членів і партнерів, таких як Україна. Розгортання CRRT на запрошення України в перші дні широкомасштабного російського вторгнення стало безпрецедентним прецедентом глобальної кібер-єдності. Це доповнюється архітектурою CyCLONe (Cyber Crisis Liaison Organisation Network), яка забезпечує координаційний центр між національними кіберцентрами під час серйозних атак, щоб держави могли узгоджувати міжгалузеві операції на стратегічному рівні.

Фінансову підтримку кіберпрограмам надає програма «Цифрова Європа» – власна програма Європейської Комісії, спрямована на розвиток цифрових навичок ЄС, таких як штучний інтелект, обробка даних, кібербезпека та цифрові навички. Україна, як країна-лідер-партнер після 2022 року, отримала доступ до цього інструменту, за допомогою якого їй дозволено брати участь у конкурсах на фінансування кіберпроєктів разом з європейськими інституціями. Ця програма не лише сприяє гармонізації технічних стандартів, а й є інструментом стратегічної інтеграції України до цифрового ринку ЄС [104].

Методологічна база дослідження кібербезпеки в ЄС формується на перетині кількох наукових парадигм. Зокрема, однією з найважливіших теоретичних основ є теорія сек'юритизації Копенгагенської школи, згідно з якою проблема стає безпековою лише тоді, коли вона представлена сильним актором

як екзистенційна загроза. Тут кібератаки та кіберзагрози розглядаються не як виключно технічна подія, а як ситуація, що потребує політичної та правової реакції, мобілізації ресурсів та адаптації нормативно-правової бази. На практиці це підтверджується прийняттям Європейським Союзом Акту про кіберсолідарність, а також різними спільними заявами ЄС щодо кібератак, які відображають політичну інституціоналізацію цифрової загрози.

Реалістичні та неореалістичні стратегії також застосовуються при аналізі кібервійни, особливо в контексті геополітичних конфліктів. Теорії державної влади, балансу загроз та конкуренції за вплив дозволяють розглядати кібер-активність як новий рівень конфлікту, де держави діють через проксі-групи, не переходячи при цьому поріг відкритої війни. Такий підхід пояснює природу кібератак Росії на Україну та ЄС як форму асиметричного тиску, що не підпадає під юрисдикцію прямого збройного конфлікту, але має стратегічний вплив.

У свою чергу, ліберальний інституціоналізм пропонує розглядати кібербезпеку як продукт взаємозалежності, співпраці та інституціоналізації. ЄС, як приклад наднаціональної моделі інтеграції, застосовує цей підхід: через встановлення стандартів, платформ для обміну інформацією та взаємного реагування. Фундаментальною в цьому процесі є робота таких організацій, як CERT-EU, CSIRTs Network і ENISA, які не обов’язково є оборонними установами, а скоріше суб’єктами транснаціонального співробітництва, що працюють на основі спільних стандартів. [26] [28] [50]

Моделі мережевої безпеки, засновані на концепції взаємозалежності та вразливості складних цифрових мереж, дозволяють аналізувати каскадні збої – коли атака на одну точку створює лавиноподібний ефект для всієї мережі. Як це сталося під час атак на енергетичну інфраструктуру України або супутникову угруповання KA-SAT, такий ефект став реальністю. Вразливість інформаційних систем, які базуються на централізованій або занадто сильно пов’язаній мережі, робить шлях децентралізації та цифрової незалежності факторами стійкості більш актуальними.

Методологічно дослідження кібербезпеки має поєднувати системний аналіз архітектури кібербезпеки, порівняльно-правовий аналіз регуляторних підходів в ЄС та Україні, інституційний аналіз ролі зацікавлених суб'єктів, таких як ENISA або CyCLONe, та емпіричний підхід на основі вивчення конкретних інцидентів [41]. Міждисциплінарність стає не просто перевагою, а методологічним імперативом, адже лише перетин правових, політичних, технічних та соціальних знань дозволяє адекватно досліджувати феномен кіберзагрози та створювати адекватні безпекові рішення. В умовах гібридної війни, розв'язаної Росією проти України, межа між воєнними діями, кібератакою та інформаційною операцією стає розмитою. Це вимагає наукового опрацювання з такою ж глибиною та гнучкістю, як і сучасна безпекова політика Європейського Союзу.

Висновки до першого розділу

Узагальнюючи теоретико-методологічні основи, слід зазначити, що кібербезпека постає як комплексне й поліцентричне явище, що охоплює юридичні категорії, політичні механізми, технологічну динаміку й соціальні наративи. Поняття, які фігурують у дослідженні – кіберзагроза, кібератака, кіберстійкість, критична інформаційна інфраструктура – мають чітко виражений правовий і функціональний зміст у нормативних документах ЄС і України. Їхня теоретична інтерпретація ґрунтується на концепціях сек'юритизації, теоріях міжнародних відносин, мережевих ризиків і європейській парадигмі resilience. Методологічно дослідження базується на системному, порівняльному, емпіричному, інституційному й міждисциплінарному підходах. Вибір цих підходів є виправданим з огляду на комплексність об'єкта дослідження та потребу адекватно відтворити взаємозв'язки між кіберпростором, політикою, правом, війною й транснаціональними процесами. Саме таке розуміння забезпечує глибину аналізу в подальших розділах цієї роботи. Хронологічні межі дослідження охоплюють період з 2014 до 2025 року – від початку гібридної агресії РФ проти України до повномасштабної війни та активної інтеграції України у кіберполітику ЄС. Географічно аналіз охоплює простір Європейського

Союзу як спільноти держав із уніфікованою політикою у сфері кібербезпеки, а також Україну як партнера, що поступово адаптує європейську модель і одночасно слугує випробувальним полем для міжнародних механізмів кіберреагування.

РОЗДІЛ ІІ. ВПЛИВ РОСІЙСЬКО-УКРАЇНСЬКОЇ ВІЙНИ НА КІБЕРБЕЗПЕКУ ЄС

2.1. Кіберагресія Росії як елемент гібридної війни та її вплив на безпеку ЄС

Російська Федерація послідовно застосовує кіберагресію як складову гібридної війни, поєднуючи кібератаки з військовими діями та інформаційно-психологічними операціями. Ще з часів конфліктів у Грузії (2008) та Україні (2014) російські хакери, пов'язані з державою, проводили атаки на урядові мережі, електромережі та медіа з метою дестабілізації обстановки. Повномасштабне вторгнення РФ в Україну у лютому 2022 року підтвердило цю тактику: за даними Європейського агентства з кібербезпеки (ENISA), інформаційні маніпуляції та кібератаки стали ключовими елементами російської агресії проти України [85].

Гібридна війна в російському розумінні передбачає досягнення військово-політичних цілей нижче порогу формального воєнного конфлікту з НАТО. Це означає, що кіберудари й інші таємні операції проводяться таким чином, щоб ускладнити атрибуцію та уникнути прямої дії у відповідь з боку Заходу. Згідно з аналізом НАТО CCDCOE, Росія свідомо обмежує масштаб своїх кібероперацій проти НАТО, уникаючи «гру» на рівні, який міг би спровокувати колективну оборону за статтею 5 Альянсу [18]. Такий підхід дозволяє РФ завдати шкоди й тиску противнику, не переходячи межі, після якої кібератака була б розцінена як збройна агресія. Це підтверджує і досвід останніх років: жоден з кіберінцидентів у країнах НАТО досі не призвів до задіяння статті 5, оскільки завдана шкода залишалася обмеженою та розмитою за походженням [77].

У ході війни проти України Росія розгорнула широкий спектр кіберзасобів, тісно пов'язаних із воєнними діями на фізичному фронті. У період підготовки до вторгнення (січень–лютий 2022 р.) фіксувалися багаторазові зламування українських державних інформаційних систем, встановлення wiper-шкідників (знищувальних програм) і дефейс вебсайтів. Зокрема, 23 лютого 2022 р. – за

кілька годин до перших ракетних ударів – було зафіксовано масовану атаку шкідливого ПЗ на урядові комп'ютери України («FoxBlade» за класифікацією Microsoft) [65, с. 32-35]. Одночасно відбулася атака на супутникову мережу Viasat, що вивела з ладу тисячі модемів супутникового інтернету в Україні і навіть в деяких країнах ЄС [58]. Цей скоординований кіберудар був спрямований на порушення зв'язку та став частиною початкового наступу. Загалом, перші тижні вторгнення супроводжувалися хвилею деструктивних кібератак: у січні-березні 2022 року в Україну було націлено щонайменше 37 деструктивних кібероперацій (наприклад, віруси-вайпери WhisperGate, HermeticWiper), які знищували дані на сотнях комп'ютерів організацій [61].

За рік після вторгнення фахівці нарахували сотні випадків кіберагресії в контексті російсько-української війни. Згідно зі звітом CERT-EU, з січня 2022 по лютий 2023 було зафіксовано 806 кібератак, пов'язаних із війною. Ці атаки були спрямовані не лише проти України, але й проти союзників України. Аналітики поділяють їх на кілька основних типів [88].

Деструктивні атаки (знищення даних) – застосування вірусів-вайперів і псевдо-вимагачів, які знищують дані або виводять з ладу системи. У перші місяці війни такі атаки (наприклад, CaddyWiper, IsaacWiper) вражали українські держустанови та енергетику. Попри побоювання, аналогічних випадків проти об'єктів у країнах ЄС не зафіксовано, що свідчить про обережність РФ у розширенні деструктивних кіберударів на НАТОвські держави [101, с. 788-792].

Кібершпигунство та проникнення в мережі – спроби отримати несанкціонований доступ до інформаційних систем для розвідки або саботажу. Російські державні хакерські групи (такі як APT28 (Fancy Bear), APT29 (Cozy Bear), Sandworm тощо) активізували фішингові кампанії та використання вразливостей нульового дня для проникнення в урядові і військові мережі України, а також для кібершпигунства за країнами НАТО. Зокрема, у квітні 2022 р. група Sandworm здійснила спробу знеструмити частину енергосистеми України за допомогою шкідника Industroyer2, поєднавши кіберпроникнення зі

знанням критичної інфраструктури. Подібні атаки потребують високої координації з воєнними цілями та глибокої підготовки [18].

Атаки типу “hack-and-leak” та інформаційні операції – викрадення конфіденційної інформації з подальшим оприлюдненням для пропагандистського ефекту. Російські спецслужби використовували злами електронної пошти та серверів для отримання даних, які потім публікувалися в мережі з метою дискредитації українських посадовців чи західних партнерів. Такі кібероперації часто є складовою інформаційно-психологічних операцій. Наприклад, у березні 2022 року було зламано акаунти українських посадовців у соцмережах і поширено діпфейкове відео про нібито капітуляцію України – ця акція поєднала кібервзлом і психологічну атаку. Аналогічно, у червні 2022 група, імовірно пов’язана з ГРУ РФ, зламала переписку військового командування України; викрадені листи оприлюднили з пропагандистськими коментарями [98].

Цілеспрямовані кампанії дезінформації – кібератаки тісно переплетені з інформаційною війною. Росія проводить активні інформаційно-психологічні операції: створює та поширює фейки, пропагандистські наративи в соцмережах, маніпулює громадською думкою через бот-мережі. Кібератаки на медіаресурси чи соцмережеві акаунти часто служать для розміщення дезінформації. Такі операції мають на меті підірвати моральний дух населення, посіяти паніку або послабити підтримку України з боку союзників. Наприклад, у 2022 році російські кіберпідрозділи неодноразово зламували регіональні новинні сайти в Україні та розміщували фейкові «новини» про втечу керівництва чи капітулянтські заяви. Цей напрям є настільки значущим, що фахівці відзначають: інформаційна маніпуляція стала однією з ключових складових російської стратегії війни, нарівні з кібернетичними та військовими засобами [63].

Хоча інтенсивність російських кібератак проти України суттєво зросла з початком вторгнення, їхній ефект залишився підтримувальним, а не вирішальним у загальному ході війни. На це вказують як українські успіхи у швидкому відновленні роботи систем після атак, так і оцінки аналітиків.

Дослідження Центру стратегічних і міжнародних досліджень (CSIS) показало, що попри збільшення кількості атак, у 2022–2023 рр. не спостерігалося якісного стрибка в їх руйнівності чи зміні типових цілей [30]. Інакше кажучи, Росія використовувала кібероперації за відпрацьованим шаблоном – для саботажу, розвідки та пропаганди – але не наважилася або не змогла завдати кіберударів, які б призвели до стратегічного перелому на полі бою. Ці висновки узгоджуються з думкою, що кіберзброя в сучасному великомасштабному конфлікті відіграє роль допоміжного засобу: вона може тимчасово дезорганізувати, зібрати розвіддані чи вплинути на інформаційне поле, але не замінює собою прямої кінетичної сили на фронті [30]. Водночас, значення кіберфронту не можна недооцінювати – він створює постійний тиск та відкриває "другий фронт" у кіберпросторі, який потребує від держав жорсткої кібероборони.

Кібервійна, розв'язана Росією проти України, відгукнулася широкими хвилями в кіберпросторі Європейського Союзу. Масштабні атаки не обмежилися територією безпосереднього конфлікту – під удари потрапили й країни ЄС, особливо ті, що активно підтримують Україну. За даними CERT-EU, кібератаки, пов'язані з війною, за рік зачепили щонайменше 23 країни ЄС. Найчастіше ціллю ставали держави на сході Європи – Польща, Латвія, Естонія, Литва – тобто країни, що межують з РФ і відкрито підтримують Київ зброєю та політично. Це відображає прагнення Кремля покарати та залякати сусідів, які допомагають Україні, через кібернетичні засоби [46].

Найпоширенішим видом ворожої активності проти ЄС стали DDoS-атаки та атаки з боку проксі-хактивістів. Так звані «групи хактивістів» на кшталт KillNet, NoName057(16) та інші, що відкрито декларують проросійські погляди, з кінця лютого 2022 р. регулярно організовували кампанії атак на європейські вебресурси. Ці напади координувалися через Telegram-канали та форуми, де учасники отримували інструкції атакувати певні цілі – зазвичай сайти державних установ, транспортних компаній, банківського сектору чи медіа в країнах ЄС. Наприклад, у травні 2022 року група KillNet взяла на себе відповідальність за

збій роботи веб-сайтів низки італійських державних органів після того, як Італія підтримала санкції проти РФ. У червні 2022 проросійські хакери атакували сайти уряду Литви на знак «помсти» за обмеження транзиту до Калінінграда. Часто такі DDoS-кампанії прив'язані до конкретних подій: у 2023 р. під удари KillNet та групи NoName057 потрапляли сайти аеропортів, парламентів та компаній Польщі, Німеччини, скандинавських країн – особливо після рішень про військову допомогу Україні або прийняття історичних рішень (наприклад, вступ Фінляндії до НАТО супроводжувався кібератакою на вебсайт фінського парламенту). Europol відзначив, що війна спричинила помітний сплеск DDoS-активності проти європейських цілей, причому найбільш масовані атаки були чітко політично мотивовані та координувалися про-російськими групами. Хоч DDoS-атаки не завдають довготривалих пошкоджень інфраструктурі, вони вимушують уряди підвищувати готовність, а суспільство – усвідомити реальність кіберзагрози [6].

Другим напрямом російської кіберагресії, який позначився на безпеці ЄС, стали цілеспрямовані атаки на критичну інфраструктуру та бізнес за межами України. Хоч масштабних руйнівних кібератак на об'єкти в ЄС Росія поки уникала, були випадки, які викликають занепокоєння. Знаковим інцидентом став вже згаданий напад на супутникову мережу KA-SAT (Viasat) 24 лютого 2022 року. Первинною мішенню була Україна – російські хакери намагалися вивести з ладу військовий зв'язок на базі супутникового інтернету. Проте ця атака мала побічний ефект для Європи: вірус відключив близько 5800 терміналів супутникового зв'язку у Польщі, Італії, Німеччині та Франції, зокрема зупинив роботу дистанційно керованих вітрових турбін у Німеччині. Таким чином, кібератака у війні спричинила технологічний збій у кількох державах ЄС, продемонструвавши транскордонний характер загроз у кіберпросторі. Інший випадок – операція "Prestige": у жовтні 2022 р. російська хакерська група (ідентифікована Microsoft як Iridium, пов'язана з угрупованням Sandworm) одночасно атакувала компанії транспортної сфери в Україні та Польщі, встановивши шкідливе програмне забезпечення типу "псевдо-вимагач", що

шифрувало дані. Ця атака була спрямована на логістичні ланцюги постачання допомоги Україні і показала, що російські кібершпигуни можуть націлюватися на компанії в державах ЄС, пов'язані з підтримкою України. На щастя, значної шкоди вдалося уникнути, але сам факт такої операції сигналізує про ризики для критичної інфраструктури Європи [3].

У травні 2023 року німецька служба кібербезпеки BSI попередила про активізацію російської групи APT28 проти німецьких об'єктів критичної інфраструктури – зловмисники маскували шкідливий код під оновлення ПЗ для інженерних систем. Хоч успішних руйнівних атак не зафіксовано, такі інциденти тримають європейські країни у напруженні, адже демонструють намагання російських хакерів проникнути в ключові системи життєзабезпечення [19].

Окремо варто згадати операції російських спецслужб з дезінформації та впливу на суспільство ЄС, які доповнюють кібернетичні атаки. Москва тривалий час веде інформаційну війну в Європі, намагаючись розколоти єдність Заходу та підірвати підтримку України. З початком вторгнення ці зусилля активізувалися: російські пропагандистські наративи (заперечення воєнних злочинів, звинувачення НАТО в «провокації конфлікту», нагнітання теми енергетичної кризи через санкції тощо) поширювалися багатьма мовами ЄС у соціальних мережах і через маргінальні медіа. Кіберінструменти тут відіграють допоміжну роль – злами акаунтів європейських політиків, фальшиві листи від їх імені, створення фейкових сайтів новин для вкидання дезінформації. Зафіксовано операції російських інформаційних агентів, націлені на аудиторії в Польщі та країнах Балтії: зловмисники через фейкові сторінки в Facebook та Twitter поширювали неправдиві історії (наприклад, про корупцію в постачанні західної зброї Україні) польською, литовською та латвійською мовами. Метою було посіяти сумніви серед громадян цих країн щодо доцільності підтримки України. Такі інформаційно-психологічні операції становлять не меншу загрозу для безпеки, ніж технічні кібератаки, оскільки вони впливають на суспільну стабільність і політичну єдність ЄС [11, с. 3-7].

Таким чином, російська кіберагресія в контексті війни проти України створила для Євросоюзу новий вимір загроз. В ЄС фактично сформувався «фронт кіберпростору», на якому державні й недержавні prorosійські актори атакують європейські цифрові ресурси. Це змусило країни ЄС переглянути свої підходи до кібербезпеки і активізувати спільні дії для захисту мереж. Важливо, що попри часті атаки, їх реальний вплив поки залишався керованим: завдяки підвищеній готовності систем, міжнародній допомозі (в т.ч. від приватних корпорацій як Microsoft, яка допомагала виявляти та нейтралізувати загрози) та своєчасному обміну інформацією, вдалося уникнути катастрофічних кіберінцидентів на території ЄС у 2022–2023 роках. Проте ця відносна успішність оборони не зменшує серйозності викликів, а скоріше підкреслює необхідність подальшого зміцнення кіберстійкості.

Події 2022–2023 років показали, що кіберпростір став ареною геополітичного протистояння, і Європейському Союзу слід розвивати кібероборону так само системно, як і традиційну безпеку. Майбутні виклики для кібербезпеки ЄС у контексті глобальних ризиків і триваючої агресії РФ охоплюють декілька ключових напрямів.

Зростання державних кіберзагроз і необхідність колективного захисту. Росія залишається однією з головних джерел кібератак на західні країни. Її діяльність стимулювала й інші держави активізувати кіберпрограми – наприклад, Китай нарощує кібершпигунство та спроможності атак на критичну інфраструктуру, що викликає занепокоєння у НАТО. У такій ситуації ЄС повинен бути готовим до багатоаспектних загроз від різних державних акторів. Війна в Україні продемонструвала важливість міжнародної координації в кіберзахисті: українські системи вистояли значною мірою завдяки об’єднаним зусиллям урядів і приватних компаній (наприклад, перенесення українських даних у захищені хмари Microsoft/Amazon, надання компанією SpaceX терміналів Starlink для резервного зв’язку тощо). Для ЄС це означає, що модель колективної кібероборони, залучення широкого кола партнерів та обміну інформацією – критично необхідні. Перспективною ініціативою в цьому напрямі

є створення Європейського центру спільного кіберпідтримання (Joint Cyber Unit) – платформи, анонсованої Єврокомісією, де експерти з держав-членів зможуть разом реагувати на масштабні кібератаки [56, с. 165-169]. В 2023 році також було вперше задіяно кіберрезерв ЄС для допомоги Україні: фахівці з Литви, Польщі та інших країн у складі кіберсил швидкого реагування ЄС (EU Cyber Rapid Response Team) консультували українські органи щодо нейтралізації російських шкідливих програм. Цей досвід колективного реагування, ймовірно, стане прообразом майбутніх спільних операцій з кібероборони в ЄС [17, с. 3-6].

Захист критичної інфраструктури та економіки від кібератак. Енергетика, транспорт, фінансовий сектор, охорона здоров'я – всі ці сфери в Європі стали потенційними цілями у світлі загроз, проявлених війною. Хоч прямі руйнівні атаки РФ на європейські об'єкти були поодинокими, ризик залишається високим. Не можна забувати урок NotPetya (2017) – російська кібератака проти України, що паралізувала порти, заводи і офіси по всьому світу та завдала збитків на ~$10 млрд [106]. Цей випадок показав, що навіть якщо атака націлена на одну країну, шкідливе ПЗ може поширитися глобально через взаємопов'язаність систем. У 2024–2025 роках особливий виклик становитиме захист енергетичної інфраструктури Європи, зважаючи на гібридні дії РФ (у 2022 р. було здійснено диверсію на газопроводі «Північний потік»). У кіберпросторі це може означати спроби атак на електромережі, газорозподільчі станції, системи керування нафтопроводами. ЄС вже реагує нормативно: ухвалено оновлену Директиву NIS2 (2022), яка зобов'язує держави-члени посилити кібербезпеку об'єктів критичної інфраструктури та запровадити жорсткіші вимоги до стійкості мереж. Також можна згадати Директиву про стійкість критичних суб'єктів (CER Directive) 2022 р. яка набула чинності 16 січня 2023 року.

В січні 2023 року створено робочу групу ЄС-НАТО з питань стійкості критичної інфраструктури, яка вже 29 червня 2023 року підготувала остаточний звіт про оцінку захисту критичної інфраструктури, у якому описано поточні виклики безпеці та представлено цільові рекомендації щодо посилення стійкості критичної інфраструктури. Група досліджує чотири ключові сектори

(енергетика, транспорт, цифрова інфраструктура та космос), а також міжгалузеві міркування.

Рекомендація, прийнята Радою Європейського Союзу 25 червня 2024 року, містить план критичної інфраструктури ЄС. Проект тексту було прийнято Європейською Комісією 6 вересня 2023 року. Рекомендацію було прийнято Радою Європейського Союзу 25 червня 2024 року та опубліковано в Офіційному журналі 5 липня 2024 року

Протидія кіберзлочинності та зловмисникам, що діють під “парасолькою” держав. Гібридна агресія РФ проявила ще одну тенденцію: розмиття меж між державними хакерами та кіберзлочинними угрупованнями. Російські рандсомваре-банди та інші кримінальні групи часто діють із мовчазної згоди влади, атакуючи західні компанії. Війна посилила цей тренд – частина кіберзлочинців стала на бік Кремля (так з’явилися “хактивісти” типу KillNet), інші ж скористалися хаосом для власного збагачення. Europol застерігає, що через війну деякі російські кіберзлочинні синдикати перемістилися в інші юрисдикції та перегрупувалися, але вони як і раніше загрожують Європі. Наприклад, група Conti, відома атаками-вимагачами, у 2022 році офіційно підтримала дії РФ проти України; хоч її діяльність була припинена зусиллями міжнародної спільноти, колишні учасники перейшли в інші угруповання. Для ЄС пріоритет – посилити міжнародне правоохоронне співробітництво у відслідковуванні і припиненні дій таких суб’єктів. Перспективи включають активне застосування санкцій ЄС проти осіб і організацій, причетних до кібернападів (з 2020 р. ЄС має правовий механізм накладення санкцій за кібератаки – його вже застосовано проти російських громадян, причетних до зламу Бундестагу у 2015 та спроб кібератак на ОЗХЗ). У 2023 році очікується розширення санкційного списку на осіб, залучених до кіберагресії під час війни в Україні. Крім того, Europol та національні кіберполіції нарощують можливості із виявлення кіберзлочинців, що діють на території ЄС під чужим прапором – наприклад, виявлення російських агентів впливу чи хакерів, які працюють зсередини європейських країн.

Вдосконалення стратегії кібероборони та співпраці з НАТО. Вторгнення РФ стало каталізатором оновлення стратегічних документів у сфері кібербезпеки. У 2022 році було прийнято Стратегічний компас ЄС, який особливу увагу приділяє кіберзагрозам і передбачає створення повноцінної системи кібероборони Євросоюзу [4]. До 2025 року ЄС планує реалізувати низку ініціатив: створення мережі оперативних центрів безпеки (SOC) по всій Європі для обміну даними про інциденти в режимі реального часу; проведення регулярних кібернавчань за участі всіх держав-членів (вже у 2022 відбулися масштабні навчання Cyber Europe, сценарії яких моделювали кібератаки на енергетику та транспорт); запуск фонду для підтримки розвитку національних кіберсил. Паралельно НАТО також зміцнює кібероборонні позиції – в 2023 на саміті у Вільнюсі була схвалена концепція посилення внеску кіберзахисту в загальну стримувальну позицію Альянсу та запуск Virtual Cyber Incident Support Capability для допомоги країнам у разі серйозних кібератак. Більшість країн ЄС є членами НАТО, тому синергія між ЄС і НАТО в цій сфері є вирішальною [29]. Уже зараз відбувається тісна координація: обмін розвідданими про кіберзагрози, спільні тренування (напр. Locked Shields під егідою CCDCOE) [59], узгодження підходів до визначення, коли кібератака може становити загрозу колективній безпеці. Перспектива на майбутнє – вироблення спільної політики кіберстримування, тобто здатності не лише оборонятися, а й чітко окреслити потенційному агресору ціну кібератаки. Це складне завдання, адже традиційних механізмів стримування (як ядерне стримування) у кіберпросторі поки не існує. Проте формування міжнародних норм і чіткої позиції («кібератака з тяжкими наслідками матиме для винуватця наслідки у вигляді санкцій, відповідних контрзаходів чи навіть застосування статті 5 НАТО в екстремальному випадку») – є важливою складовою кібероборони. Тут ЄС разом з НАТО може відіграти провідну роль, просуваючи відповідальну поведінку держав у кіберпросторі на глобальних майданчиках (ООН, закріплення норм міжнародного права, притягнення до відповідальності за кіберзлочини).

Технологічні виклики та необхідність інновацій. Кібероборона – це динамічна сфера, де загрози швидко еволюціонують. Нові технології несуть як ризики, так і можливості. З одного боку, такі явища як штучний інтелект можуть бути використані нападниками для автоматизації атак, створення правдоподібних фішингових повідомлень або генерування масової дезінформації (напр. фейкових відео). Уже сьогодні спостерігається зростання складності соціальної інженерії з використанням AI, що ускладнює відрізнення правди від обману. З іншого боку, ті ж технології можуть стати інструментом захисників – для проактивного виявлення атак (AI для моніторингу аномалій трафіку), автоматичного закриття вразливостей, перекладу рутинних задач кібербезпеки на машини. Перспектива кібероборони ЄС включає інвестування в інновації: програми досліджень у сфері кібербезпеки (Horizon Europe фінансує відповідні проекти), підтримку стартапів, що розробляють засоби захисту нового покоління, створення загальноєвропейських платформ обміну аналітикою про загрози (Threat Intelligence). ENISA у своїх звітах наголошує, що для протидії державним кіберзагрозам Європі потрібна «стала кіберстійкість»: постійне удосконалення технологій захисту, підготовка кваліфікованих кадрів, розвиток культури кібергігієни в усьому суспільстві. Війна зробила ці тези не теоретичними, а дуже конкретними – від рівня захищеності серверів або, скажімо, надійності резервних каналів зв’язку може залежати не лише економіка, а й життя людей у кризовий момент.

Інформаційний фронт і психологічна стійкість. Гібридна агресія РФ проти України продемонструвала, що інформаційна війна є невід’ємною частиною сучасного конфлікту. Для ЄС це означає, що кібероборона має включати заходи проти інформаційно-психологічних операцій: виявлення та нейтралізацію дезінформаційних кампаній, підвищення стійкості суспільства до впливу фейків, захист демократичних процесів (виборів, референдумів) від маніпуляцій. ЄС уже зробив кроки в цьому напрямі – з 2015 року діє підрозділ EU vs Disinfo для моніторингу й викриття проросійської дезінформації. Після початку війни його активність зросла багатократно: лише за перші півроку повномасштабної війни

було ідентифіковано тисячі нових випадків дезінформації, пов’язаних із нападом РФ. Перспектива – посилення співпраці між платформами соціальних мереж і урядами ЄС щодо швидкого блокування ворожих інформаційних операцій, впровадження законодавчих вимог до великих онлайн-платформ (DSA – Акт про цифрові послуги ЄС) з прозорості алгоритмів, які можуть використовуватися для поширення шкідливого контенту. Врешті, психологічна стійкість громадян стає частиною національної безпеки: країни Балтії, маючи історичний досвід протистояння пропаганді, вже включили медіаграмотність і освіту з кібербезпеки в свої стратегії. Інші держави ЄС теж приділяють цьому увагу, розуміючи, що підготовлене інформаційно суспільство менш вразливе до зовнішніх впливів [37, с. 8-13].

Кіберагресія Росії проти України висвітлила нову реальність, у якій кіберпростір став полем бою між державами. Для Європейського Союзу це одночасно виклик і стимул до дії. Російські кібератаки як елемент гібридної війни безпосередньо вплинули на безпеку ЄС, продемонструвавши необхідність міцної колективної кібероборони. На 2024–2025 роки ЄС входить з набутим гірким досвідом і розумінням, що кіберфронт – це постійний фронт. Перспективи кібероборони Євросоюзу полягають у поглибленні співпраці (як всередині Союзу, так і з НАТО та глобальними партнерами), у вдосконаленні законодавства та інфраструктури кібербезпеки, а також у розвитку інноваційних підходів до протидії державним кіберзагрозам. В умовах глобальних ризиків – від агресивних дій авторитарних режимів до терористичних кібернападів – ЄС поступово формує цілісну систему реагування. Ставка робиться на стійкість: здатність запобігати більшості атак, швидко виявляти та нейтралізувати інциденти, мінімізувати шкоду і продовжувати функціонування навіть під натиском ворожих дій. Війна в Україні стала болісним, але важливим каталізатором цього процесу, висвітливши слабкі місця і водночас показавши, що об’єднаний кіберзахист здатен успішно протистояти навіть одній з найпотужніших кібердержав світу. Це означає, що майбутні виклики, хоч і

будуть значними, цілком можна подолати за умови збереження єдності, рішучості та інноваційного підходу Європейського Союзу у сфері кібербезпеки.

2.2. Кіберзагрози критичній інфраструктурі та цифровій безпеці ЄС

Критична інфраструктура (КІ) охоплює всі важливі сфери економіки та державного управління – енергетику, транспорт, зв'язок, охорону здоров'я, фінанси, державні послуги тощо. Їх оцифрування надало величезні переваги, але водночас зробило їх вразливими до атак з боку кіберзагроз. Останніми роками кібер-активність та кібератаки на комунікаційну інфраструктуру ЄС значно зросли. Одним з особливо помітних факторів стало повномасштабне вторгнення Росії в Україну в 2022 році, яке повністю змінило кіберландшафт. За даними Агентства ЄС з кібербезпеки (ENISA), кібервійна стала «п'ятим виміром» нової війни, а державні кібератаки на критичну інфраструктуру зросли в геометричній прогресії. З початком вторгнення очікувалася хвиля руйнівних кібератак на українську КІ, що могло мати катастрофічні наслідки для Європи. Хоча російські кібергрупи дійсно збільшили масштаби своїх операцій, до цього часу мало хто говорив про «кіберЧорнобиль». Однак таку відносну стриманість не слід трактувати як привід для самозаспокоєння – експерти прогнозують, що рівень кіберагресії проти України та її союзників у Європі залишатиметься на високому рівні, насамперед у вигляді атак на ланцюги поставок та інші непрямі цілі. Вже протягом другої половини 2022 року майже половина кібератак, пов'язаних з війною, була спрямована проти країн ЄС (порівняйте це з приблизно 10% атак на країни за межами України в перші місяці війни). Це свідчить про те, що агресор все частіше націлюється на європейський кіберпростір, намагаючись дестабілізувати роботу критично важливих служб, покарати за проукраїнські симпатії та вести кібершпигунство проти урядів країн-союзників.

Окрім державних суб'єктів (передусім Росії, а також Китаю та Ірану), загрозу для КІ становлять кіберзлочинні синдикати. Їхні операції, як правило, економічно мотивовані (наприклад, атаки програм-вимагачів, вимоги викупу за розшифрування даних), але можуть мати опосередкований вплив на життєво важливі послуги для населення. У 2021-2023 роках було чимало випадків, коли лікарні, трубопроводи або державні служби були виведені з ладу злочинними

хакерами. Цікаво, що протягом усієї війни існували злочинні угруповання, які переходили на бік Росії та політично націлювалися на об'єкти країн ЄС. Одним з таких прикладів є те, що з початку 2022 року проросійське угруповання KillNet влаштовувало цикли DDoS-атак на веб-ресурси державних установ, транспортних центрів та лікарень країн-членів НАТО, нібито на підтримку України. Таким чином, кібербезпека критичної інфраструктури ЄС сьогодні формується як під впливом геополітичних загроз (цілеспрямовані атаки з боку держав-агресорів та їхніх «хактивістів»), так і під впливом організованої кіберзлочинності з метою отримання прибутку або «заради справи» [70].

Далі буде розглянуто ситуацію в найважливіших сферах критичної інфраструктури ЄС з огляду на останні події 2022-2023 років та специфіку загроз для кожної з них.

Енергетичний сектор у минулому також був головною мішенню для кібератак через потенційну можливість спричинити масові перебої у постачанні електроенергії та газу. Для державних суб'єктів кібератаки на енергетичний сектор можуть бути інструментом шоку і дестабілізації, а для злочинних організацій – інструментом тиску з метою вимагання викупу, враховуючи нагальну потребу в безперебійній роботі енергетичних мереж. За останні кілька років європейські країни пережили неодноразові кіберподії у цій сфері. Україна отримала дуже відчутний досвід у 2015-2016 роках, коли її енергосистема зазнала кібератак (угруповання «Піщаний черв'як», пов'язане з російським ГРУ, завдавало ударів по підстанціях, спричиняючи відключення електроенергії) – перші у світі приклади успішного кібервтручання в роботу електромереж. У 2022 році, в період тотальної війни, російські кібератаки знову намагалися знеструмити Україну: навесні було знайдено та знешкоджено шкідливе програмне забезпечення Industroyer2, спрямоване на дестабілізацію енергосистеми. Атака не вдалася, але довела рішучість та технічні можливості ворога. Крім того, експерти прогнозують створення нових шкідливих інструментів для впливу на промислові системи: у 2023 році було виявлено зразок шкідливого програмного забезпечення COSMICENERGY [39, с. 67],

призначеного для відключення електроенергії шляхом дистанційного керування обладнанням електромереж.

Серйозні інциденти також були зареєстровані в ЄС. Найбільша в історії Данії кібератака на енергетичний сектор сталася в травні 2023 року: через уразливість мережевих пристроїв зловмисники скомпрометували мережі 22 регіональних енергетичних компаній одночасно. Зловмисникам вдалося зламати мережі компаній, і їм навіть довелося перейти в режим «острова» (тимчасове відключення від центральної мережі), щоб ізолювати інцидент, повідомляє данський Центр кіберзахисту критичної інфраструктури SektorCERT [68]. Незважаючи на історичний характер атаки, завдяки своєчасній реакції фахівців вдалося уникнути фактичних відключень, що свідчить про те, що європейська енергосистема має певний запас міцності. Водночас це показує реальну загрозу атаки: вона є повсякденним актом диверсії на енергосистему і може бути здійснена одночасно на десятки об'єктів. У січні 2022 року кібератака на IT-системи деяких нафтових і транспортних компаній у Німеччині та Нідерландах призвела до зупинки відвантаження нафтопродуктів у портах (таких як Гамбург і Роттердам) – хоча це була кримінальна атака з вимогою викупу, її вплив поширився на фізичне постачання енергії. Примітно, що Європейська комісія відзначає збільшення кількості інцидентів в енергетичному секторі: лише у 2023 році у світі було зафіксовано понад 200 кібератак на енергетичний сектор, і більше половини з них вразили європейську інфраструктуру. Виною тому як активність проросійських хакерів (у відповідь на санкції проти Росії та допомогу Україні), так і загальне зростання кібератак на промислові мережі [73].

Окремо слід згадати інцидент із супутниковим зв'язком Viasat у перший день вторгнення (лютий 2022 року), який, хоч і був пов'язаний з телекомунікаціями, але мав глибокий вплив на енергетичний ринок ЄС. Російська кібератака знищила наземні модеми супутникового інтернету KA-SAET, відключивши тисячі українських клієнтів від мережі. Атака також мала транскордонні наслідки, оскільки в Німеччині понад 5800 вітрових турбін були дистанційно вимкнені з центрів управління. Хоча самі турбіни все ще були здатні

виробляти електроенергію, оператор був змушений підтримувати їх у робочому стані вручну, що демонструє вразливість навіть віддаленого аспекту енергетичної інфраструктури до «непрямих» кібератак. Це один з таких випадків, коли атака на канал зв'язку фактично була спрямована на енергетичний сектор – класична демонстрація міжгалузевого характеру цифрової безпеки КІ.

В умовах зростаючих загроз ЄС робить особливий акцент на захисті енергетичного сектору. Спільно з представниками енергетичних компаній та урядовими групами реагування проводяться кібернавчання. Зокрема, у червні 2024 року відбулися великі навчання «Кібер Європа 2024», де відпрацьовувався сценарій кібератаки на енергетичну інфраструктуру Європи. Ці заходи покликані підвищити готовність до кризових ситуацій та розробити механізми координації дій у разі реальної атаки на енергосистему [73]. Крім того, застосовуються нові регуляторні вимоги – згідно з Директивою NIS2 (2022), роздрібні торговці електроенергією та інші критичні підприємства повинні посилити заходи кібербезпеки та звітувати про інциденти, а Директива про стійкість критичних об'єктів (CER) вимагає від держав оцінювати загрози для енергетичних об'єктів та вживати заходів для захисту від кібер- та фізичних атак. Метою є створення багаторівневої системи безпеки, здатної протистояти як поодиноким атакам, так і гігантським кампаніям проти енергетичної інфраструктури ЄС.

Транспортна інфраструктура – ще один стратегічно важливий сектор, що зазнає зростаючого кібертиску. Аеропорти, залізниці, морські порти та логістичні центри залежать від складних ІТ-систем для обробки транзиту пасажирів і вантажів, і будь-яке порушення роботи цих систем має негайний вплив на економіку та безпеку. Для держав-агресорів кібератаки на транспорт є засобом зриву поставок військової та гуманітарної допомоги, а для злочинців – можливістю отримати викуп або здійснити крадіжку (наприклад, контрабандисти зламують портові системи для контрабанди товарів) [22, с. 3].

У російсько-українському конфлікті кібератаки на транспорт стали частиною ширшої стратегії дестабілізації. Жовтень 2022 року: Під час бойових дій в Україні з'явилася нова програма-вимагач Prestige, яка майже одночасно

вразила комп'ютерні мережі кількох логістичних і транспортних фірм в Україні та Польщі. Корпорація Майкрософт поклала відповідальність за атаку на російське угруповання (яке називає себе «Ірідіум») і розглядає її як спробу порушити ланцюги поставок у сусідніх з Україною областях. Програма-вимагач Prestige зашифрувала дані на комп'ютерах компаній і залишила записку з вимогою викупу, але очевидно, що грошовий аспект був вторинним – атака мала репресивний і військовий характер, а її метою було порушення роботи транспорту. Ця подія довела, що транспортна мережа союзників України також є вразливою: під удар може потрапити не лише власне Україна, а й навіть транзитні пункти в ЄС, які є основою її постачання [64].

Ще один показовий епізод стався у серпні 2023 року в Польщі. Анонімні хакери вивели з ладу не ІТ-мережі, а систему радіозв'язку залізниці, скориставшись недоліком у процедурі аварійної зупинки. На північно-західних залізницях Польщі вони передали сигнал, що імітував запит на екстрену зупинку, і навіть увімкнули по службовому радіо фрагменти російського гімну. В результаті було зупинено одночасно близько 20 поїздів, які перебували в дорозі. Це був свідомий саботаж, вважає польська влада – поліція затримала двох осіб, підозрюваних у проросійському саботажі на залізниці. Хоча використана технологія була дуже примітивною (радіопередавач і знання коду сигналу), результати були реальними: рух поїздів на деяких ділянках зупинився на кілька годин. Включення російського гімну та промови зловмисників свідчать про політичну мотивацію, оскільки вони демонстрували підтримку агресії та залякування [55]. Цей випадок довів, що така транспортна інфраструктура може бути порушена не лише кібер-вірусами, але й втручанням у пристрої управління та зв'язку, які зазвичай не мають належного захисту. Польські експерти зрозуміли, що ці події свідчать про наявність довгострокових проблем з безпекою в інфраструктурі залізничної системи та необхідність приведення її у відповідність.

Кібератакам піддаються й інші види транспорту. За останні два роки європейські аеропорти неодноразово ставали мішенню DDoS-атак, переважно з

боку проросійських хактивістів. Наприклад, у 2023 році угруповання KillNet оголосило, що «карає» країни, які підтримують Україну, атакувавши веб-сайти деяких найважливіших аеропортів та авіакомпаній Німеччини, Нідерландів та скандинавських країн (у більшості випадків це було лише тимчасове закриття веб-сайтів та систем бронювання). Морські порти також потрапляють під пильну увагу: рік тому, у 2017 році, кібератака вірусу NotPetya (яка спочатку була спрямована на українські компанії) паралізувала роботу данського судноплавного гіганта Maersk, спричинивши затримки в портах по всьому світу, включаючи Роттердам. У 2022-2023 роках безпосередньо державних кіберсаботажів проти європейських портів не було, але небезпека залишається реальною – спецслужби ЄС посилюють безпеку портових систем, згадуючи про випадки глушіння GPS і шпигунських програм, виявлених уздовж основних морських шляхів [47, с. 34-38].

Варто зазначити, що кіберстійкість транспортного сектору також стає предметом інтересу на законодавчому рівні. Нові правила Директиви NIS2 поширюються на транспортних операторів (залізничних, повітряних, водних, автомобільних) і вимагають від них забезпечення кібербезпеки та обміну інформацією про інциденти. Крім того, ЄС і НАТО проводять навчання з кіберзахисту транспортної інфраструктури. Метою цих зусиль є запобігання обставинам, за яких кібератака призведе до зупинки, наприклад, європейської залізничної системи або послуг з управління повітряним рухом. Адже її наслідки відчують мільйони громадян, а її вплив вийде далеко за межі кіберсвіту.

Телекомунікаційна галузь є основою нової цифрової економіки, яка пов’язує між собою всі інші галузі. Мобільні оператори, інтернет-провайдери, супутниковий зв’язок, дата-центри – їхня безперебійна робота є необхідною умовою для діяльності решти життєво важливих об’єктів інфраструктури. Не дивно, що телекомунікації є однією з головних мішеней для ворожих державних суб’єктів, а також кіберзлочинності.

Найвідомішим нещодавнім випадком стала вищезгадана атака на мережу KA-SAT (Viasat), що сталася 24 лютого 2022 року. Дивним у ній є те, що

мішенню був канал зв’язку, а не кінцеві точки. Російські кіберактивісти зламали наземну інфраструктуру супутника і розіслали шкідливі інструкції на десятки тисяч модемів користувачів, зробивши їх непридатними для використання. Фактично, більша частина України була відрізана від Інтернету, що мало на меті припинити зв’язок у перші години вторгнення. Примітно, що ця атака спричинила ланцюгову реакцію: інші клієнти супутникової компанії в країнах ЄС, окрім вітрових турбін у Німеччині, також відчули проблеми зі зв’язком. Через кілька місяців після цього США та ЄС офіційно звинуватили Росію в атаці на Viasat, вперше в історії країну публічно звинуватили в запуску кібератаки з транскордонним впливом на комунікаційну інфраструктуру [96]. Інцидент продемонстрував новий факт: супутниковий та інтернет-зв’язок може стати полем бою, а цивільні користувачі за межами безпосередньої зони конфлікту також можуть постраждати.

Окрім відкритих диверсій, телекомунікаційний сектор постійно стає об’єктом кібершпигунства. Державні суб’єкти (російські, китайські та іранські) намагаються проникнути в мережі телекомунікаційних операторів, щоб отримати доступ до даних про трафік, перехопити комунікації або відстежити пересування людей. Наприклад, у 2021-2022 роках спливло кілька кампаній, проведених китайськими групами APT, які приховано відстежували мережі європейських телекомунікаційних компаній. У Бельгії в 2022 році розслідували масштабний злам IT-інфраструктури Федеральної служби державної безпеки, і китайських хакерів підозрювали в тому, що вони перехоплювали офіційну електронну пошту протягом більше року, можливо, використовуючи доступ через телекомунікаційну інфраструктуру. Аналогічно, у 2020 році провідна телекомунікаційна компанія Норвегії Telenor повідомила про складну кампанію кібершпигунства у своїй мережі, яка тривала кілька місяців (атаку приписували китайському угрупованню APT31). Ці приклади показують, що периметр телекомунікаційної безпеки повинен враховувати не лише технічні збої, але й зловмисні атаки на дані та конфіденційність [102].

Під час війни в Україні спостерігачі відзначають посилення активності російських спецслужб проти європейських телекомунікаційних та інтернет-вузлів. У червні 2022 року компанія Microsoft виявила спроби російських хакерів зламати мережі 42 країн, які підтримують Україну, з метою розвідки та шпигунства. Дві третини з них були членами НАТО, передусім США і Польща. Телекомунікаційні компанії та центри обробки даних також були пріоритетними цілями, оскільки вони зберігають гігантський обсяг інформації про діяльність урядів і збройних сил [89]. Хоча багато зусиль було успішно відбито, Microsoft відзначила, що майже 30% російських кібершпигунських атак на союзників були ефективними (тобто, зловмисники проникли в дані) [54].

Кібератаки на інтернет-сервіси та дата-центри – ще одна загроза для цифрових баз Європи. У липні 2023 року сталася інтригуюча подія: невдале оновлення програмного забезпечення компанією з кібербезпеки спричинило глобальний збій у роботі мереж кількох авіакомпаній та лікарень. Хоча це не була спланована атака, подія продемонструвала взаємозалежність сучасних IT-інфраструктур. Хакери також наживаються на цьому: у 2021-2022 роках атаки на MSP та хмарних провайдерів стали сумнозвісними, що дозволило хакерам атакувати численних клієнтів одночасно (наприклад, злам SolarWinds у 2020 році, який також вплинув на європейські установи) [94].

Безпека телекомунікаційних і цифрових послуг в ЄС гарантується як технологічними заходами (системи спостереження за трафіком, альтернативні канали зв’язку, шифрування), так і юридичними зобов’язаннями. Телекомунікаційні оператори та центри обробки даних включені Директивою NIS2 до переліку операторів критичної інформаційної інфраструктури, які зобов’язані мати план безпеки та повідомляти про серйозні інциденти. Крім того, у 2023 році ЄС прийняв регламент DORA (Digital Operational Resilience Act), який спрямований на забезпечення стійкості цифрових послуг у фінансовому секторі, але опосередковано вплине на вимоги до постачальників хмарних та мережевих послуг [95]. Вживаються і практичні заходи: з 2022 року Оперативна група ЄС з протидії кіберкризам (EU-CyCLONe) займається координацією

реагування на значні інциденти, які можуть вплинути на кілька країн одночасно (наприклад, злом великого міждержавного вузла зв'язку). Всі ці дії спрямовані на те, щоб зробити цифрову інфраструктуру Європи стійкою навіть в умовах екстремальних навантажень від кібератак або гібридного тиску [12, с. 198-199].

Медична галузь є однією з найбільш вразливих і, водночас, найбільш критичних щодо кібер-ризиків. Лікарні, клініки, системи швидкої допомоги, фармацевтичні компанії – всі вони мають величезну IT-інфраструктуру (медичні інформаційні системи, картки пацієнтів, мережеве обладнання). Кібератака на медичний заклад може безпосередньо загрожувати життю та здоров'ю людей, паралізуючи надання медичних послуг. На жаль, за останні два роки злочинці все частіше націлюються на лікарні та медичні установи [40].

Основною загрозою є програми-вимагачі. Згідно зі звітом ENISA, протягом 2021-2022 років більше половини (54%) всіх кібератак на європейську охорону здоров'я були атаками з вимогами викупу. Зловмисники шифрують медичні дані та інфраструктуру, вимагаючи викуп; навіть за наявності резервних копій відновлення може зайняти кілька днів. Однією з найбільш резонансних була атака в Ірландії в травні 2021 року, коли банда Конті зламала IT-мережу лікарні HSE. Сотні лікарняних серверів були зашифровані, а вся система електронних записів вийшла з ладу. Лікарні скасували зустрічі, відклали операції та повернулися до паперового документообігу. Повне відновлення після цієї кіберкризи в ЄС зайняло кілька місяців, а економічні втрати склали сотні мільйонів євро. Цей досвід став тривожним дзвінком для всіх в ЄС щодо реальності загрози: атака вірусу-вимагача на один великий медичний заклад може фактично вивести з ладу систему охорони здоров'я цілої країни [40].

На жаль, не всі засвоїли ці уроки. У 2022-2023 роках деякі європейські лікарні також стали жертвами атак. Лікарня Centre Hospitalier Sud Francilien (CHSF) у серпні 2022 року поблизу Парижа була атакована вірусом LockBit: хакери вимагали викуп у розмірі 10 мільйонів доларів, погрожуючи, що опублікують персональні дані пацієнтів [48]. Уряд відмовився платити, і лікарня

була змушена кілька тижнів працювати в екстреному режимі, відправляючи важкохворих пацієнтів до інших лікарень [15].

Існує також хактивістський елемент у загрозах охороні здоров'я, спричинених війною в Україні. У січні 2023 року проросійська хактивістська команда KillNet оголосила «хрестовий похід» на медичні центри в країнах, близьких до України. Наприкінці січня та на початку лютого 2023 року було зафіксовано понад 90 скоординованих DDoS-атак на клініки та лікарні в декількох країнах ЄС на знак солідарності (Нідерланди, Німеччина, Польща та країни Балтії) [92]. Наприклад, у Нідерландах тимчасово не працювали зовнішні веб-сайти та сервіси Медичного центру Університету Гронінгена, а в Німеччині – кілька клінік у регіонах. Ці атаки не завдали постійної шкоди, але стали актом залякування, продемонструвавши, що навіть лікарні не захищені від кібератак. Більше того, російські хактивісти відкрито вихвалялися такими операціями в соціальних мережах, підкреслюючи свою мету «покарати» Захід за підтримку України [53]. Таким чином, на суто кримінальні ризики в галузі охорони здоров'я наклався ризик бути втягнутим у геополітичну кібервійну.

Фінансовий сектор (банки, біржі, платіжні системи, страхові компанії тощо) є «кровоносною системою» економіки, а отже, злочинці цікавилися ним завжди. Фінансові установи є природним об'єктом атак кіберзлочинців у сенсі наживи (крадіжка грошей, шахрайство, шантаж). Для ворожих держав – це зброя впливу: вдаривши по фінансовій системі, вони здатні викликати паніку, заблокувати платежі, підірвати довіру до економіки супротивника. З початком війни в Україні ризик цього сильно зріс, і регулятори ЄС пішли назустріч. У січні 2022 року Європейський центральний банк попередив великі банки про підвищений ризик російських кібератак і рекомендував підвищити пильність. Банки провели незвичайні кібернавчання, щоб підготуватися до випадків, коли російські хакери атакують SWIFT, платіжні системи або інтернет-банкінг у відповідь на санкції [71].

Деякі з цих побоювань матеріалізувалися у вигляді DDoS-атак і зломів банківських веб-сайтів. Наприклад, у січні 2023 року згадана група KillNet

атакувала сайти кількох відомих німецьких банків (таких як Deutsche Bank і Commerzbank) невдовзі після того, як Берлін вирішив надати танки Україні. Хакери публічно заявили, що це була «відплата» за політичне рішення, сподіваючись викликати обурення широких верств населення. Німецьке агентство кібербезпеки BSI підтвердило факт атаки, але заявило, що вона по суті не вплинула на фінансові транзакції – лише на тимчасове перевантаження сайтів та онлайн-банкінгу. Те ж саме відбулося і в інших країнах: навесні 2022 року від кібератак (переважно короткочасних DDoS) постраждали сайти фінансових регуляторів та фондових бірж у Польщі, Румунії та країнах Балтії. Незважаючи на те, що такі дії безпосередньо не завдають економічної шкоди, вони є інструментом інформаційного та психологічного тиску – проросійські Telegram-медіа широко висвітлюють їх як «удари по Заходу» [90].

Однак на цьому тлі відбулася більш зловісна атака. Європейський інвестиційний банк (ЄІБ), найбільша фінансова установа ЄС, зазнав кібератаки в червні 2023 року. Робота веб-сайтів ЄІБ була порушена і тимчасово виведена з ладу хакерами. Атака сталася через кілька днів після того, як російські маріонеткові війська пообіцяли «ініціювати обвал західних фінансових ринків» як міру помсти за підтримку України. Відповідальність за атаку взяла на себе орбітальна група KillNet, яка назвала її лише початком ініціативи, спрямованої проти європейського фінансування України. ЄІБ швидко відновив функціональність своїх онлайн-сервісів, не допустивши впливу на внутрішні транзакції та дані. Але справа в тому, що це геополітично вмотивована пряма атака на фінансову систему ЄС. Багато хто називає це першим випадком, коли проксі-хакерам вдалося паралізувати роботу установи такого масштабу на континенті, принаймні на деякий час [76]. Це показало, що фінансова індустрія не застрахована від сценарію, коли хакери намагатимуться дестабілізувати фінансові ринки.

На рівні ЄС посилюється нормативно-правова база фінансової кіберстійкості. Відповідний регламент DORA (набув чинності наприкінці 2022 року) об’єднує вимоги до кібербезпеки як для банків, так і для страхових та

фондових компаній, зокрема, щодо управління ІКТ-ризиками, тестування на проникнення та контролю ризиків сторонніх ІТ-постачальників. Фактично, DORA доповнює NIS2, зосереджуючись на фінансовій інформації та операційній стійкості (тобто здатності фінансових установ функціонувати навіть у разі кібератаки). Європейський центральний банк, у свою чергу, проводить галузеві кібернавчання TIBER-EU, які імітують банківські атаки для оцінки вразливостей. Після початку війни режим навчань був переглянутий і тепер включає сценарії масових атак з боку держави [105].

Коротко кажучи, фінансовий сектор ЄС сьогодні перебуває під подвійним тиском: з одного боку, високотехнологічні злочинні угруповання працюють вдень і вночі, щоб придумати способи крадіжки грошей через кіберпростір; з іншого боку, хакери, спонсоровані державою і режимом, розглядають банки і біржі як законні цілі в гібридній війні. Це змушує галузь постійно бути пильною та інвестувати в кібербезпеку, оскільки успішний злам може мати системні наслідки для економічної стабільності.

Органи державної влади та управління (міністерства, органи місцевого самоврядування, правоохоронні органи, державні установи) володіють важливими інформаційними ресурсами та надають основні послуги населенню. Їх інфраструктура є природною мішенню як для кібершпигунства (викрадення секретної інформації, доступу до державних реєстрів), так і для деструктивних атак (паралізація роботи порталів державних послуг, саботаж у кризових ситуаціях). У воєнний час важливість кіберзагроз для цього сектору ще більше зростає, оскільки урядові мережі стають безпосереднім полем бою між спецслужбами.

З початком широкомасштабної агресії Україна опинилася під потужним тиском на державному цифровому фронті. Російські кіберзловмисники штурмували урядові веб-сайти, виводили з ладу портали державних послуг та зламували мережі супутникового зв’язку, що обслуговують міністерства. Ці атаки мали на меті вивести з ладу систему управління країною і водночас здійснити вторгнення в неї. У відповідь українські та західні експерти посилили

захист, і більшість атак було зірвано або їхні наслідки були швидко ліквідовані. Іноземна допомога також відіграла вирішальну роль: Країни ЄС підтримали Україну в питаннях кіберзахисту, а приватний сектор (Microsoft, ESET, Cloudflare тощо) оперативно підключився до відбиття ворожих кампаній. В результаті жодна кібератака не призвела до тривалої недієздатності державного апарату України. Але й агресор не здався – з 2022 року російські спецслужби також посилили кібершпигунство проти західних урядів. Компанія Microsoft повідомила, що 128 організацій у 42 країнах (переважно урядові та пов'язані з урядом) були атаковані російською кіберактивністю в перший рік вторгнення. Серед них – міністерства закордонних справ, оборони та енергетики ЄС, аналітичні центри та постачальники послуг зв'язку для них. Цілі цих операцій очевидні: збір розвідувальної інформації про позицію союзників, наміри допомогти Україні та внутрішню політику ЄС щодо війни. Більшість цих атак здійснювалися таємно Більшість цих атак здійснювалися таємно і мали на меті викрадення даних (наприклад, офіційного листування, документів, облікових даних для входу в систему). Але були й відверто руйнівні атаки на державні активи країн ЄС. У червні 2022 року на литовські державні служби було здійснено величезну DDoS-атаку, хакерський колектив KillNet заявив, що зробив це у відповідь на блокування транзиту до Калінінграду. Тимчасово були недоступні веб-сайти державних установ, урядові онлайн-платформи і навіть деякі приватні портали. Зловмисники стверджували, що вони «вивели з ладу 1652 веб-ресурси» в Литві. Хоча це твердження було перебільшеним, атака дійсно стала однією з найпотужніших кібератак на членів НАТО, що змусило ЄС активувати механізми взаємодопомоги в кіберпросторі. Паралельні, хоча і менш масштабні, атаки були здійснені проти Латвії, Естонії та Румунії у 2022-2023 роках у формі переважно DDoS-атак на урядові веб-сайти або дефейсингу (злому сторінок з пропагандистським контентом) [89].

Більшість урядових ІТ-рішень є застарілими, сповненими вразливостей, а рівень підготовки персоналу різний. Під час війни та пандемії діджиталізація

державних послуг відбувалася швидкими темпами, але часто без належного захисту.

Для підвищення стійкості державних установ ЄС впроваджує організаційні та технологічні заходи. У рамках співпраці з ННД створено мережу урядових CERT, які обмінюються інформацією про інциденти. Тривають експериментальні пілотні проекти програми кіберспівпраці (адже різниця між збройними силами та цивільною інфраструктурою зменшується – кібератаки на енергетику чи транспорт можуть спричинити військовий удар). НАТО, у свою чергу, прийняло Україну як члена до Центру передового досвіду з кіберзахисту (Cooperative Cyber Defence Centre of Excellence, CCDCOE) [25] у 2023 році, запровадивши спільну базу знань щодо російських стратегій кібер-атак. Крім того, ЄС також планує створити Європейський центр управління кіберкризами (Joint Cyber Unit) для координації зусиль у разі скоординованих атак на ключові об’єкти інфраструктури та залучення ресурсів кількох країн.

Аналіз кіберзагроз ключовій інфраструктурі ЄС у 2024-2025 роках прогнозує складну і напружену ситуацію. Критичні сектори – транспорт, телекомунікації, енергетика, охорона здоров’я, фінанси та державне управління – стикаються з постійним кібертиском з боку різних суб’єктів. Державні хакери (передусім російські) використовують кіберпростір як театр гібридної війни, атакуючи інфраструктуру України та ЄС (прямо чи опосередковано). Групи кіберзлочинців використовують вразливість критично важливих сервісів для отримання фінансової вигоди, що зазвичай призводить до суспільно небезпечних інцидентів. Проросійські «хактивісти» відкрили фронт кібератак, поширивши конфлікт на віртуальний світ і націлившись на цивільні об’єкти в Європі з політичних мотивів.

Європейський Союз протидіє цим загрозам комплексно: через модернізацію законодавства (NIS2, CER, DORA), посилення міжнародної співпраці (спільні кібернавчання, обмін розвідданими) та залучення приватного сектору до оборони (державно-приватне партнерство у сфері кібербезпеки). Помітною особливістю стало підвищення кіберстійкості самих систем: багато

атак, які могли б призвести до катастрофи, були вчасно виявлені та нейтралізовані завдяки вдосконаленню захисту та транскордонному співробітництву. Війна в Україні, за іронією долі, стала рушійною силою європейської цифрової безпеки, оскільки уряди і компанії нарешті усвідомили реальність загрози і прискорили інвестиції в захист критичної інфраструктури.

Водночас загрози залишаються надзвичайно високими. Плани масштабних кібератак – таких як виведення з ладу електромереж, порушення фінансових розрахунків або втручання в системи управління транспортом – залишаються в центрі уваги зловмисників і фахівців з безпеки. Геополітична напруженість не спадає, тому критична інфраструктура ЄС залишатиметься під прицілом. Посилення координації дій, обмін досвідом з Україною та впровадження нових технологій кіберзахисту (наприклад, штучного інтелекту для виявлення атак) визначатимуть, наскільки добре ЄС зможе протистояти загрозам у п’ятій сфері війни. В епоху Інтернету забезпечення безпеки та надійності критично важливих мереж є обов’язковою умовою національної та колективної безпеки, і досвід 2022-2023 років лише підтверджує це.

2.3. Кіберзлочинність як виклик кібербезпеці ЄС.

Кіберзлочинність в Європейському Союзі за останні роки досягла безпрецедентних масштабів, ставши однією з головних загроз цифровій безпеці регіону. У 2023 році кількість кібератак та інцидентів різного типу різко зросла, що значною мірою пов'язано з геополітичними подіями та швидкою еволюцією загроз. Корпоративні магнати та урядові структури, а також малі підприємства та окремі громадяни не захищені від кібератак. Кіберзлочинці мають високу адаптивність – вони швидко опановують нові технології, інструменти та засоби соціальної інженерії, використовуючи вразливості віртуальної інфраструктури та низький рівень обізнаності користувачів. Таким чином, на сучасній кіберзлочинності в ЄС домінують різноманітні загрози: від масштабних планів шахрайства до цілеспрямованих атак з боку хакерів, що фінансуються державою. Крім того, ми розглянемо найбільш значущі форми кіберзлочинності, які ставлять кібербезпеку ЄС перед викликом, наводячи характерні приклади атак і тенденції у 2024-2025 роках.

Пару слів про індивідуальні методи кіберзлочинності, виводи грошей, атаки на бізнес, і схожі типи атак. Індивідуальні кібернапади, зокрема фішинг, компрометація бізнес-комунікацій, атаки на криптовалютні біржі та онлайн-шахрайство, ботнети і вимагання мають не лише локальний економічний ефект, а й стратегічні наслідки, оскільки значна частина отриманих таким чином коштів спрямовується до країн під санкціями – передусім Росії, Ірану та Північної Кореї. Згідно з аналітичними звітами Chainalysis та даними ООН, викрадені через кібероперації фінанси використовуються для підтримки військових програм (наприклад, розробки ракет у КНДР), обходу санкцій у банківському секторі Ірану, або ж забезпечення матеріально-технічної спроможності російських силових структур [103]. Більшість з цього було згадано в попередніх підрозділах, тому тут вони не будуть згадані надалі. Тут буде більше уваги на державних атаках і їх видах.

У 2023 році частота та інтенсивність DDoS-атак зросла. Європейські країни неодноразово ставали мішенню потужних кампаній «розподіленої відмови в

обслуговуванні». Зокрема, на початку року прокремлівські хактивісти (організації на кшталт KillNet та Anonymous Sudan) розпочали скоординовані атаки на урядові сайти та сайти критичної інфраструктури проукраїнських країн-членів ЄС. За даними ENISA, у 2022-2023 роках DDoS зрівнялися з програми-вимагачами як найпоширеніша кіберзагроза: разом вони становили майже половину всіх зареєстрованих випадків. При цьому середній обсяг трафіку DDoS-атак продовжує зростати: у 2023 році було зафіксовано низку рекордних атак з обсягом трафіку понад 1 Тбіт/с. Водночас зростає і складність: все більш популярними стають багатовекторні DDoS-атаки, коли різні техніки (UDP-флуд, HTTP-флуд, SYN-флуд тощо) використовуються в комбінації, щоб обійти системи захисту [88].

DDoS-атаки все частіше використовуються не тільки як самостійні, але й у поєднанні з іншими видами атак. Зловмисники розробили тактику «DDoS як відволікаючий маневр»: спочатку вони запускають масовану атаку на публічні сервіси організації, щоб відволікти увагу від IT-безпеки, а тим часом здійснюють приховане вторгнення в мережу з метою шпигунства або крадіжки даних. Це робить бізнес більш ризикованим, оскільки під час усунення збоїв у роботі веб-сайтів зловмисники можуть викрасти секретну інформацію. Загалом, ботнети та DDoS залишаються серйозною проблемою: незважаючи на створення рішень для боротьби з DDoS, злочинці знаходять нові способи збільшення потужності атак (наприклад, використання вразливих VPN-сервісів або зламаних серверів замість слабкого Інтернету речей, щоб генерувати трафік з меншою кількістю «більш потужних» ботів. У контексті конфлікту в Україні DDoS став інструментом кіберпротестів і репресій: прокремлівські протестувальники відкрито здійснюють атаки на національні урядові сайти країн ЄС, намагаючись продемонструвати «силову присутність» онлайн.

У 2022-2024 роках геополітичний вимір, зокрема війна Росії проти України, сильно вплинув на європейське кіберсередовище. Російські кіберзлочинці, значна кількість яких має прямі чи опосередковані зв’язки з російськими спецслужбами, різко збільшили кількість атак на країни ЄС.

Більшість з цих атак і груп були покриті в попередніх розділах, але тут вони згадані в задля розкриття теми. З одного боку, зросла кількість деструктивних атак і шпигунських кампаній проти урядових мереж, дипломатичних представництв і оборонних компаній проукраїнських держав. Зокрема, група APT28 (Fancy Bear), яку пов'язують з російським ГРУ, у 2023 році здійснила серію зломів електронних поштових скриньок чиновників у Польщі, Німеччині та країнах Балтії. У травні 2024 року уряд Німеччини офіційно звинуватив Росію у втручанні в особисту електронну пошту членів партії канцлера у 2023 році, що стало результатом кібероперацій тієї ж групи Fancy Bear. Тип атаки спрямований на шпигунство та потенційну крадіжку документів і стратегічних даних, які можуть дати зловмиснику перевагу. Водночас проросійські хактивістські групи (NoName057(16), KillNet, Anonymous Sudan та інші) почали масово атакувати європейські веб-сайти та сервіси після політичних протистоянь. Свою діяльність вони здійснювали у формі DDoS-атак та дефолтів веб-сайтів, зазвичай публічно заявляючи, що це була «помста» за підтримку України. Наприклад, у березні 2023 року «Анонімний Судан» взяв на себе відповідальність за серію DDoS-атак на різні французькі міністерства, назвавши це реакцією на заяви французького уряду про допомогу Україні.

Такі форми кібербулінгу іноді організовуються через канали Telegram, де тисячі «добровольців» об'єднуються, щоб одночасно спрямувати трафік на обрану ними ціль. Хоча ці атаки не мають катастрофічних довгострокових наслідків, вони створюють атмосферу нестабільності і психологічного стресу, а отже, демонструють, що на цифровий простір ЄС можна впливати. Іншою постійною загрозою є кібершпигунство з боку інших держав. Окрім Росії, активно діють китайські кіберрозвідники, а також іранські та північнокорейські зловмисники, кожен з яких націлений на щось своє. Китайські хакери найбільше зацікавлені у крадіжці інтелектуальної власності та технологій. Один гучний випадок розслідується в Бельгії: було встановлено, що між 2021 і 2023 роками група, пов'язана з китайською розвідкою, таємно мала доступ до електронної пошти бельгійської Служби державної безпеки (VSSE) через вразливість в

одному з її інструментів захисту електронної пошти [21]. Як показало дослідження, хакерам вдалося перехопити до 10% офіційної електронної пошти VSSE протягом двох років, що називають найбільшою в історії компрометацією європейської розвідки. Хоча ніякої секретної інформації не було зламано (вона, ймовірно, надсилалася іншими каналами), було зламано персональні дані майже половини співробітників VSSE. Це показовий приклад того, наскільки витонченими і довготривалими можуть бути кампанії кібершпигунства: зловмисники діяли тихо, використовували законну, але скомпрометовану утиліту безпеки (за гіпотезою, популярний поштовий шлюз, який був зламаний під час атаки «0-day» у 2023 році) і тривалий час залишалися під радаром.

Державні зловмисники воліють використовувати «легальні» та багатоцільові інструменти, намагаючись уникнути виявлення. ENISA зазначає, що фінансовані державою суб'єкти все частіше використовують загальнодоступні інструменти адміністрування та легальне програмне забезпечення для злому з метою шпигунства. Наприклад, російські та китайські хакери відомі тим, що використовують комерційні програми віддаленого доступу, утиліти адміністратора (оскільки їх важче заблокувати, щоб не порушити роботу IT-систем) і вбудовані системні скрипти – цей метод називається «Життя за межами країни». Також трапляються випадки зараження троянами легітимних програмних бібліотек або патчів, як, наприклад, скомпрометовані патчі SolarWinds у 2020 році, що стало знаковим випадком. У 2023 році повідомлялося про те ж саме: під час однієї з атак, розслідуваної в Нідерландах, китайський ПНП модифікував прошивку мережевого маршрутизатора, щоб отримати копії трафіку з мережі цільової установи. Це підходить під стратегію гібридної війни, яка виконується під радаром з низькою інтенсивністю.

Окрім кібершпигунства, зловмисні кібератаки є ще однією сферою державної кіберагресії. Традиційним прикладом є російська атака вірусу-здирника NotPetya у 2017 році, коли він порушив роботу систем кількох європейських фірм; ця ж загроза повторилася у 2022-2023 роках під час війни в

Україні, коли зловмисні програми-шифрувальники знищували інформацію українських установ. Європейські країни уважно стежать за такими атаками, оскільки ті ж самі групи можуть націлитися і на ЄС. Наприклад, у жовтні 2023 року, під час нового витка війни на Близькому Сході, було виявлено вірус-стирач «ВіВі», який Росія раніше використовувала проти України, а також постраждали деякі організації в Ізраїлі [24]. Це ілюструє транскордонний характер кібервійни: тактика та інструменти, випробувані в одній війні, негайно переносяться в іншу.

Державні кібероперації зазвичай передують або маскуються під кримінальні операції. Дедалі частіше трапляються випадки, коли програми-вимагачі діють у координації з державами: або безпосередньо замовляють атаку на ціль (щоб завдати економічної шкоди чи отримати розвідувальні дані під прикриттям вимагання), або після цього «передають» викрадені дані розвідувальним органам своєї країни. Наприклад, північнокорейські угруповання не лише викрадають криптовалюту для фінансової вигоди режиму, але й викрадають конфіденційну інформацію у жертв у США та Європі, яка може мати розвідувальну цінність [103]. У 2022 році російські групи вимагачів відкрито декларували політичну лояльність (група Conti присягнула на вірність російській державі), а деякі атаки на українські та польські об’єкти мали ознаки державного замовлення. Така співпраця між державами та кіберзлочинністю унеможливлює реагування: традиційні правоохоронні інструменти (розшук та покарання злочинців) є неефективними, коли злочинці перебувають під захистом власної держави.

Відповіддю ЄС на гібридні кіберзагрози є посилення колективного кіберзахисту. Створено системи обміну інформацією про атаки між країнами (через CERT-EU, кіберцентри НАТО), проводяться кібернавчання для відпрацювання сценаріїв, в яких кібератака супроводжує військову агресію або спрямована на дестабілізацію виборів. У регуляторному законодавстві набула чинності Директива NIS2 (2022), яка зобов’язує розширене коло операторів критичної інфраструктури запровадити положення про кібербезпеку та інформування про інциденти, в тому числі щодо атак, спричинених державними

засобами ураження, що підтримуються зброєю. ЄС також вперше запровадив санкції проти іноземних кіберзлочинців, найнятих державою: санкції були введені проти осіб, які стояли за операцією Sofacy, спрямованою проти німецького Бундестагу та розповсюдження вірусу NotPetya. Це політична заява про те, що кібератаки сприймаються як загроза міжнародному порядку, а не як злочинні дії.

Висновки до другого розділу

Кіберзлочинність стала гідрою з численними головами, яка атакує кібербезпеку ЄС на всіх фронтах. Від простого фішингу, що загрожує всім, хто користується Інтернетом, до складних шпигунських операцій, що потенційно впливають на політику, – різноманітність загроз охоплює весь цифровий світ. Актуальність цього питання у 2024-2025 роках рекордно висока: тенденції пророкують подальшу появу та зростання кіберзлочинності. У відповідь на цей виклик ЄС відчуває себе зобов’язаним підвищити рівень координації між державами, інвестувати в кіберзахист та розробляти нові механізми стримування злочинців. Постійний обмін розвідданими про загрози, налагодження державно-приватного партнерства (залучення ІТ-компаній до кіберзахисту) та раціоналізація нормативно-правової бази – все це є ключовими факторами. Однак досвід доводить, що кіберзлочинність не стоїть на місці: вона еластично обходить бар’єри, шукає ніші та слабкі місця.

РОЗДІЛ ІІІ. ЄВРОПЕЙСЬКІ МЕХАНІЗМИ ПРОТИДІЇ КІБЕРЗАГРОЗАМ У ВОЄННИЙ ЧАС

3.1. Правове регулювання кіберпростору в Європейському Союзі.

На 2024-2025 роки Європейський Союз запропонував загальну систему правил для всієї кіберсфери, що охоплює багато аспектів кібербезпеки, захисту даних та стійкості систем. Вона ґрунтується на кількох директивах і регламентах ЄС, які встановлюють обов'язкові зобов'язання для держав-членів і бізнесу, а також формують інституційні механізми координації та взаємодії за кордоном. Далі ми обговоримо найважливіші закони ЄС у сфері кібербезпеки, роль кваліфікованих інституцій та участь ЄС у міжнародних інструментах.

Одним із наріжних каменів правової бази ЄС у сфері кібербезпеки є Директива (ЄС) 2022/2555 про заходи для забезпечення високого спільного рівня кібербезпеки в межах Союзу (також відома як NIS2) [69]. Вона була прийнята 14 грудня 2022 року на заміну Директиві 2016/1148 (NIS 1) і набула чинності в січні 2023 року [33]. NIS 2 значно розширює сферу дії попереднього акта, встановлюючи гармонізовані стандарти кібербезпеки для 18 секторів економіки. До перелічених вище секторів (енергетика, транспорт, фінанси, охорона здоров'я, водопостачання, цифрова інфраструктура тощо) додаються нові: провайдери електронних комунікацій, поштові та кур'єрські послуги, виробництво критично важливих товарів, соціальні медіа, державне управління на центральному та регіональному рівнях, космічна галузь тощо. Загалом, директива поширюється на середній та великий бізнес у відповідних галузях; вони класифікуються як «важливі» або «суттєві» органи залежно від ступеня критичності їхніх послуг та розміру, що визначає ступінь нагляду та штрафи.

NIS 2 встановлює ряд зобов'язань для країн-членів ЄС. Кожна держава повинна розробити та впровадити національну стратегію кібербезпеки (ст. 7 Директиви 2022/2555) – установчий документ, в якому представлені основні напрямки та інструменти національної кібербезпеки, такі як політика управління ризиками, стандартизація та сертифікація у цій сфері, розподіл повноважень

компетентних органів, механізми державно-приватного партнерства, процедури інформування про інциденти тощо. Однією з обов'язкових складових стратегії є план реагування на кіберінциденти та кризові ситуації (ст. 9 (4) NIS 2), який визначає порядок дій держави у випадку масштабних кібератак – цілі та порядок управління кризовими ситуаціями, залучені органи, структури обміну інформацією, заходи з підготовки (навчання, тренінги, навчання) тощо. Крім того, держави-члени повинні призначити національні компетентні органи у сфері кібербезпеки, контактну особу та національний центр реагування на інциденти (CSIRT) (статті 8, 10) з метою виконання зобов'язань, передбачених Директивою.

Директива NIS 2 також безпосередньо накладає зобов'язання на бізнес-операторів у відповідних секторах. Вони повинні вживати заходів з управління кіберризиками (стаття 21), таких як: оцінка ризиків мережі та інформаційних систем, впровадження заходів безпеки (наприклад, шифрування, контроль доступу, резервне копіювання даних тощо), управління безперервністю надання послуг, оцінка вразливості постачальників (ланцюжок поставок) та інші організаційні та технічні заходи. Визначено конкретні вимоги до звітності щодо інцидентів (стаття 23 NIS 2): оператори повинні інформувати національний компетентний орган або CSIRT про значні інциденти без невиправданої затримки. Вперше на рівні ЄС запроваджено процедуру послідовного повідомлення: первинне попередження має бути надіслано протягом 24 годин після виявлення серйозного інциденту, а детальне повідомлення з інформацією та попередніми висновками про інцидент має бути надіслано протягом 72 годин. Після того, як інцидент буде вирішено, організація повинна буде подати заключний звіт з аналізом першопричин та заходів реагування, вжитих протягом одного місяця з моменту інциденту. Це узгоджується з аналогічною вимогою щодо надання звітів протягом одного місяця про порушення даних відповідно до GDPR (див. нижче) і має на меті подальшу підтримку своєчасного обміну інформацією про кібератаки в межах ЄС.

Для нагляду за застосуванням NIS 2 та обміну найкращими практиками між державами-членами було створено Групу співпраці – консультативний орган, до складу якого входять представники всіх держав-членів, Європейської Комісії та Агентства ЄС з кібербезпеки (ENISA). Група розробляє керівні принципи і рекомендації щодо застосування Директиви і сприяє зближенню методів між державами-членами. Крім того, взаємозв'язок національних груп реагування (CSIRT) забезпечує оперативну координацію в разі кібератак, а нещодавно створена структура ЄС для реагування на значні кіберінциденти – EU-CyCLONe (Європейська мережа реагування на кіберкризи) – покликана забезпечити швидкий обмін інформацією та координацію в умовах транскордонних кіберкриз [41]. NIS 2 має бути імплементована в національне законодавство держав-членів до 17 жовтня 2024 року; якщо цього не буде зроблено, Європейська Комісія вже ініціювала перші кроки в процедурі порушення, надіславши офіційні повідомлення 23 державам ЄС у жовтні 2024 року (більшість держав завершать транспозицію директиви на початку 2025 року).

Безпека кіберпростору та захист персональних даних йдуть пліч-о-пліч, як це видно із Загального регламенту про захист даних (ЄС) 2016/679 (GDPR) [80]. GDPR, який в першу чергу спрямований на захист прав фізичних осіб, коли мова йде про їхні дані, включає ключові вимоги в контексті кібербезпеки. Зокрема, стаття 32 GDPR передбачає, що контролери та обробники даних повинні вживати «відповідних технічних та організаційних заходів» для забезпечення належного рівня безпеки, пропорційного ризикам обробки даних. Регламент, очевидно, пропонує ілюстрації таких заходів: псевдонімізація та шифрування даних, конфіденційність даних, доступність та стійкість інформаційної системи та цілісність даних, періодичне тестування ефективності процедур безпеки тощо (с. 51). Крім того, статті 33-34 GDPR встановлюють відповідальність за розкриття інцидентів безпеки персональних даних: контролер зобов'язаний повідомити національний наглядовий орган, відповідальний за захист персональних даних, про настання такого інциденту протягом 72 годин з моменту, коли йому стало

відомо про факт настання такого інциденту, якщо такий витік персональних даних може спричинити ризик для прав фізичних осіб. У випадку, коли інцидент може становити серйозну небезпеку для самих осіб (наприклад, для такої крадіжки, що стосується чутливих даних), контролер повинен негайно повідомити про це залучених осіб». Ці правила забезпечують прозорість кіберпорушень щодо індивідуальної інформації та підштовхують компанії до більшої безпеки, щоб не наражатися на драконівські штрафи – GDPR передбачає штрафи до 20 млн євро або 4% світового обороту за правопорушення, в тому числі за неналежний захист даних (ст. 83).

Захист даних та кібербезпека в ЄС пов'язані між собою в обох напрямках. І навпаки, недоторканність приватного життя є передумовою кібербезпеки: право на недоторканність приватного життя не може бути забезпечене без належного захисту інформаційних систем від несанкціонованого доступу. Саме на цій підставі GDPR згадує забезпечення безпеки обробки даних як основоположний принцип (статті 5 і 32) і визнає операції з кібербезпеки інформації та мереж законним інтересом (див. преамбулу, параграф 49 GDPR). З іншого боку, операції з кібербезпеки повинні здійснюватися з належною повагою до законодавства про захист даних: моніторинг трафіку, обробка журналів подій, обмін інформацією про кіберзагрози між організаціями – все це по суті обробляє персональні дані (IP-адреси, облікові записи тощо) і повинно здійснюватися відповідно до GDPR. Європейська модель регулювання передбачає баланс у цьому питанні. Варто зазначити, що Агентство ЄС з кібербезпеки (ENISA) Регламентом 2019/881 наділене повноваженнями спеціаліста з питань захисту даних: воно забезпечує реалізацію політики ЄС щодо захисту даних на рівні кібербезпеки та, у разі необхідності, може запропонувати експертизу Європейській раді з питань захисту даних (робоча група національних органів захисту даних) [82]. Звідси випливає, що обидві правові бази ЄС щодо кібербезпеки та персональних даних співпрацюють між собою, синергетично поєднуючись задля створення захищеного середовища цифрових продуктів, яким можна довіряти.

Регламент 2019/881 перетворив ENISA з тимчасового агентства (спочатку створеного в 2004 році з обмеженим у часі мандатом, який регулярно поновлювався) на стабільну інституцію ЄС з широким спектром діяльності. Відповідно до статей 5-8 Регламенту, ENISA надає експертну допомогу у формуванні та реалізації політики ЄС у сфері кібербезпеки, а саме: готує аналітичні огляди та рекомендації до законопроектів; підтримує держави-члени ЄС у гармонізованій імплементації директив (і, таким чином, ENISA є одним з основних радників з імплементації NIS/NIS 2); заохочує обмін кращими практиками між державами; підтримує розвиток потенціалу кібербезпеки (наприклад, організовує тренінги, кібернавчання, розробляє методологічні інструменти). ENISA також координує мережеве та оперативне співробітництво: є секретаріатом вищезгаданої Групи співробітництва ННД та мережі CSIRTs, здійснює експертну оцінку кіберготовності держав-членів та проводить щорічний огляд дотримання кіберстандартів у всьому ЄС. Крім того, Агентство відповідає за підготовку загальноєвропейських звітів про кіберзагрози (ENISA щороку публікує звіт Threat Landscape про існуючі кіберзагрози) та функціонування Бази даних інцидентів у сфері кібербезпеки. Зокрема, ENISA стала основним гравцем у сфері сертифікації: вона розробляє пропозиції щодо нових схем сертифікації, залучаючи експертів та зацікавлені сторони (через Групу з питань сертифікації при ENISA), а також може виступати в якості оціночного або координаційного центру для окремих схем (статті 56, 58).

Європейська схема сертифікації кібербезпеки. Закон про кібербезпеку запровадив гармонізований метод сертифікації безпеки ІТ-продуктів та послуг в ЄС (статті 46-65 Регламенту 2019/881). Раніше існували різні схеми сертифікації в кожній країні-члені, що ускладнювало взаємне визнання сертифікатів і створювало бар’єри для входу на ринок. Нове правило встановлює структуру, за якою все частіше будуються європейські схеми сертифікації – загальні стандарти та процедури тестування безпеки для певних видів ІКТ-продуктів або послуг. Кожна така схема визначає рівні довіри (базовий, суттєвий, високий), що засвідчують рівень надійності та стійкості продукту або послуги (стаття 52).

Сертифікація за прийнятою схемою визнається в усіх країнах ЄС без додаткових національних випробувань, що сприяє створенню єдиного ринку. Наразі вже існує декілька схем, що діють або розробляються: зокрема, ЄС схвалив схему сертифікації основних ІТ-продуктів (відповідно до стандартів Common Criteria), ведеться робота над розробкою схеми для хмарних сервісів (EU Cloud Cybersecurity Scheme) та ін. Хоча членство в більшості схем наразі є добровільним, галузеве законодавство може зробити сертифікати обов'язковими в деяких випадках (стаття 56). Наприклад, проєкт майбутнього Закону про кіберстійкість (CRA), який очікує остаточного ухвалення у 2024 році, встановлює обов'язкові вимоги до продуктів ІКТ щодо відповідності мінімальним вимогам безпеки і може спиратися на механізм сертифікації, встановлений Регламентом 2019/881.

Питання кібербезпеки нерозривно пов'язані з фізичною та технічною стійкістю всієї критичної інфраструктури. Щоб підвищити стійкість критично важливих об'єктів у різних секторах, ЄС розробив Директиву (ЄС) 2022/2557 про стійкість критично важливих об'єктів (CER) [72]. Директива була прийнята разом з NIS 2 (14 грудня 2022 року) і доповнює її, акцентуючи увагу на стійкості критично важливих об'єктів в 11 сферах: енергетика, транспорт (повітряний, залізничний, водний, автомобільний та міський громадський транспорт), банківська справа, фінансові ринки, охорона здоров'я (медичні послуги, фармацевтика та виробники медичного обладнання), питна вода та водовідведення, цифрова інфраструктура (зокрема, центри хмарних обчислень та електронні комунікаційні мережі), державне управління (центральна влада), космічна інфраструктура та харчова промисловість (масове виробництво та розподіл продуктів харчування). Директива CER замінила колишню Директиву 2008/114/ЄС про європейську критичну інфраструктуру, значно розширивши перелік охоплених секторів і запровадивши сучасні методи оцінки ризиків.

Директива CER встановлює паралельний режим зобов'язань для держав-членів та критично важливих підприємств, гармонізований з кібердирективою NIS 2. Держави-члени розроблятимуть національну стратегію стійкості для

критично важливих підприємств та проводитимуть оцінку ризиків на періодичній основі (статті 3-5). На основі цього кожна країна визначатиме перелік критично важливих суб'єктів у певних секторах – тобто компаній або установок, вихід з ладу яких потенційно матиме серйозний вплив на суспільство, економіку, безпеку або здоров'я людей (статті 6-7). Держави-члени надають допомогу та здійснюють нагляд за кваліфікованими критично важливими суб'єктами: надають консультації, проводять навчання, інспекції, а в разі невиконання вимог – застосовують примусові заходи (статті 8-11). Також передбачено особливий інструмент – перевірка біографічних даних осіб, які обіймають відповідальні посади на об'єктах критичної інфраструктури (стаття 11).

У свою чергу, критичні суб'єкти (компанії, визначені кожною державою відповідно до критеріїв, викладених у Директиві) повинні управляти ризиками безперервності надання своїх послуг. Вони повинні проводити самостійний аналіз ризиків та виявляти загрози, які можуть призвести до збоїв (ст. 13), впроваджувати адекватні заходи безпеки та стійкості – фізичні (безпека об'єктів, захист від стихійних лих, резервні потужності) та кібернетичні (захист IT-систем, резервне копіювання даних тощо) – відповідно до найкращих практик (ст. 14). Компанії також зобов'язані повідомляти органам влади про випадки, які призводять до значного призупинення надання основних послуг (стаття 15). Слід зазначити, що правила Директиви CER мають обмежене застосування у сфері цифрової інфраструктури, банківської справи та фінансових ринків, оскільки вони регулюються окремими актами (для цифрової інфраструктури – NIS 2, для фінансового сектору – Регламентом (ЄС) 2022/2554, тобто DORA, про цифрову операційну стійкість кредитних установ та інвестиційних компаній) [95]. Таким чином, телекомунікаційні оператори, хмарні сервіси, банки та біржі залишаються зобов'язаними забезпечувати кіберстійкість згідно з відповідним законодавством, але CER спрямований проти інших секторів.

Для забезпечення координації в рамках ЄС Директива 2022/2557 створила Групу з питань стійкості критично важливих об'єктів (Critical Entity Resilience

Group, CERG) – експертну групу, що базується в Брюсселі та складається з представників кожної держави і очолюється Європейською Комісією [34]. CERG зосереджується на зміцненні співпраці, обміні знаннями про транскордонні ризики та передовий досвід, а також на гармонізації заходів з надання допомоги критично важливим об'єктам. Європейська Комісія, зі свого боку, уповноважена організовувати за власною ініціативою так звані консультативні місії для наднаціональних критично важливих суб'єктів (що діють у 6 і більше державах) – групи експертів можуть перевіряти плани таких компаній у сфері кібербезпеки та пропонувати вдосконалення (ст. 15, ст. 21). Директива CER має бути транспонована до жовтня 2024 року, і переважна більшість організацій з високим рівнем ризику, які підпадають під її критерії визначення, ймовірно, одночасно будуть також підпадати під вимоги кібербезпеки NIS 2. Таким чином, NIS 2 та Директива CER забезпечують наскрізне регулювання – від цифрової безпеки до загальної стійкості – основних інфраструктур ЄС.

На додаток до регуляторних вимог ринку, ЄС також інвестує в науково-технічний потенціал у сфері кібербезпеки. З цією метою Регламентом (ЄС) 2021/887 від 20 травня 2021 року було створено Європейський промисловий, технологічний та дослідницький центр передового досвіду з кібербезпеки та мережу координаційних центрів (Європейський центр компетенції з кібербезпеки, ECCC) [83]. Новий Центр компетенцій розташований у Бухаресті, Румунія, і фактично функціонує як агентство ЄС, відповідальне за координацію інвестицій та експертизи в галузі кібербезпеки.

Основними завданнями Центру компетенцій (ст. 4) є: координація фінансування проектів з кібербезпеки в рамках програм «Цифрова Європа» та «Горизонт Європа» (на ці програми ЄС зосередив значні кошти на дослідження, інновації та впровадження кіберзаходів); сприяння тісній співпраці між бізнесом, науковими колами та державним сектором для створення передових кібертехнологій; стимулювання впровадження результатів досліджень на практиці, зокрема, для захисту промисловості та малого бізнесу; розвиток компетенцій через освітню роботу, тренінги, обмін експертами тощо. З метою

посилення координації національних зусиль Регламент також передбачає створення мережі національних координаційних центрів: кожна країна-член ЄС призначає свій центр (в Україні, наприклад, після приєднання до програми «Цифрова Європа» його функції виконує Державна служба спеціального зв'язку та інформатизації). Ці центри взаємодіють з Європейським центром, створюючи своєрідний «хаб» спеціальних знань у сферах ЄС. Центр також об'єднує більш широку Спільноту компетенцій з кібербезпеки – групу університетів, науково-дослідних інститутів, асоціацій, приватних компаній та інших суб'єктів, що дозволяє їм обмінюватися інформацією та визначати потенційних партнерів для реалізації проектів (ст. 8).

На глобальному рівні основним міжнародним договором, що охоплює кіберпростір, є Конвенція про кіберзлочинність 2001 року [7], інакше відома як Будапештська конвенція. Хоча ЄС, як наднаціональна інституція, не є підписантом цього договору (його підписантами є окремі держави, в тому числі всі країни-члени ЄС та Україна), сам Союз активно підтримує ідеали Конвенції та закликає треті держави приєднатися до неї. Будапештська конвенція встановлює гармонізовані методи криміналізації кіберзлочинів (несанкціонований доступ, системне втручання, злочини у сфері комп'ютерних даних тощо) та механізми міжнародної співпраці правоохоронних органів. ЄС імплементував його положення у власне законодавство, а саме Директиву 2013/40/ЄС про атаки на інформаційні системи, яка гармонізувала рамки кіберзлочинності та покарання в ЄС [32]. У 2022 році було відкрито для підписання Другий Будапештський протокол, який уможливив більшу співпрацю та обмін електронними доказами; Європейська Комісія надала державам-членам дозвіл на приєднання до Протоколу, оскільки він відповідає політиці ЄС у сфері кіберзлочинності (Рішення Ради (ЄС) 2022/1700) [84]. Таким чином, використовуючи правові інструменти Ради Європи, ЄС розвиває міжнародні правові стандарти боротьби з кібератаками та створює мережу співпраці з країнами, які не є членами ЄС.

Незважаючи на те, що нормативно-правова база ЄС гармонізує вимоги, всі країни-члени продовжують розробляти власні закони про кібербезпеку, адаптуючи їх до національної специфіки і навіть виходячи за рамки європейського рівня. Наприклад, Німеччина прийняла перший Закон про IT-безпеку (IT-Sicherheitsgesetz) у 2015 році, який вимагає від операторів критичної інфраструктури впроваджувати заходи з кібербезпеки та повідомляти про інциденти національному регулятору [16]. У 2021 році набув чинності «IT-Sicherheitsgesetz 2.0», який значно розширив повноваження Федерального відомства з безпеки інформаційних технологій (BSI) [93]: закон запровадив обов'язкову сертифікацію критично важливого обладнання (наприклад, обладнання мереж 5G), надав BSI повноваження видавати обов'язкові до виконання директиви щодо усунення вразливостей, встановив штрафи до 2 млн євро у разі невиконання вимог, а також створив правові підстави для заборони небезпечних постачальників (на практиці це означає заборону використання обладнання Huawei/ZTE у критично важливих мережах).

Франція інтегрувала вимоги НСД ще у 2018 році в Закон про цифрову безпеку та опублікувала кілька правил через агентство ANSSI (наприклад, вимоги до операторів основних послуг мати принаймні певну форму кіберзахисту). Естонія, яка має високорозвинену цифрову інфраструктуру, вже має окремий Закон про організацію державної інформаційної системи з 2009 року, а в 2018 році транспонувала Директиву NIS, запровадивши суворі вимоги до постачальників цифрових послуг. Таким чином, національне законодавство держав-членів ЄС описує та доповнює правила Союзу. Водночас, в рамках реалізації NIS 2 у період 2024-2025 років держави проводять масштабне оновлення свого законодавства з метою приведення його у відповідність до нових європейських стандартів. Так, наприклад, Німеччина розробляє поправки до закону про BSIG, Франція оновлює кіберстратегію та декрети щодо розширення переліку типів організацій, які підпадають під дію NIS 2, Італія у 2021 році створила незалежне Національне агентство з кібербезпеки тощо. Таким чином, взаємодія законодавства ЄС та національних законодавств у сфері

кібербезпеки є динамічною: Європейські правила встановлюють мінімальні пороги та схему співпраці, в той час як держави можуть запроваджувати більш жорсткі правила відповідно до свого досвіду та загроз».

У сучасному віртуальному просторі безпека кіберпростору та приватність особи – це дві сторони однієї медалі, а тому регуляторні структури ЄС демонструють їхню близькість. З одного боку, як ми вже говорили, GDPR приймає положення, що безпосередньо стосуються безпеки інформаційних систем як засобу (стаття 32), завдяки чому заходи кібербезпеки також передбачають жорстку відповідальність за порушення даних. З іншого боку, заходи кібербезпеки повинні також захищати право на недоторканність приватного життя: надмірний або незаконний моніторинг користувачів в ім'я кібербезпеки може суперечити GDPR. ЄС хоче зважити ці цілі в єдиному наборі правил. Наприклад, Директива NIS 2 в обов'язковому порядку вимагає співпраці між уповноваженими суб'єктами та органами захисту даних у разі інцидентів, пов'язаних з порушенням персональних даних (ст. 8(6) NIS 2), щоб переконатися, що заходи протидії кібератаці є комплексними і вирішують всі питання. Аналогічно, згодом, у 2020 році, Європейська рада із захисту даних (EDPB) надала пропозиції щодо того, як режими NIS та GDPR взаємодіють між собою, зосередившись на тому, щоб про кібератаки повідомлялося в рамках обох актів у тандемі (як кібернетичним органам, так і органам захисту даних) [8, с. 38]. Крім того, ЄС розробляє оновлений режим електронної приватності (новий Регламент про електронну приватність, який замінить Директиву 2002/58/ЄС) для забезпечення чіткого регулювання захисту електронного комунікаційного трафіку та метаданих, який також має конкретне застосування для цілей кібербезпеки (наприклад, законодавство про файли cookie, шифрування, сканування трафіку для цілей кібербезпеки). Загалом, нормативно-правова база ЄС підкреслює узгодженість цілей кібербезпеки та захисту даних, щоб забезпечити їхнє спільне застосування та взаємодоповнення.

3.2. Інституційна структура та механізми забезпечення кібербезпеки ЄС.

Європейський Союз створив ефективну систему інституцій та механізмів для забезпечення високого рівня кібербезпеки. Вона включає спеціалізовані агентства, мережі співпраці між країнами-членами, обмін інформацією та реагування на інциденти, а також державно-приватне партнерство. Протягом 2024-2025 років ця структура буде вдосконалюватися шляхом прийняття нового політичного законодавства та посилення існуючої структури. Проаналізуємо інституційну структуру кібербезпеки ЄС, відносини між основними органами та управління кризами на практиці, спираючись на законодавство ЄС та наукову літературу.

CERT-EU (Computer Emergency Response Team forEurope) – це спеціалізований підрозділ, який відповідає за кібербезпеку інституцій, органів та агенцій ЄС. CERT-EU діє з 2012 року на міжінституційному рівні, а в 2023 році його статус і мандат були об'єднані Регламентом (ЄС, Євратом) 2023/2841. Відповідно до цього Регламенту, CERT-EU було перейменовано на «Службу кібербезпеки для інституцій, органів та агентств ЄС» (скорочена назва CERT-EU була збережена через її впізнаваність), а її компетенції значно розширені. Зокрема, CERT-EU мав координувати реагування на кібератаки на інституційному рівні ЄС, здійснювати моніторинг та аналіз загроз і вразливостей, обмінюватися інформацією з усіма інституціями ЄС (ст. 12). CERT-EU діє як координаційний центр з розкриття вразливостей інституцій ЄС, оскільки національні координаційні центри знаходяться в державах-членах відповідно до NIS 2 (стаття 12(1) Директиви (ЄС) 2022/2555) (ст. 12(1)). CERT-EU також проводить тренінги та кібернавчання з ENISA, бере участь у кібернавчаннях ЄС та надає експертні консультації установам з питань кіберзахисту Розширений мандат до 2023 року зобов'язує голову CERT-EU регулярно звітувати перед новоствореною Радою з кібербезпеки (IICB) та подавати стандарти та пропозиції щодо покращення кіберстійкості інституцій

ЄС. Таким чином, CERT-EU став центральним технічним пунктом кіберзахисту на всіх рівнях інституцій ЄС [26].

ENISA (Агентство ЄС з кібербезпеки) також відіграє ключову роль як експертний центр та координатор. ENISA надає підтримку державам-членам та інституціям ЄС у формуванні політики кібербезпеки, забезпечує навчання та проводить регулярні загальноєвропейські навчання (наприклад, серія «Кібер Європа»). Агентство має постійний мандат в рамках Закону про кібербезпеку 2019 року (Регламент (ЄС) 2019/881) і відповідає за впровадження Європейської системи сертифікації кібербезпеки та розробку схем сертифікації продуктів та послуг ІКТ. Хоча в попередніх розділах було докладено значних зусиль для заглиблення в специфіку ролі ENISA, слід підкреслити його поточну роль як сегрегатора для конкретних мереж співпраці: ENISA надає адміністративну і технічну підтримку мережі CSIRTs і мережі EU-CyCLONe, сприяючи обміну інформацією між національними групами реагування і органами управління кризовими ситуаціями. Крім того, ENISA сприяє роботі нових центрів реагування (наприклад, Європейського кіберщита), надаючи ноу-хау та проводячи аналіз кібервразливостей [50].

Європейський центр компетенції з кібербезпеки (ECCC) – це нове агентство ЄС, створене у 2021 році для підтримки європейських можливостей, досліджень і технологій у сфері кібербезпеки. ECCC, відповідно до Регламенту (ЄС) 2021/887, розташований у Бухаресті та керує інфраструктурою національних координаційних центрів і координує діяльність на рівні держав-членів у сфері досліджень та інновацій. Центр був організований з метою спрямування фінансування ЄС (а саме «Горизонт Європа», «Цифрова Європа») на розвиток кіберінструментів високого рівня, промислового та наукового партнерства. ECCC розвиває Спільноту компетенцій – широку платформу, що представляє представників промисловості, наукових кіл та інших зацікавлених сторін. По суті, це Співтовариство є рамками державно-приватного партнерства, що дозволяє залучати експертизу приватного сектору до реалізації стратегії кібербезпеки ЄС та обмінюватися кращими практиками [45]. Наприклад,

Європейська організація з кібербезпеки (ECSO), створена у 2016 році як договірний партнер Європейської Комісії у сфері кібердосліджень, приєдналася до спільноти ECCC і досі робить значний внесок у координацію між галуззю та урядом [49].

Europol/EC3 (Європол та Європейський центр боротьби з кіберзлочинністю) є правоохоронним органом ЄС у сфері кібербезпеки. Європол через свій Центр кіберзлочинності (EC3) виявляє, розслідує та бореться з кіберзлочинністю, тісно співпрацюючи з національними правоохоронними органами. EC3 надає спеціалізовану та технічну допомогу в розслідуванні складних кібератак, координує спільні оперативні зусилля проти кіберзлочинних угруповань та бере участь у роботі Об'єднаної цільової групи з протидії кіберзлочинності (J-CAT) [44]. Хоча кримінальні питання є основним предметом занепокоєння Європолу, його діяльність перетинається із загальною структурою кібербезпеки ЄС: розвіддані про кіберзагрози та тактику кіберзловмисників, зібрані EC3, можуть бути передані іншим агентствам ЄС, включаючи CERT-EU та ENISA. Регламент 2023/2841 передбачає співпрацю в обміні інформацією між CERT-EU та Європолом/ЄК3, зокрема щодо тенденцій та загроз кіберзлочинності, що посилює міжінституційну координацію (ст. 12(5)). Таким чином, технічні та правоохоронні аспекти кібербезпеки ЄС взаємозалежні: EC3 займається забезпеченням дотримання законодавства щодо злочинців, тоді як CERT-EU та інші технічні органи зайняті нейтралізацією загроз і захистом інфраструктури тут і зараз.

Галузеві регуляторні органи сектору безпеки – галузеві органи ЄС все більше інтегрують кібербезпеку в сферу своєї компетенції. До них відносяться Європейське агентство з авіаційної безпеки (EASA), яке видає правила авіаційної кібербезпеки; Агентство ЄС із залізничних перевезень (ERA), яке встановлює специфікації кібербезпеки на залізничному транспорті; і Космічне агентство ЄС (EUSPA), яке забезпечує безпечну роботу систем Galileo/EGNOS і координує кібербезпеку космічних служб. Ці агентства мають зв'язки з центральними кіберінфраструктурами: наприклад, EASA та ENISA уклали угоди про

співпрацю, спрямовані на врахування кібернетичних загроз при створенні стандартів повітряного простору [66]. Члени таких агентств також входять до складу мереж співпраці ЄС: на підставі Регламенту 2023/2841 члени Мережі агентств ЄС (EUAN) входять до складу Міжвідомчої ради з кібербезпеки, яка координує міжгалузеві пріоритети у сфері кібербезпеки. Таким чином, галузевий вимір додає багатства інституційній структурі – кіберстійкість розглядається не лише як функція IT, а й як центральний сектор безпеки в транспорті, енергетиці, космосі та інших галузях.

EDA (Європейське оборонне агентство) – координує діяльність держав-членів у сфері військового кіберзахисту в рамках Спільної політики безпеки і оборони ЄС. Хоча кіберзахист, в кінцевому рахунку, є відповідальністю держав-членів, EDA відіграє вирішальну роль у розвитку спільних сил і засобів та проведенні навчань. Зокрема, EDA дозволяє створювати спільні кіберполігони і кібернавчальні курси для збройних сил ЄС. Агентство сприяло створенню Постійної структурованої співпраці (PESCO) у сфері кіберзахисту, прикладом якої є ініціатива «Кібернетичні групи швидкого реагування» (CRRT). В рамках цієї ініціативи деякі країни-члени (на чолі з Литвою) створили спільні групи кібер-експертів, які надаватимуть допомогу іншим країнам-членам у разі виникнення значних кіберзагроз на їхній запит. Вперше можливості такої команди були використані наприкінці 2022 року, коли CRRT здійснила виїзд на місця для виявлення вразливостей та підтримки кіберзахисту в реальних умовах. EDA також бере участь у створенні Військової мережі CERT (MICNET) – як зазначено в новій політиці кіберзахисту ЄС, вона буде спрямована на об’єднання військових груп реагування держав для обміну інформацією про загрози та координації дій. Внесок EDA вводить військовий компонент у загальну архітектуру кібербезпеки ЄС, а співпраця EDA з ENISA та Європолом, як зазначено у висновках Ради ЄС, має на меті гармонізувати військові та цивільні заходи реагування на кіберпростір [57, с.79-86].

Група співробітництва ННД є основною платформою для стратегічного співробітництва між державами-членами у сфері кібербезпеки. Створена

Директивою NIS 2016 року, її застосування було розширено Директивою (ЄС) 2022/2555 (NIS 2). Вона об'єднує представників національних органів кібербезпеки, Європейської Комісії та ENISA з метою вироблення спільних підходів, обміну політикою та найкращими практиками. Вона розробляє необов'язкові керівні принципи та рекомендації щодо імплементації Директиви NIS 2, сприяє гармонізації підходів держав-членів та розглядає транскордонні загрози [86, с. 3-7]. Група співробітництва стала основним майданчиком для зближення позицій, на приклад, щодо кібербезпеки мереж 5G, хмарних обчислень, мінімальних вимог безпеки для операторів критичної інфраструктури тощо [100, с. 228-233]. Варто підкреслити, що Директива CER 2022/2557 зобов'язує Групу співробітництва ННД проводити щонайменше щорічні спільні засідання з новоствореною Групою стійкості критично важливих об'єктів (CERG) з метою надання загальної оцінки кібер- та фізичних загроз. Таким чином, Група співробітництва ННД є міжцивільним національним координатором органів кібербезпеки для забезпечення узгодженості політики ЄС.

Мережа CSIRTs є оперативним механізмом співпраці між національними CERT/CSIRTs держав-членів. Вона також була створена Директивою NIS та змінена Директивою NIS 2 (стаття 14 Директиви 2022/2555). До її складу входять представники національних груп реагування та CERT-EU (від імені інституцій ЄС), а ENISA виконує функції її секретаріату. Мережа CSIRTs періодично збирається для обміну інформацією про кіберінциденти, технічний характер загроз, вразливості та заходи реагування. Вона створює стандартні процедури для комунікації у випадку транскордонних кібератак (так званий «blueprint»), координує спільні технічні навчання і тренінги між країнами. Роль мережі особливо очевидна у випадку масових кібератак: згідно з процедурою, якщо подія зачіпає кілька держав, мережа CSIRTs встановлює безпечні канали обміну інформацією (платформа MeliCERTes), координує технічний аналіз атаки та узгоджує спільні дії для її нейтралізації. Таким чином, мережа CSIRTs є технічним «хребтом» європейської системи реагування на кіберкризи, що

об’єднує можливості команд реагування всіх країн-членів ЄС та механізми ЄС [36, с. 528-529].

EU-CyCLONe (Європейська мережа зв’язку з кіберкризами) – це інноваційна організація, що відповідає за координацію реагування на кіберкризи на оперативному рівні. Офіційно створена відповідно до статті 16 Директиви NIS 2, EU-CyCLONe об’єднує представників національних органів управління кіберінцидентами та кризами (як правило, належним чином уповноважених посадових осіб в урядових підрозділах або відомствах) (ст. 16). ENISA забезпечує роботу секретаріату EU-CyCLONe, сприяючи розвитку інфраструктури та підтримці діалогу. Діяльність EU-CyCLONe полягає у швидкому обміні інформацією та оцінці ситуації у випадку великомасштабних інцидентів, спільному прийнятті рішень щодо заходів реагування, оцінці транскордонного впливу та наслідків атак, а також перенесенні потреб на політичний рівень (наприклад, попередження Ради ЄС). Мережу EU-CyCLONe очолює представник країни, яка головує в Раді ЄС, що сприяє інтеграції механізму в загальну систему кризового управління ЄС. Практика роботи EU-CyCLONe проявляється в типових кібероперація̈х: Проводяться CySOPEx (кібероперативні навчання для офіцерів) та BlueOLEx (навчання для вищих посадових осіб), де відпрацьовуються спільні дії в умовах загальноєвропейських сценаріїв кіберкриз. Таким чином, EU-CyCLONe об’єднує технічних фахівців (мережа CSIRT) та політиків, які приймають рішення: вона забезпечує оперативну координацію реагування на рівні різних держав та миттєве поширення інформації серед усіх зацікавлених сторін [51, с. 108-112].

CERG – це група з питань стійкості важливих об’єктів, створена відповідно до Директиви 2022/2557 (CER) для координації фізичної та кіберстійкості об’єктів критичної інфраструктури. CERG є експертною групою Європейської Комісії, що складається з одного представника від кожної держави-члена (з відповідним допуском до державної таємниці) та представників Комісії (ст. 19(2)). Її основним завданням є заохочення співпраці між державами в імплементації Директиви CER, обмін передовим досвідом у сфері захисту

критичних об’єктів, а також перегляд національних звітів і стратегій щодо ризиків та інцидентів (ст. 19(3) (a-g)). Вимагається, щоб CERG забезпечувала узгодженість стратегій кібербезпеки та фізичної безпеки: Стаття 19(5) Директиви прямо передбачає постійну співпрацю між CERG та Групою співробітництва ННД з метою обміну інформацією та розробки загальних рішень. Таким чином, CERG створює інституційний механізм координації між двома взаємопов’язаними вимірами безпеки – кібернетичним і фізичним – на стратегічному рівні. Ця спільнота вже розробляє непублічні рекомендації щодо оцінки загроз у різних секторах та навчання стійкості, а її діяльність буде спрямована на те, щоб зробити Союз більш підготовленим до протидії гібридним загрозам, які включають як кібератаки, так і фізичний вплив.

ІІСВ (Міжінституційна рада з питань кібербезпеки) – це новий координаційний орган в інституційній системі ЄС. Створена Регламентом 2023/2841, ІІСВ покликана забезпечувати належний рівень кібербезпеки в усіх інституціях та органах ЄС (ст. 10). До складу Ради входять представники основних інституцій (Парламенту, Ради, Комісії, Суду ЄС тощо) та три представники Мережі агентств ЄС (EUAN), а також представники Європейського центру компетенції з кібербезпеки (ECCC) та Європейського нагляду за захистом даних (EDPS). Головою ІІСВ є представник Європейської Комісії. ІІСВ несе відповідальність лише за моніторинг та надання допомоги у виконанні нового регламенту ЄС щодо інституційної кібербезпеки та забезпечує стратегічне керівництво CERT-EU. Зокрема, Рада затверджує довгострокову стратегію вдосконалення кібербезпеки інституцій ЄС, надає рекомендації керівнику CERT-EU та затверджує перелік послуг та рівні послуг, що надаються CERT-EU інституціям. ІІСВ також розглядає інституційні звіти про виконання заходів з кіберзахисту та уповноважений виносити обов’язкові до виконання постанови (заклики до дій) для усунення виявлених недоліків (ст. 7, 18). Таким чином, вперше в історії ЄС створено централізований механізм управління кібербезпекою внутрішньої мережі органів влади ЄС. ІІСВ дозволяє уникнути фрагментарних практик різних інституцій, забезпечує контакт на рівні експертів

(директор CERT-EU бере участь у всіх засіданнях Ради) та гарантує єдиний високий рівень безпеки інформаційних систем ЄС (ст. 15(2)). Цей приклад внутрішньої координації є важливим кроком до зміцнення кіберстійкості самого механізму ЄС [86].

Європейський кіберщит – це пропозиція щодо створення загальноєвропейського механізму раннього попередження та реагування на кіберзагрози, яка була реалізована в рамках Акту про кіберсолідарність ЄС 2023-2024 років. Він базується на підключенні національних і транскордонних операційних центрів безпеки (SOC) в ЄС до передових рішень зі штучного інтелекту та аналізу даних для моніторингу кіберпростору. Мережа SOC, що є складовою «кіберщита», виявляє індикатори кібератак у режимі реального часу та поширює попередження компетентним органам різних країн. Перший етап проекту розпочався в листопаді 2022 року, коли програма «Цифрова Європа» відібрала три транскордонні консорціуми SOCs з 17 держав-членів (та Ісландії) для пілотного розгортання цієї інфраструктури [52, с. 142-143]. Законодавчо, Регламент 2025/38 (Закон про кіберсолідарність) створює Європейську систему кіберсолідарності та деталізує умови, за яких вона може брати участь. Очікується, що «кіберщит» значно підвищить ситуативну обізнаність про кіберзагрози в усьому ЄС, з можливістю виявляти атаки на ранніх стадіях і запобігати їхньому перетворенню на масштабні інциденти. Наприклад, єдина мережа SOC полегшить миттєвий обмін індикаторами компрометації та іншими деталями між державами, що особливо корисно при роботі з APT-атаками або новими шкідливими програмами, що розробляються.

Механізм кіберсолідарності та реагування – це новий інструмент ЄС для підтримки готовності та скоординованого реагування на великі кіберподії. Він був створений тим же Законом про кіберсолідарність і складається з трьох основних компонентів: (1) Підготовча робота – фінансування та проведення колективних тестів на вразливість і стрес-тестів стратегічних підприємств у стратегічних секторах (енергетика, транспорт, фінанси, охорона здоров’я тощо) за загальноєвропейськими сценаріями ризиків; (2) Резерв кібербезпеки ЄС –

створення резервного пулу «довірених провайдерів» з приватного сектору, які на контрактній основі готові надавати послуги з реагування (реагування на інциденти, цифрова криміналістика, відновлення роботи системи) у випадку масованої атаки. Вперше створюються умови для швидкої мобілізації зовнішньої компетенції та ресурсів на підтримку постраждалої країни або інституції ЄС. Передбачається, що резерв складатиметься з акредитованих компаній ЄС, чиї послуги (наприклад, команди реагування на інциденти) можуть бути швидко мобілізовані за рахунок фінансування ЄС; (3) механізми взаємодопомоги – ефективний процес, за допомогою якого одна держава-член може офіційно звернутися за технічною допомогою до іншої у випадку кібератаки, а ЄС фінансуватиме та координуватиме таку місію підтримки. По суті, це такий самий інструмент солідарності, як і цивільний захист, але в кіберпросторі: заможна країна може направити експертів або групи реагування на допомогу іншій країні, і це координується на рівні ЄС [87].

Механізм солідарності також включає Механізм розгляду інцидентів у сфері кібербезпеки. За ініціативою Європейської Комісії або мереж EU-CyCLONe/CSIRTs ENISA зобов'язана провести пост-аудит конкретного значного або масштабного кіберінциденту та підготувати звіт з висновками та пропозиціями. Це стає звичайною практикою аналізу великих атак на рівні ЄС з метою систематичного підвищення готовності на основі досвіду реальних подій.

Обмін кіберінформацією та система оповіщення – на додаток до основних систем, ЄС будує технічні платформи для обміну інформацією між уповноваженими сторонами. З моменту прийняття першої Директиви про НІС існує платформа MeliCERTes, яка забезпечує платформу для безпечного обміну даними між національними CSIRT. Протягом останніх років були створені й інші федеративні інформаційні системи, які підтримують автоматизований обмін індикаторами загроз. Однією з цілей кіберстратегії ЄС є створення EFIS для федеративного обміну кіберданими між різними мережами та центрами. Бачення в цьому випадку полягає в тому, щоб зробити джерела кіберрозвідки, розрізнені від державних CERT, корпоративних SOC і файлів правоохоронних органів,

єдиним каналом співпраці за допомогою правових гарантій (захист від конкуренції, секретність тощо). Аналогічно, інформаційно-аналітичні центри (ІАЦ) набувають транскордонного характеру: Європейська комісія фінансує створення європейських ІАЦ у різних секторах (фінанси, енергетика, транспорт тощо). ISACs об'єднують компанії з певного сектору та зацікавлені органи влади для обміну технічною інформацією про інциденти, тенденції загроз та найкращі практики безпеки. Наприклад, Європейський фінансовий ISAC був створений у банківському секторі, де банки ЄС можуть обмінюватися інформацією про кібератаки, такі як DDoS або спроби вторгнення в платіжні системи, з регуляторами. Державно-приватний обмін інформацією в рамках ISAC не є обов'язковим, але активно заохочується Європейською Комісією: Стаття 11 NIS 2 зобов'язує держави створити умови для такого обміну та усунути правові перешкоди [72]. Таким чином, поряд з офіційними урядовими мережами в ЄС створюється альтернативне середовище обміну кіберрозвідданими з бізнесом, що підвищує загальний рівень обізнаності про загрози.

Інструментарій «кібердипломатії» ЄС також вражає, хоча і стосується зовнішньої сторони реагування. Цей набір дій дозволяє ЄС гармонізувати дипломатичні відповіді на зловмисну кіберактивність, наприклад, запровадження санкцій проти іноземних фізичних або юридичних осіб, причетних до кібератак. Наприклад, у 2020-2022 роках ЄС запровадив санкції проти виконавців атак WannaCry, NotPetya, Cloud Hopper тощо. Цей інструмент діє в рамках Спільної зовнішньої та безпекової політики, але у взаємодії з внутрішніми інституціями ЄС: статистичні дані CERT-EU, Європолу та національних розвідувальних служб можуть слугувати основою для прийняття рішень Радою ЄС. Хоча «кібердипломатичний інструментарій» виходить за рамки суто внутрішньої політики ЄС, він доповнює її у наданні політичної відповіді на кібератаки, особливо якщо вони є іноземними або належать до ширших геополітичних загроз [74, с. 1327-1331].

Іншою важливою сферою ДПП є галузеві інформаційно-аналітичні центри (ГІАЦ), про які згадувалося раніше. Вони діють як неофіційні центри довіри між

конкуруючими компаніями, які в іншому випадку могли б не ділитися інформацією про інциденти. Європейський енергетичний ISAC (EFISAC), транспортний ISAC тощо були створені за фінансування ЄС. На рівні ЄС консорціум EU-ISACs забезпечує налагодження взаємодії між окремими центрами та впорядковує протоколи обміну даними. Державно-приватний характер ISACs проявляється в тому, що бізнес є ініціатором зусиль, тоді як органи влади (регулятори, CERT) частіше виступають у ролі спостерігачів або дорадчих зацікавлених сторін, які отримують оперативну інформацію про атаки від бізнесу та роблять відповідні попередження та рекомендації [78, с. 400-404].

Іншим рівнем партнерства є залучення приватних суб'єктів до швидкого реагування. Чудовим прикладом є новий резерв кібербезпеки ЄС, створений Законом про кіберсолідарність: приватні корпорації стають офіційними партнерами ЄС з реагування на кризові ситуації, сертифікованими як «довірені провайдери» (Trusted Providers). Це формалізує ринок керованих послуг з кібербезпеки в ЄС. Однією з віх стало внесення цільової поправки до Закону про кібербезпеку (Регламент 2025/37), яка встановлює схеми сертифікації керованих послуг з безпеки (наприклад, реагування на інциденти, пентестування, аудит безпеки) [87]. Таким чином, ЄС стимулює виробництво високоякісних послуг і вселяє довіру до них, щоб державні органи могли безпечно користуватися послугами приватних фахівців. Така «передова» співпраця означає, що під час екстремальної атаки, скажімо, на європейську енергосистему, найкращі приватні команди, найняті ЄС, працюватимуть спільно з державними експертами.

Нарешті, в рамках моделі ДПП також проводяться спільні тренінги та навчання. ENISA також регулярно проводить масові кібернавчання, відомі як «Кібер Європа», в яких беруть участь державні органи влади та ключові постачальники послуг (банки, телекомунікаційні компанії, енергетичні оператори). Це зміцнює їхню довіру один до одного та відпрацьовує ситуації взаємодії. Так само платформа Cybersecurity Skills Academy, запущена у 2023 році, була розроблена завдяки партнерству між державою та великими IT-компаніями, щоб обійти дефіцит кадрів – бізнес допомагає розробляти навчальні

програми та забезпечувати стажування, а державний сектор стандартизує освіту та сертифікує навички [60].

Таким чином, державно-приватне партнерство в ЄС охоплює стратегічний рівень (спільне планування інновацій через ECCC/ECSO), операційний рівень (обмін інформацією через ISACs, спільне реагування через резерв) та людський фактор (навчання). Ця багаторівнева модель максимально використовує досвід приватного сектору, що є критично важливим у швидкозмінній сфері кіберзагроз.

Робота Європейської служби зовнішніх справ (ЄСЗС), і зокрема Відділу кібербезпеки ЄСЗС, зараз стала важливою для координації зовнішніх і внутрішніх аспектів кібербезпеки. ЄСЗС забезпечує кібердіалоги з третіми країнами, а також організовує так звані Кібердіалоги високого рівня між столицями і брюссельською штаб-квартирою, де зустрічаються представники міністерств закордонних справ, міністерств оборони та ІТ-агентств країн-членів ЄС. Метою цих дискусій є обмін стратегічною інформацією про небезпеки (зовнішні та внутрішні для ЄС) та узгодження позицій на міжнародних майданчиках (ООН, ОБСЄ) щодо відповідальної поведінки держав у кіберпросторі. Така багатостороння форма обговорення гарантує, що цивільні, військові та дипломатичні голоси ЄС будуть почуті в однаковій мірі з питань глобальної кіберстабільності [75 с. 4-11].

Загалом, Європейський Союз рухається до моделі «безшовного кіберпростору», де різні інституційні елементи – від національних CERT до військового кіберкомандування – є частиною єдиного механізму реагування на кризові ситуації. На думку науковців, ЄС прагне створити «нормативну базу для активних заходів кіберзахисту», щоб у разі необхідності використовувати весь арсенал можливостей без мілітаризації кіберпростору Союзу. Зокрема, незважаючи на інтеграцію, розподіл повноважень залишається чітким: цивільні інституції керуються правовою базою NIS 2 та пов’язаними з нею актами, військові – національними завданнями та координацією через EDA, а правоохоронні органи – мандатом Європолу. Координація забезпечується за

допомогою обміну інформацією, спільних структур (наприклад, EU-CyCLONe або CERG) і взаємоузгоджених стратегій. Процедури проактивного врегулювання криз (наприклад, протокол Blueprint у 2017 році) вже включають паралельну взаємодію: технічну оцінку Мережею CSIRTs, оперативну синхронізацію EU-CyCLONe, політичне рішення IPCR, дипломатичну відповідь за допомогою інструментів кібердипломатії та оборонну готовність за допомогою координації EEAS/EDA. Така багатостороння відповідь покликана забезпечити стійкість і гнучкість ЄС перед кібератаками будь-якого масштабу.

Стратегічні документи відіграють вирішальну роль у відображенні цієї взаємодії. У Кіберстратегії ЄС до 2020 року вперше чітко вказано на необхідність створення Спільного кіберпідрозділу як платформи для співпраці спільнот у кризові часи. Хоча JCU все ще не є актуальною у фізичному сенсі як координаційна програма, її концепція – віртуальний спільний кіберкризовий центр – вже існує через вищезгадані інструменти (EU-CyCLONe та ін.). Стратегічний компас (2022) і рекомендації Ради з кіберзахисту 2023 року формують політику, на основі якої ЄС повинен: розгорнути перші спільні кібернавчання ЄС і НАТО наприкінці 2020-х років, створити європейський центр кіберрозвідки і забезпечити взаємну підтримку між ННД 2 і оборонними заходами. Ці керівні принципи гарантують, що планування в цивільному і військовому секторах враховують один одного.

Таким чином, інституційна структура ЄС для забезпечення кібербезпеки у 2024-2025 роках є взаємопов’язаною системою механізмів і органів, що включає: координацію регулювання (Група співробітництва ННД, CERG), технічне і оперативне реагування (CSIRTs Network, EU-CyCLONe, CERT-EU), правоохоронний і розвідувальний компоненти (Європол/EC3, обмін розвідданими), оборонний компонент (EDA, PESCO, MICNET), а також тісну співпрацю з приватним сектором (ECCC, ISACs, Кіберрезерв). Конвергенція цивільного, технічного та військового вимірів, підкріплена стратегічними рамками, дозволяє ЄС протидіяти кіберзагрозам у цілісний та інтегрований спосіб, безпрецедентно підвищуючи загальну кіберстійкість Союзу.

3.3. Співпраця України та ЄС у посиленні кіберстійкості держав.

З початком російської агресії Європейський Союз значно збільшив підтримку кіберстійкості України. Існує низка спільних ініціатив та проєктів, спрямованих на покращення кібербезпеки української держави. Однією з них є ініціатива EU4Digital, яка підтримує цифровий розвиток та кібербезпеку в країнах Східного партнерства, включаючи Україну. Зокрема, програма EU4DigitalUA (2020-2025) у розмірі 20,5 млн євро забезпечує гармонізацію цифрового простору України з Єдиним цифровим ринком ЄС, розвиток електронного урядування, посилення кібербезпеки та захисту персональних даних [42]. Проект розвивається на базі ініціативи EGOV4Ukraine, яка забезпечила необхідну інфраструктуру для надання електронних послуг (система обміну даними «Трембіта» тощо). Важливу роль у реалізації EU4DigitalUA відіграють європейські партнери – Естонська академія електронного урядування та іспанський фонд FIIAPP, які реалізують аспекти кібербезпеки та захисту даних.

Під час початку повномасштабної війни ЄС оперативно запустив окремі проекти екстреної кібердопомоги для України. У березні 2022 року стартував проєкт ЄС «Підтримка посилення кібербезпеки в Україні» з акцентом на швидке реагування на кібератаки та підвищення стійкості державних послуг. Вартість цього проєкту склала понад 10 мільйонів євро (кошти NDICI), які були витрачені до лютого 2023 року на невідкладні потреби кіберзахисту. Проєкт реалізовувався Естонською академією електронного урядування у тісній співпраці з Міністерством цифрової трансформації України. Він мав три пріоритети: по-перше, фінансування системи безпечного обміну даними «Трембіта» та захист державних реєстрів (виявлення та нейтралізація кіберзагроз); по-друге, захист критичної інфраструктури та публічної інформації, включаючи заміну знищеного обладнання; по-третє, надання інструментів безпеки фахівцям, які обслуговують критичні системи. Ці зусилля надали Україні цінні ресурси для підтримки цифрових державних послуг та захисту даних протягом першого півріччя конфлікту – як зазначив Віце прем’єр-міністр Михайло Федоров,

«цифрова держава (портал і додаток “Дія”) продовжує працювати, а урядові дані – у безпеці» [5].

Окрім короткострокових заходів, ЄС також залучає Україну до середньо- та довгострокових цифрових ініціатив. Україна стала першою країною-партнером, яка приєдналася до програми «Цифрова Європа» у вересні 2022 року. Це дозволяє українським організаціям подавати заявки на фінансування спільних проєктів у сфері високопродуктивних обчислень, штучного інтелекту, цифрових навичок та кібербезпеки. Зокрема, партнерство з «Цифровою Європою» дозволяє Україні долучитися до створення Європейського кіберрезерву – колективного ресурсу для протидії масштабним кібератакам. Саме через цей процес Україна долучиться до реалізації Акту про кіберсолідарність ЄС, нового інструменту ЄС, який дозволяє створити загальноєвропейську систему оперативної кіберпідтримки. Україна, за словами Михайла Федорова, прагне приєднатися до Кіберрезерву ЄС в рамках програми «Цифрова Європа», що дозволить зміцнити критичну інфраструктуру та посилити захист від російської агресії [14].

Також варто згадати проєкт EU4Digital: CyberEast, що реалізується у співпраці з Радою Європи протягом 2019-2023 років для країн Східного партнерства. CyberEast спрямований на розвиток потенціалу для переслідування кіберзлочинів, впровадження стандартів Будапештської конвенції та загальне підвищення кіберстійкості інфраструктури в Україні, Молдові, Грузії та інших країнах регіону. У вересні 2023 року розпочалася нова фаза програми «КіберСхід+», яка продовжує розпочату діяльність, а саме: тренінги для українських правоохоронних органів та обмін досвідом щодо захисту критично важливих систем. Залучаючи Україну до регіональних ініціатив з розвитку кіберпростору, ЄС таким чином сприяє передачі найкращих практик кіберзахисту та підвищенню кваліфікації українських експертів [31].

Також варто згадати Національну програму інформатизації (НПІ) України, державну програму цифрового розвитку, яка була оновлена у 2023 році і також спрямована на кібербезпеку. НПІ спрямована на створення нової інформаційної інфраструктури, застосування цифрових технологій та підвищення рівня

кібербезпеки держави. Європейський Союз надає підтримку в реалізації НІС шляхом експертної та фінансової допомоги в рамках своїх програм цифрової трансформації. Звіти EU4Digital показують, що у 2023 році заходи НІС вже вплинули на безпеку та ефективність органів державної влади та підвищили цифрову компетентність громадян [43].

Значного прогресу було досягнуто з Агентством ЄС з питань кібербезпеки (ENISA). У листопаді 2023 року Україна та ENISA підписали історичну Робочу угоду – першу в своєму роді з країною за межами ЄС. Угода передбачає структуровану співпрацю у короткостроковій перспективі та закладає основу для довгострокового зближення політик у сфері кібербезпеки [103]. Серед практичних дій – залучення українських посадовців до загальноєвропейських кібернавчань та тренінгів як партнерів або спостерігачів; можливість відрядження українських експертів до інституцій ЄС для обміну досвідом; спільне використання засобів підвищення обізнаності у сфері кібергігієни. Ще один напрямок – обмін кращими практиками щодо гармонізації законодавства, наприклад, прийняття Директиви NIS2 в Україні. Також триватиме обговорення ситуаційної обізнаності: обмін аналітичною інформацією про кіберзагрози та моделі атак з метою вироблення спільного розуміння загрозливого середовища. Високий представник ЄС Жозеп Боррель підкреслив, що ця угода є лише частиною загальної підтримки, спрямованої на допомогу Україні в захисті від російської агресії в кіберсфері, а Секретар РНБО Олексій Данілов наголосив, що відтепер Україна разом з ЄС долучатиметься до створення стратегічних стратегій та політики кібербезпеки на міжнародному рівні [67].

Саме завдяки цій співпраці стало можливим залучення України до навчань ENISA «Кібер Європа». «Кібер Європа» – це тренувальна кібератака на критичну інфраструктуру кількох країн, яка відбувається в масовому масштабі протягом двох років. Наразі ми опрацьовуємо питання щодо участі українських експертів у майбутніх навчаннях у якості спостерігачів, щоб разом з європейськими партнерами отримати безцінний досвід реагування на кризові ситуації. У 2022 році Україна вже брала участь у деяких міжнародних кібернавчаннях

(наприклад, в рамках платформ НАТО), а тепер, можливо, стане частиною тренувальних процесів ЄС.

Те саме можна сказати і про процеси управління кіберкризами в ЄС. EU-CyCLONe (EU Cyber Crisis Liaison Liaison Network) та Національна мережа CSIRTs були створені в рамках першої Директиви NIS і об'єднують відповідальних національних представників країн-членів для співпраці та узгоджених дій під час довготривалих кібератак. Україна не є повноправним членом цих структур, але після отримання статусу кандидата та гармонізації з NIS2 Україна буде частково залучена до роботи, що проводиться цими мережами. Вже зараз українські компетентні органи (Держспецзв'язку, РНБО та ін.) мають оперативні контакти з EU-CyCLONe та спільно відпрацьовують сценарії кіберкризових ситуацій. Потенціал отримувати ранні попередження про загальноєвропейські події та координувати дії за допомогою цих засобів значно підвищує готовність України до кіберінцидентів.

Україна також бере активну участь у європейській правоохоронній мережі у сфері кібербезпеки. З 2016 року діє угода про оперативне співробітництво з Європолом, а у 2022-2023 роках проводилися спільні операції з Європолом з протидії кіберзлочинності, пов'язаній з війною (нейтралізація бот-мереж, захоплення серверів для здійснення атак). У 2023 році Європол підписав з Україною оперативну угоду про обмін інформацією щодо кіберзагроз, що доповнює суто військовий аспект кіберспівпраці. Таким чином, створено багаторівневу систему координації: стратегічну, тобто участь у кібердискусіях та робочих групах ENISA; оперативну, тобто обмін інформацією через CERT-EU, Європол, EU-CyCLONe; тактичну, тобто спільні навчання та тренування.

ЄС зараховує Україну до загальноєвропейської системи кібербезпеки. У спільній заяві для преси за підсумками 3-го Кібердіалогу Україна-ЄС (липень 2024 року) сторони звернули увагу на те, що у воєнний час кіберзагроза України є загрозою і для Європи, а покращення співпраці є спільним інтересом. ЄС пообіцяв додаткову всебічну підтримку кіберстійкості України та глибшу інтеграцію українських інституцій у європейські механізми обміну інформацією,

навчання та колективного реагування [2]. Налагодження такої координації вже принесло свої плоди: у 2022-2023 роках українські та європейські експерти спільно ідентифікували низку російських хакерських спільнот та обмінялися технічними даними про шкідливе програмне забезпечення, яке було націлене на енергетичні об'єкти та банки. Таким чином, інтеграція України до координаційних структур ЄС у сфері кібербезпеки не лише покращує власну безпеку, а й підвищує безпеку всього європейського кіберпростору.

PESCO (Permanent Structured Cooperation) – це оборонна структура ЄС, яка реалізує спільні проекти з розвитку потенціалу збройних сил, наприклад, у сфері кіберзахисту. Україна, як країна, що не є членом ЄС, зацікавлена у приєднанні до окремих проектів PESCO, зокрема у сфері кібербезпеки. Вже є відчутні плоди співпраці: у лютому 2022 року, на початку російської атаки, на прохання України була розгорнута Кібернетична група швидкого реагування ЄС (CRRT) – це перший випадок, коли спроможність, розроблена PESCO, була розгорнута для підтримки третьої країни.

Групи швидкого реагування на кібератаки (CRRT) є одним з ключових елементів кіберзахисту PESCO, ініціатором створення якого виступила Литва. Шість країн-членів ЄС (Естонія, Литва, Польща, Хорватія, Румунія, Нідерланди) створили колективну команду з 8-12 кібер-експертів, які можуть бути швидко розгорнуті для надання допомоги в разі кібератак. 23 лютого 2022 року Міністерство оборони Литви публічно оголосило про розгортання CRRT на прохання України – експерти команди почали надавати допомогу українським установам у сфері кіберзахисту дистанційно та з можливими виїздами на місця. Найважливішими напрямками діяльності CRRT були допомога в розслідуванні кіберінцидентів, цифрова криміналістика, сканування вразливостей та консультації щодо покращення безпеки мереж.

Поглиблення співпраці України з PESCO стало більш можливим після отримання статусу кандидата. У 2023 році набули чинності нові правила, які дозволяють третім країнам приєднуватися до певних проєктів PESCO в якості гостей за ініціативою учасників. Український уряд також висловив

зацікавленість в участі у кіберпроєктах PESCO – не лише CRRT, а й інших, таких як проєкт зі створення Європейського координаційного центру кіберзахисту або обміну інформацією про кібервразливості. План заходів з реалізації зовнішньополітичної стратегії України (затверджений урядом у квітні 2023 року) чітко передбачає завдання щодо участі України в окремих обраних безпекових проєктах PESCO.

Кіберсанкції ЄС, які є ключовим компонентом «дипломатичного інструментарію», також слугують інтересам України. Вже у 2020 році ЄС вперше запровадив санкції проти фізичних та юридичних осіб, які стоять за масованими кібератаками (зокрема, вірусом NotPetya, спрямованим на українські мережі у 2017 році). Санкції були застосовані до офіцерів російської військової розвідки, які брали участь в операції проти України. Також було посилено санкційний механізм: з 2023 року під кіберсанкції ЄС підпадають найбільш значні хакерські групи ГРУ, націлені на українські енергетичні та державні установи. Україна надає ЄС докази для прийняття такого рішення – дані розвідки, результати операцій СБУ тощо. Фактично формується єдина політика стримування: З одного боку, Україна розвиває свій спротив, а з іншого – ЄС створює міжнародний тиск на агресора через санкції та правові заходи.

По-третє, під егідою Спільної зовнішньої та безпекової політики (СЗБП) Україна узгоджує свої дії з ЄС, прагнучи встановити норми для міжнародного кіберпростору на глобальному рівні. Обидві країни поділяють свої зобов’язання щодо рамок ООН щодо кібервідповідальної поведінки держав та норм міжнародного права для кіберпростору. На практиці це означає, що Україна та ЄС у спільних публічних заявах засуджують агресивну кіберактивність Росії на міжнародній арені та виступають за створення механізмів відповідальності для кібератак (аж до Міжнародного суду ООН, якщо кібератака є частиною збройної агресії).

Таким чином, завдяки співпраці в рамках PESCO та інструментам кібердипломатії ЄС Україна отримує подвійну вигоду: негайну допомогу у створенні кіберзахисту (як у випадку з групами швидкого реагування) та в

довгостроковій перспективі на міжнародній арені для стримування та санкціонування кіберагресії. З іншого боку, Європейський Союз зміцнює власну безпеку, спираючись на унікальний досвід України у боротьбі з російськими хакерами та створюючи прецедент колективної відповіді на кібератаки за межами своїх кордонів.

Найбільш актуальною є імплементація Директиви ЄС NIS2 (2022/2555) про безпеку мереж та інформаційних систем. NIS2 закріплює існуючі стандарти кібербезпеки для низки ключових секторів інфраструктури. Україна вже розпочала імплементацію цієї директиви: Михайло Федоров стверджує, що вже ведеться велика робота з приведення українського законодавства у відповідність до NIS2. Це буде використано для підвищення стійкості критичної інфраструктури України та посилення захисту від нападів з боку Росії, зокрема, енергетичних, транспортних та фінансових об’єктів. Директива NIS2 набула чинності в ЄС 16 січня 2023 року, і держави-члени мають до жовтня 2024 року імплементувати її положення в національне законодавство. Україна намагається не відставати: у 2023 році при Раді національної безпеки і оборони було створено міжвідомчу робочу групу для перегляду положень NIS2 та імплементації їх у новий закон про критичну інформаційну інфраструктуру. Фактично йдеться про часткове приєднання України до NIS2 ще до набуття членства, шляхом одностороннього віддзеркалення його вимог у національних нормативно-правових актах.

Аналогічним чином триває процес імплементації Директиви CER (Critical Entities Resilience Directive, 2022/2557), яка регулює питання стійкості критично важливих суб’єктів господарювання. Директива CER слідує за NIS2 у висвітленні фізичного захисту та стійкості критичної інфраструктури (енергетика, транспорт, водопостачання, цифрова інфраструктура тощо) до різних видів загроз, включаючи кібератаки. Розглядається можливість використання Україною деяких положень CER, а саме здійснення оцінки ризиків основних об’єктів та застосування заходів для забезпечення стійкості їх функціонування. Це стало особливо актуальним після масштабних російських

атак на енергетичну систему, оскільки кіберзахист залежить від фізичної безпеки. Часткова гармонізація з КЗК сприятиме членству в системі колективної безпеки європейської критичної інфраструктури, коли українські об'єкти (наприклад, енергосистеми, що належать до європейської мережі ENTSO-E) будуть розглядатися в рамках спільної системи безпеки.

На високому рівні характерними є спільні заяви за підсумками самітів Україна-ЄС. Наприклад, Спільна заява 24-го саміту (3 лютого 2023 року, Київ) містила спеціальний розділ, присвячений боротьбі з кібератаками та гібридними загрозами. ЄС підтвердив свою солідарність з Україною у протистоянні кібер- та гібридним атакам і пообіцяв продовжувати підтримку у цій сфері. Члени Комісії відзначили інтенсифікацію співпраці у сфері кібербезпеки та намір досягти конкретних результатів інтеграції, а також підкреслили необхідність протидії російській пропаганді та забезпечення стійкості кіберінфраструктури України. Ця заява фактично об'єднала існуючі проєкти (наприклад, допомога ЄС у забезпеченні кіберстійкості енергетичного сектору під час атак на нього взимку 2022-23 років) та окреслила нові контури, наприклад, залучення України до європейських інструментів управління кіберкризами [1].

Подібні положення містилися також у спільних комюніке за підсумками зустрічей високого рівня. Наприклад, спільне засідання Уряду України та Європейської Комісії у лютому 2023 року завершилося підписанням планів наближення України до цифрового ринку ЄС, де кібербезпека визначена як пріоритет. ЄС послався на «приклад стійкості України до кібератак» і заявив про готовність залучити Україну до майбутніх ініціатив ЄС у сфері кібербезпеки. Це було підкріплено на практиці: у липні 2023 року Україна отримала спеціальний дозвіл на підписання операційної угоди з ENISA, що вимагало рішення Єврокомісії (оскільки раніше цього не було). Іншими словами, політичні домовленості санкціонували бюрократичні процедури для інтенсифікації співпраці. Одним із найважливіших документів стала Спільна заява на підтримку України, підписана 12 липня 2023 року керівництвом ЄС та більшістю країн-членів на саміті НАТО у Вільнюсі. Будучи рамковим документом щодо гарантій

безпеки, вона, зокрема, передбачає розгляд можливості використання всього обсягу наявної Угоди про асоціацію та інших інструментів для надання допомоги Україні у сфері безпеки, включаючи кібербезпеку. Фактично, ЄС взяв на себе довгострокове зобов'язання підтримувати відновлення України та зміцнення її кібернетичного імунітету проти майбутніх загроз у рамках загальних гарантій безпеки.

Двосторонні домовленості між Україною та ЄС не є єдиними; резолюції Європейського парламенту також мають значення. У резолюції ЄП від 19 травня 2022 року про наслідки війни для Європи депутати Європарламенту, зокрема, закликали держави-члени та Європейську комісію надати Україні максимальну підтримку для її кібербезпеки, зокрема обладнання, програмне забезпечення та допомогу фахівців, а також посилити координацію у протидії російським кібератакам. Ця політична резолюція висловила згоду серед законодавців ЄС щодо необхідності інтеграції України в європейські кіберсистеми.

На національному рівні, як згадувалося раніше, Кабінет Міністрів України ухвалив рішення про підтримку Плану заходів з реалізації Стратегії зовнішньої політики до 2023 року, який прямо включає кроки з кіберінтеграції: співпрацю з ENISA, членство в коаліціях ЄС з протидії кіберзагрозам тощо. Документ є внутрішньою дорожньою картою, що відповідає політичним деклараціям ЄС. Ці заяви та документи не є формальними юридичними документами, але вони важливі: вони артикулюють узгодженість стратегічного бачення Києва та Брюсселя щодо кібербезпеки та створюють політичний імпульс для реалізації окремих проектів. У 2022 році і надалі тональність цих заяв кардинально змінилася – від загальних намірів до прямих слів про інтеграцію та взаємну протидію противнику в кіберсфері. Це означає, що кібербезпека була включена до порядку денного Україна-ЄС і стала одним із критеріїв готовності України до членства.

2022-2024 роки, коли відбувалася повномасштабна війна, стали випробуванням на міцність для кіберстійкості України та інституційної основи

міжнародної солідарності в кіберпросторі. У ці роки відбулося кілька серйозних кібератак, які вимагали спільної відповіді з боку України та ЄС.

Однією з перших таких атак стала масована кібератака в ніч на 24 лютого 2022 року на супутникову мережу Viasat KA-SAT, що забезпечує доступ до Інтернету в Україні. Атака, здійснена російськими хакерами, вивела з ладу тисячі модемів одночасно в Україні та спричинила перебої в роботі інших європейських країн (зокрема, дистанційне відключення близько 5800 вітрових турбін у Німеччині). Реакція ЄС була швидкою: протягом декількох днів Європейська служба зовнішніх справ організувала обмін інформацією з українськими чиновниками про технічні деталі атаки. 10 травня 2022 року ЄС офіційно поклав відповідальність за цю кібератаку на Росію та підтвердив зацікавленість ЄС у протидії таким атакам у співпраці з Україною, а також охарактеризував атаку KA-SAT як приклад дій держави-агресора в кіберпросторі, які можна назвати лише безвідповідальними. Важливо, що ЄС вже попереджав про ризик «ефекту зараження», коли атака на Україну може мати системні наслідки для європейської безпеки, і це сприяло поглибленню взаємодії ЄС з українським кіберзахистом.

Задовго до початку вторгнення, у січні 2022 року, українські урядові веб-сайти зазнали масованої атаки з погрозливими повідомленнями. ЄС вперше ініціював «Механізм координації кіберкриз» (так званий «Талліннський механізм»), щоб об’єднати свої держави-члени для підтримки України. Хоча цей механізм не має офіційного статусу, країни ЄС, включаючи Литву, Польщу та Румунію, негайно направили експертів та обладнання для підтримки українських команд реагування. Це стало передумовою для подальшого розгортання Групи кібернетичного реагування PESCO (CRRT), про що вже згадувалося раніше. Таке непряме європейське втручання у відбиття атаки стало підтвердженням того, що союзники готові до дій у відповідь ще до офіційних дій [8].

У 2022 році українські та європейські експерти співпрацювали, щоб запобігти численним прикладам зловмисних атак у стилі «двірник», які російські хакери проводили проти українських систем (WhisperGate, CaddyWiper та ін.).

Інформація про ці загрози була негайно передана через платформи обміну CERT-EU та мережі кіберрозвідки всім членам ЄС, щоб вони могли посилити власні системи на випадок спроб поширення вірусу за межами України. Наприклад, шкідливе програмне забезпечення Industroyer2, виявлене у квітні 2022 року під час спроби відключення підстанції Укренерго, було спільно досліджено Держспецзв'язку України та словацькими фахівцями ESET, після чого ENEISA опублікувала попередження для операторів мереж ЄС про характеристики шкідливого програмного забезпечення. Такого рівня координації в режимі реального часу не існувало до 2022 року і стало прямим наслідком війни.

Восени 2022 та 2023 років, коли Росія відкрито бомбардувала транспортну та енергетичну інфраструктуру України, ЄС надав не лише технічну, а й стратегічну підтримку в кіберзахисті критично важливих секторів. Європейська Комісія та відповідні відомства організували серію тренінгів та консультацій для українських операторів інфраструктури щодо кіберстійкості у разі нападу, зокрема в рамках ініціативи ЄС «Енергетична стійкість» (яка мала кіберкомпонент). Водночас, у грудні 2022 року на Паризькій конференції з відновлення України було започатковано механізм координації допомоги у сфері енергетичної та цифрової стійкості, в рамках якого ЄС разом з G7 бере участь у постачанні в Україну обладнання та ноу-хау для відновлення пошкоджень, спричинених атаками. У кіберпросторі це передбачає переміщення ще більшої кількості систем резервного копіювання даних, супутникових терміналів, зашифрованого зв'язку – всього того, що дозволяє державним службам працювати в режимі онлайн навіть під час атак на них.

Окремо слід відзначити Консультативну місію ЄС в Україні (КМЄС) – цивільну місію ЄС, яка з 2016 року підтримує реформування сектору цивільної безпеки. Після початку війни КМЄС переорієнтувала свої зусилля на надання консультацій з питань кібербезпеки Міністерству внутрішніх справ, Службі безпеки України та Прокуратурі. У 2022-2023 роках КМЄС провела серію тренінгів з розслідування кіберзлочинів, пов'язаних з війною, та навчань для відпрацювання спільного реагування поліції та ІТ-спеціалістів на кібератаки в

містах. Це призвело до посилення співпраці між українськими правоохоронними органами та їхніми колегами з ЄС, такими як Європол та Євроюст, у розслідуванні транскордонних кіберзлочинів, таких як атаки з вимогами викупу, що пов'язані з Росією та Білоруссю.

Така ж реакція була досягнута і в інформаційній сфері. ЄС та Україна діяли в тандемі проти кремлівських хвиль дезінформації та кібератак, що підривають підтримку України на Заході. Платформа EU vs Disinfo тісно співпрацює з українським Центром протидії дезінформації для викриття фейків та кіберпровокацій. Коли російське кібершпигунство націлилося на європейські ресурси (наприклад, DDoS-атаки на сайти урядів Польщі та Фінляндії), українські фахівці надали розвіддані про тих, хто за цим стоїть (групи KillNet тощо), щоб допомогти ЄС вжити контрзаходів. У відповідь український інформаційний простір став на захист європейських союзників: Компанії ЄС з ініціативи урядів перенаправляли частину інтернет-трафіку України в захищені канали, щоб зменшити вплив DDoS-атак.

Як наслідок, у 2022-2024 роках відбулася надзвичайна колективна відповідь на кіберагресію. Україна стала своєрідною «тестовою зоною», де відточувалися інструменти кіберспівпраці, теоретично задумані, але ще не випробувані на практиці. ЄС вперше використав свої спільні інструменти (CRRT, дипломатичні ноти, санкції) в інтересах держави-партнера, а Україна продемонструвала, що досвід та уроки з нього визначають обороноздатність Європи. Цей синергетичний підхід, коли напад на одного розглядається як спільна перешкода, з якою стикаються всі, став новим стандартом у відносинах між Україною та ЄС. Він не лише виявився ефективним у відбитті конкретних кібератак під час війни, але й заклав основу для довгострокової співпраці у сфері кібербезпеки між Україною та Європейським Союзом, яка залишиться актуальною і після завершення бойових дій.

Висновки до третього розділу

Війна росії проти України стала і випробуванням, і каталізатором для формування нової європейської архітектури кібербезпеки. Перед обличчям

зростаючих глобальних ризиків, ескалації агресивної поведінки авторитарних режимів і невизначеності щодо майбутніх конфліктів, Європейському Союзу вдалося розпочати перехід до більш стійкої, взаємопов'язаної та інноваційно підтримуваної системи кіберзахисту. Але ця система потребує подальшого розвитку: від удосконалення технологій та правового регулювання до зміцнення громадської обізнаності, медіаграмотності та політичної волі. Лише шляхом поєднання стратегічного бачення, інституційної готовності та єдності дій Європейський Союз зможе ефективно захистити себе в епоху цифрових технологій, де безпека не обмежується державними кордонами, а атаки здійснюються не через кордони, а через мережі.

Висновки

Війна Російської Федерації проти України, яка розгорнулась до повномасштабної в лютому 2022 року, стала переломним моментом у розвитку глобальної системи безпеки. Одним із найменш помітних, але водночас найбільш руйнівних фронтів цього конфлікту став кіберпростір. Аналіз показує, що кіберагресія в рамках гібридної війни стала ключовим інструментом реалізації стратегічних цілей Кремля. Це включає не лише суто технічні атаки на інформаційні системи, а й широкомасштабне використання кібершпигунства, диверсій, руйнівного впливу на критичну інфраструктуру, а також інтенсивні інформаційно-психологічні операції, які мають глибокі наслідки для цифрової безпеки країн Європейського Союзу.

В умовах російсько-української війни кібероперації перестали бути допоміжним компонентом і набули самостійного політико-стратегічного значення. Російські атаки мають комплексний характер: вони поєднують елементи деструктивного програмного забезпечення (вайпери), шкідливі кампанії зі злому облікових записів чиновників, паралізування енергетичних і транспортних систем, порушення супутникового зв’язку, кібершпигунство і навіть хакерські атаки, які реалізуються з метою маніпулювання суспільною свідомістю. Усі ці атаки формують новий тип загрози – транскордонну, політично вмотивовану, гнучку за формою та невловиму за змістом. Росія використовує кіберзасоби як інструмент для прихованого впливу на ЄС: з одного боку, масштаби атак здебільшого не перевищують порогу, який може активувати статтю 5 НАТО, а з іншого боку, вони несуть відчутні ризики для критичних секторів країн-членів. Особливо важливим є те, що ці загрози стосуються передусім держав, які активно підтримують Україну: Польщі, Литви, Латвії, Естонії, Німеччини, Італії, Франції. У цих країнах спостерігалися найінтенсивніші хвилі атак, включаючи DDoS-атаки, збої в логістичних системах, злом телекомунікаційних мереж, атаки на медичні установи та енергетичну інфраструктуру. Відповідальність за ці дії часто беруть на себе хактивістські угруповання, які, незважаючи на формальну незалежність, діють

синхронно з російською зовнішньополітичною лінією, вдаючись до інформаційних атак, скоординованих через Telegram-канали, форуми та даркнет-платформи. Зазвичай за ними стоїть глибша структура впливу, будь то спецслужби чи підтримка держави у вигляді ігнорування міжнародного права та кримінального переслідування.

Критична інфраструктура країн ЄС, яка є основою їх національної безпеки, економічної стабільності та соціального добробуту, стала пріоритетною ціллю. Дослідження показало, як інфраструктура транспорту, енергетики, телекомунікацій та охорони здоров'я зазнає зростаючого тиску як з боку державних суб'єктів, так і з боку кіберзлочинних синдикатів, які діють з територій, ворожих ЄС. Атаки на ланцюги поставок, компрометація логістичних компаній, маніпулювання інформаційними потоками в транспортному секторі – це не лише виклики, які створюють ризики для окремих секторів, але й серйозна загроза функціональній єдності внутрішнього ринку ЄС.

Телекомунікації, як нервова система цифрової економіки, опинилися в особливо вразливій зоні. Приклад атаки на KA-SAT є яскравим прикладом того, як втручання в комунікаційну інфраструктуру може мати мультиплікаційний ефект для енергетики, оборони, логістики та доступу до інформації. Це підкреслює необхідність комплексного підходу до кібербезпеки, де безпеку каналів зв'язку слід оцінювати не лише з точки зору безпеки даних, але й як фактор національної життєздатності під час кризи. Подібним чином приклади злому систем радіозв'язку на польських залізницях або атак на системи бронювання в аеропортах вказують на критичну потребу посилити регулювання, стандарти та міжгалузеву координацію щодо кібербезпеки на транспорті.

Медичний сектор, як найбільш гуманітарно чутливий сегмент, став мішенню атак з використанням програм-вимагачів. У європейських лікарнях були зашифровані системи електронного обліку пацієнтів, реєстри операцій, навіть мережі обладнання. Ці атаки, попри свій кримінальний характер, часто мали політичне підґрунтя, оскільки торкалися країн, які надавали найбільшу допомогу Україні. Оцінюючи відповідь Європейського Союзу на ці виклики,

варто визнати її еволюційний характер. Політичні ініціативи (Директива NIS2, CER, регулювання DORA), створення інституцій швидкого реагування (EU-CyCLONe, кіберрезервні сили), об'єднання зусиль з приватними компаніями (Microsoft, Amazon, Starlink), запуск навчань за участю всіх держав-членів (Cyber Europe, Locked Shields) – усе це формує багаторівневу модель кіберзахисту, що розвивається в напрямку високої адаптивності. У цьому плані співпраця з НАТО набуває особливого значення, оскільки синергія обох структур відкриває можливості для посилення кіберзахисту в довгостроковій перспективі.

Інформаційна безпека, яка раніше вважалася другорядним аспектом, тепер стає стратегічно важливою. Європейський Союз поступово інтегрує інформаційну та психологічну стійкість у парадигму кібербезпеки: запуск ініціативи EU vs Disinfo, ухвалення Закону про цифрові послуги, активна взаємодія з соціальними мережами, а також законодавчі зобов'язання щодо прозорості алгоритмів та обмеження впливу ботнетів – усе це свідчить про нове бачення цифрового суверенітету.

Війна росії проти України стала і випробуванням, і каталізатором для формування нової європейської архітектури кібербезпеки. Перед обличчям зростаючих глобальних ризиків, ескалації агресивної поведінки авторитарних режимів і невизначеності щодо майбутніх конфліктів, Європейському Союзу вдалося розпочати перехід до більш стійкої, взаємопов'язаної та інноваційно підтримуваної системи кіберзахисту. Але ця система потребує подальшого розвитку: від удосконалення технологій та правового регулювання до зміцнення громадської обізнаності, медіаграмотності та політичної волі. Лише шляхом поєднання стратегічного бачення, інституційної готовності та єдності дій Європейський Союз зможе ефективно захистити себе в епоху цифрових технологій, де безпека не обмежується державними кордонами, а атаки здійснюються не через кордони, а через мережі.

Список використаних джерел:

1. 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: https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:32019R0881.

2. NIS2 Directive: new rules on cybersecurity of network and information systems. URL: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

3. Про основні засади забезпечення кібербезпеки України : Закон України від 05.10.2017 № 2163-VIII. URL: https://zakon.rada.gov.ua/laws/show/2163-19#Text.

4. Maulny J. P., Di Bernardini L. Moving PeSCo forward: what are the next steps. ARES Policy Paper. 2019. No. 39. URL: https://www.iris-france.org/wp-content/uploads/2019/05/ARES-39.pdf.

5. Enhancing EU resilience: A step forward to identify critical entities for key sectors. European Commission. URL: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3992.

6. ENISA Threat Landscape 2023. ENISA. URL: https://www.enisa.europa.eu/sites/default/files/publications/ENISA%20Threat%20Landscape%202023.pdf.

7. Santos M. C. D. Identity and discourse in securitisation theory. Contexto Internacional. 2018. Vol. 40, No. 2. P. 229–248.

8. Craig A. J., Valeriano B. Realism and cyber conflict: Security in the digital age. Realism in Practice. 2018. Vol. 85, No. 3. P. 1–11.

9. Arslan A. S. Neorealist Analysis of Security Dilemma in Cyberspace; A Quantitative Study. 2024.

10. Zhao R. Constructing International Norms for the Governance of Cyber Terrorism–An Analytical Framework of Neo-liberal Institutionalism. Journal of Jishou University (Social Sciences Edition). 2020. Vol. 41, No. 4. P. 85.

11. Rajkumar V. S. et al. Cyber attacks on power grids: Causes and propagation of cascading failures. IEEE Access. 2023. Vol. 11. P. 103154–103176.

12. The Digital Europe Programme. URL: https://digital-strategy.ec.europa.eu/en/activities/digital-programme.

13. CSIRTs Network. URL: https://csirtsnetwork.eu/.

14. Савчук С. О. Виклики та можливості інтеграції України в систему кібербезпеки ЄС. Економіка, управління та адміністрування. 2024. № 2 (108). С. 198–203.

15. Smeets M. No shortcuts: Why states struggle to develop a military cyber-force. London : Hurst Publishers, 2022.

16. Berghel H. Bruce Schneier on AI Security.

17. Roguski P. Russian cyber attacks against Georgia, public attributions and sovereignty in cyberspace. 2020.

18. Prucková M. Cyber attacks and Article 5–a note on a blurry but consistent position of NATO. The NATO Cooperative Cyber Defence Centre of Excellence (CCDOE), 2022.

19. Microsoft. Defending Ukraine: Early Lessons from the Cyber War. 22.06.2022. URL: https://blogs.microsoft.com.

20. Lin H. Russian cyber operations in the invasion of Ukraine. The Cyber Defense Review. 2022. Vol. 7, No. 4. P. 31–46.

21. Magafas L., Demertzis K. Russia vs Ukraine Cyberwarfare: Lessons Learned.

22. Russia’s war on Ukraine: one year of cyber operations. CERT-EU. URL: https://cert.europa.eu/blog/1yua-cyberops.

23. Takamaa M., Lehto M. Cyber Operations in Ukraine: Emerging Patterns in Cases // Proceedings of the European Conference on Cyber Warfare and Security. 2024. Vol. 23, No. 1. Academic Conferences International Ltd.

24. Aljohani T. M. Cyberattacks on energy infrastructures: Modern war weapons. arXiv preprint arXiv:2208.14225.

25. Sufi F. Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges. Information. 2023. Vol. 14, No. 9. P. 485.

26. Sufi F. Social media analytics on Russia–Ukraine cyber war with natural language processing: Perspectives and challenges. Information. 2023. Vol. 14, No. 9. P. 485.

27. Mejova Y., Capozzi A., Monti C., Morales G. D. F. Narratives of War: Ukrainian Memetic Warfare on Twitter. arXiv preprint arXiv:2309.08363.

28. Cyber Operations during the Russo-Ukrainian War From Strange Patterns to Alternative Futures. CSIS. URL: https://www.csis.org/analysis/cyber-operations-during-russo-ukrainian-war.

29. EUROPOL Spotlight – Cyber-Attacks: The Apex of Crime-as-a-Service. 2023.

30. Кібератаки Росії проти України: досвід у боротьбі із цифровим ворогом 2014–2022 рр. Науковий блог. URL: https://naub.oa.edu.ua/kiberataky-rosiyi-proty-ukrayiny-dosvi.

31. Гнатюк С. Кіберскладник російсько-української війни: уроки та оцінки міжнародної спільноти. НІСД. URL: https://niss.gov.ua/sites/default/files/2022-06/az_cysecwar-2022-global-views_gn_24-06.pdf.

32. APT28 cyberattacks using the CVE-2023-23397 vulnerability. Рада національної безпеки і оборони України. URL: https://www.rnbo.gov.ua/files/НКЦК/2023/APT28%20cyberattacks%20using%20the%20CVE-2023-23397%20vulnerability%20-%20report.pdf.

33. Пшетачник Я., Тарпова С. Війна Росії проти України: хронологія кібератак. ДСЄП | Дослідницька служба Європейського парламенту. URL: https://www.europarl.europa.eu/RegData/etudes/BRIE/2022/733549/EPRS_BRI(2022)733549_XL.pdf.

34. Lázár B. Comparison of the NATO and EU cyber defence in the light of recently approved NATO cyber defence policy and the decision of establishing EU Joint Cyber Unit. Military National Security Service. P. 164.

35. Ahmed M. F., Molla A. H., Uddin M. R., Chowdhury T. R. Advancing cyber resilience: Bridging the divide between cyber security and cyber defense. International Journal for Multidisciplinary Research (IJFMR). 2023. Vol. 5, No. 6.

36. Wolff J. How the NotPetya attack is reshaping cyber insurance. 2021.

37. Давимука О. О. Ухвалення «Стратегічного компасу» Європейського Союзу. НІСД. URL: https://niss.gov.ua/sites/default/files/2022-04/evropeyskiy_kompas.pdf.

38. Cyber defence. NATO. URL: https://www.nato.int/cps/en/natohq/topics_78170.htm.

39. Locked Shields. CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/locked-shields/.

40. Durach F., Bârgăoanu A., Nastasiu C. Tackling Disinformation: EU Regulation of the Digital Space. Romanian Journal of European Affairs. 2020. Vol. 20, No. 1.

41. Noman M., Ali K. Cybercrime Syndicates and Financial Crime: Law Enforcement Strategies Against Online Scams. 2025.

42. Nearly two dozen Danish energy companies hacked through firewall bug in May. Cyber Security News | The Record from Recorded Future News. URL: https://therecord.media/danish-energy-companies-hacked-firewall-bug.

43. Pan-European exercise to foster preparedness in case of large-scale cyber-attacks in energy sector. Energy. URL: https://energy.ec.europa.eu/news/pan-european-exercise-foster-preparedness-case-large-scale-cyber-attacks-energy-sector-2024-06-20_en.

44. Beretas C. P. The Most Important Types of Cyber Attacks that France is Expected to Face in the Future and the Cyber Security Measures it Must Implement to Protect Critical Infrastructure, Telecommunication Networks and Personal Data. Universal Library of Engineering Technology. 2024. Vol. 1, No. 1.

45. Microsoft says Ukraine, Poland targetted with novel ransomware attack. Zeba Siddiqui. URL: https://www.reuters.com/technology/microsoft-says-ukraine-poland-targetted-with-novel-ransomware-attack-2022-10-14.

46. Kość W. Polish train chaos blamed on radio hackers. POLITICO. URL: https://www.politico.eu/article/poland-train-chaos-radio-hackers-russia-ukraine-war.

47. Guchua A., Zedelashvili T. Anonymous Sudan and Killnet Factor in the Russia-Ukraine War in the Context of Cyber Security. Future Human Image. 2023. No. 19.

48. Slowik J. Reviewing the 2022 KA-SAT Incident & Implications for Distributed Communication Environments. 2024.

49. Tatam M., Shanmugam B., Azam S., Kannoorpatti K. A review of threat modelling approaches for APT-style attacks. Heliyon. 2021. Vol. 7, No. 1.

50. Russian cyber spies attack Ukraine's allies, Microsoft says. Zeba Siddiqui. URL: https://www.reuters.com/world/russian-hacking-groups-step-up-cyber-espionage-ukraine-allies-microsoft-says-2022-06-22.

51. Konkel F. Microsoft: Russia Stepping Up Hacking, Cyber Penetration Efforts on 42 Ukraine Allies. Nextgov.com. URL: https://www.nextgov.com/cybersecurity/2022/06/microsoft-russia-stepping-hacking-cyber-penetration-efforts-42-ukraine-allies/368514.

52. Significant Cyber Incidents. CSIS. URL: https://www.csis.org/programs/strategic-technologies-program/significant-cyber-incidents.

53. Škorjanc Ž. Digital Operational Resilience Act. Zeitschrift für das gesamte Bank- und Börsenwesen. 2023. Vol. 71, No. 9. P. 658. DOI: https://doi.org/10.47782/oeba202309065801.

54. Савчук С. О. Виклики та можливості інтеграції України в систему кібербезпеки ЄС. Економіка, управління та адміністрування. 2024. № 2 (108). С. 198–203.

55. Enisa threat landscape: health sector. ENISA. URL: https://www.enisa.europa.eu/sites/default/files/publications/Health%20Threat%20Landscape.pdf.

56. Hackers Release Stolen Data after French Hospital Refuses to Pay Decryption Ransom. Hot for Security. URL: https://www.bitdefender.com/en-us/blog/hotforsecurity/hackers-release-stolen-data-after-french-hospital-refuses-to-pay-decryption-ransom.

57. A French hospital was forced to reschedule procedures after cyberattack. Security Affairs. URL: https://securityaffairs.com/162057/hacking/french-hospital-cyber-attack.html.

58. Scroxton A. Russian DDoS hacktivists seen targeting western hospitals. Computer Weekly. URL: https://www.computerweekly.com/news/365529957/Russian-DDoS-hacktivists-seen-targeting-western-hospitals.

59. KillNet's Targeting of the Health and Public Health Sector (December 2022 – March 2023). United States health and public health (HPH) sector. URL: https://www.hhs.gov/sites/default/files/202304051200-killnet-analyst-note-tlpwhite.pdf.

60. O'Donnell J., Jones H. European, U.S. regulators tell banks to prepare for Russian cyberattack threat. Reuters. URL: https://www.reuters.com/markets/europe/european-us-regulators-tell-banks-prepare-russian-cyberattack-threat-2022-02-09.

61. Russia-Ukraine War: Cyberattack and Kinetic Warfare Timeline. MSSP Alert. URL: https://www.msspalert.com/news/ukraine-russia-cyberattack-timeline-updates-amid-russia-invasion.

62. Pro-Russian hackers attack the European Investment Bank. The Paypers. URL: https://thepaypers.com/digital-identity-security-online-fraud/pro-russian-hackers-attack-the-european-investment-bank--1263136.

63. Valkeasuo T. TIBER-EU Preparation Phase Framework; case study Nixu: optimizing TIBER-EU engagements. 2023.

64. CCDCOE – The NATO Cooperative Cyber Defence Centre of Excellence. URL: https://ccdcoe.org/.

65. The 2023 Crypto Crime Report. Chainalysis. URL: https://hkibfa.io/wp-content/uploads/2023/02/Crypto_Crime_Report_2023.pdf.

66. Belgium probes suspected Chinese hack of state security service. The Record from Recorded Future News. URL: https://therecord.media/belgium-investigation-alleged-china-cyber-espionage-vsse.

67. Bestuzhev D., The BlackBerry Research and Intelligence Team. BiBi Wiper Used in the Israel-Hamas War Now Runs on Windows. BlackBerry Blog. URL: https://blogs.blackberry.com/en/2023/11/bibi-wiper-used-in-the-israel-hamas-war-now-runs-on-windows.

68. 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. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2016/1148/oj/eng.

69. EU CyCLONe | ENISA. URL: https://www.enisa.europa.eu/topics/eu-incident-response-and-cyber-crisis-management/eu-cyclone.

70. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation – GDPR). EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng.

71. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA and on information and communications technology cybersecurity certification (Cybersecurity Act). EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2019/881/oj/eng.

72. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

73. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2022/2557/oj/eng.

74. Regulation (EU) 2021/887 of the European Parliament and of the Council of 20 May 2021 establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. EUR-Lex. URL: https://eur-lex.europa.eu/eli/reg/2021/887/oj/eng.

75. Конвенція про кіберзлочинність : Конвенція Ради Європи від 23.11.2001. URL: https://zakon.rada.gov.ua/laws/show/994_575#Text.

76. Directive (EU) 2013/40 of the European Parliament and of the Council of 12 August 2013 on attacks against information systems and replacing Council Framework Decision 2005/222/JHA. EUR-Lex. URL: https://eur-lex.europa.eu/eli/dir/2013/40/oj/eng.

77. Resolution (EU) 2022/1700 of the European Parliament. EUR-Lex. URL: https://eur-lex.europa.eu/eli/res/2022/1700/oj/eng.

78. Act on increasing the security of IT systems (German IT Security Act 1.0). Federal Office for Information Security. URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/1-0/it_sig-1-0_node.html.

79. Second act on increasing the security of IT systems (German IT Security Act 2.0). Federal Office for Information Security. URL: https://www.bsi.bund.de/EN/Das-BSI/Auftrag/Gesetze-und-Verordungen/IT-SiG/2-0/it_sig-2-0_node.html.

80. CERT-EU – Cybersecurity Service for the Union Institutions, Bodies, Offices and Agencies. European Union. URL: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies/cybersecurity-service-union-institutions-bodies-offices-and-agencies-cert-eu_en.

81. Home | ENISA. URL: https://www.enisa.europa.eu/.

82. European Cybersecurity Competence Centre and Network. URL: https://cybersecurity-centre.europa.eu/index_en.

83. Home – ECSO. ECSO. URL: https://ecs-org.eu/.

84. European Cybercrime Centre – EC3 | Europol. URL: https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3.

85. Minghini M., Cetl V., Kotsev A., Tomas R., Lutz M. INSPIRE: The entry point to Europe's big geospatial data infrastructure. In Handbook of Big Geospatial Data. Cham: Springer International Publishing, 2021. P. 619–641.

86. Leuprecht C., Hamilton R. New opportunities in common security and defence policy: Joining PESCO. Australian and New Zealand Journal of European Studies. 2019. Vol. 11, No. 3.

87. Ruohonen J. A Systematic Literature Review on the NIS2 Directive. arXiv preprint arXiv:2412.08084. 2024.

88. Szpor G. The evolution of cybersecurity regulation in the European Union law and its implementation in Poland. Rev. Eur. & Comp. L. 2021. Vol. 46. P. 219.

89. Dubois E., Tatar U. Mitigating global cyber risk through bridging the national incident response capacity gap. In International Conference on Cyber Warfare and Security. 2022. P. 527–XI.

90. Jacuch A. Comparative analysis of cybersecurity strategies. European union strategy and policies. Polish and selected countries strategies. Online journal modelling the new Europe. 2021. No. 37. P. 102–120.

91. Kavyn S., Bratsuk I., Lytvynenko A. Regulatory and legal enforcement of cyber security in countries of the European Union: The experience of Germany and France. Teisė. 2021. Vol. 121. P. 135–147.

92. Ruohonen J. The Incoherency Risk in the EU's New Cyber Security Policies. In Conference on e-Business, e-Services and e-Society. Cham: Springer Nature Switzerland, 2024. P. 284–295.

93. Olesen N. European public-private partnerships on cybersecurity – an instrument to support the fight against cybercrime and cyberterrorism. In: Combatting Cybercrime and Cyberterrorism: Challenges, Trends and Priorities. 2016. P. 259–278.

94. Priyono U., Swastanto Y., Pramono B. Cyber Diplomacy (A Perspective From Indonesia-Australia Cyber Cooperation). International Journal Of Humanities Education and Social Sciences. 2023. Vol. 2, No. 4.

95. Rajamäki J., Feyesa A., Nepal A. E-EWS-based Governance Framework for Sharing Cyber Threat Intelligence in the Energy Sector. European Conference on Cyber Warfare and Security. 2024. Vol. 23, No. 1. P. 398–406. DOI: https://doi.org/10.34190/eccws.23.1.2073.

96. Ludvigsen K. R. Creating Cybersecurity Regulatory Mechanisms, as Seen Through EU and US Law. arXiv preprint arXiv:2503.07250. 2025.

97. Procedda M. G. Public-Private Partnerships: A “Soft” Approach to Cybersecurity? Views from the European Union. In: Security in Cyberspace: Targeting Nations, Infrastructures, Individuals. 2014. P. 183–211.

98. EU4DigitalUA – підтримка цифрової трансформації та кібербезпеки в Україні (2020–2025). EU4Digital, 2023. URL: https://eufordigital.eu.

99. ЄС підтримав кібербезпеку в Україні на суму понад 10 млн євро: прес-реліз Представництва ЄС в Україні від 21.10.2022. EU4Digital. URL: https://eufordigital.eu.

100. Україна імплементує директиву NIS2 щодо безпеки мереж і інформаційних систем – М. Федоров. Інтерфакс-Україна. 24.02.2025.

101. CyberEast та співпраця у рамках кібербезпеки між Україною та ЄС. URL: https://thecyberexpress.com/eu-ukraine-stronger-cybersecurity-partnership.

102. EU4DigitalUA. Результати роботи проєкту підтримки цифрової трансформації України. URL: https://www.eeas.europa.eu/delegations/ukraine/european-union-supports-ukraines-digital-transformation-results-eu4digitaluas-work_en.

103. Операційна угода між Україною та ENISA (липень 2023). URL: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels.

104. Muncaster P. EU Formalizes Cybersecurity Support For Ukraine. Infosecurity Magazine. URL: https://www.infosecurity-magazine.com/news/eu-formalizes-cybersecurity/.

105. 3-й Кібердіалог Україна–ЄС (липень 2024). URL: https://thecyberexpress.com/eu-ukraine-stronger-cybersecurity-partnership.

106. 24-й саміт Україна–ЄС (3 лютого 2023, Київ). URL: https://www.eeas.europa.eu/node/99530_fr.

107. Механізм координації кіберкриз ЄС («Талліннський механізм», січень 2022). URL: https://digital-strategy.ec.europa.eu/en/news/ukraine-3rd-cyber-dialogue-european-union-takes-place-brussels.

Summary

The study comprehensively examines the transformation of the European Union's cybersecurity system under the conditions of Russia's full-scale aggression against Ukraine, highlighting the ways in which the war reshaped strategic priorities, institutional mechanisms, and international partnerships within the EU. The analysis demonstrates that the war became a turning point for European cyber policy, revealing both structural vulnerabilities and a strong capacity for collective response. It also emphasizes that Ukraine has become a practical testing ground for European cyber defence mechanisms, elevating the strategic significance of cooperation between Ukraine and the EU.

First, the research confirms that cyberattacks have become an integral component of modern hybrid warfare. Russia's actions in cyberspace—ranging from attacks on critical infrastructure to disinformation campaigns—illustrate how digital tools are used to destabilize states, undermine public trust, and influence political processes. The intensity and scale of these attacks increased dramatically after February 2022, expanding their impact beyond Ukraine to EU member states, particularly in sectors such as energy, communications, transportation, and public governance. This demonstrates that the war has erased traditional geographic boundaries of conflict, making cybersecurity inseparable from broader European security.

Second, the study shows that before the full-scale war, the EU had already established a complex legal and institutional system aimed at protecting cyberspace. However, the unprecedented cyber pressure arising from the war revealed significant gaps in the EU's preparedness: fragmentation of national cybersecurity systems, uneven digital resilience levels among member states, insufficient cross-border coordination, and the need for more agile crisis-management tools. This prompted the EU to accelerate reforms, such as the implementation of NIS2, development of the EU Joint Cyber Unit, strengthening of ENISA, and expansion of capacities for threat intelligence sharing.

Third, the work emphasizes the crucial role of collective defence mechanisms and supranational coordination. The EU, for the first time, mobilized joint response instruments in support of a partner state under attack. This included the deployment of Cyber Rapid Response Teams (CRRTs), the use of diplomatic instruments and sanctions, and the unprecedented level of intelligence exchange. The synergy between EU institutions and national cybersecurity centers significantly enhanced the Union's ability to counter multi-vector cyber threats. According to the study, this collective response became not only a demonstration of solidarity, but also a new operational standard for EU cyber defence.

Fourth, the research identifies that cyber threats to the EU during the war can be grouped into several key categories: targeted attacks by state-sponsored actors, cybercrime as a service, ransomware campaigns, disruptions of critical infrastructure, and large-scale disinformation operations aimed at manipulating public opinion. The war has shown that cybercrime syndicates and politically motivated hacker groups increasingly overlap and sometimes act in coordination with state interests. This blurring of lines requires a rethinking of both the legal framework and practical mechanisms for cyber incident management.

Fifth, the study highlights the deepening and strategic importance of cooperation between Ukraine and the European Union. Ukraine's experience—shaped by years of countering Russian cyberattacks since 2014—proved invaluable for European partners. Ukrainian institutions shared practical knowledge, incident data, and technological solutions that later contributed to improving EU-wide cyber resilience. At the same time, the EU provided Ukraine with large-scale support: capacity-building programs, financing of cybersecurity projects, technical assistance, and integration into European cyber networks. This cooperation has laid the foundation for Ukraine's future integration into the EU's digital security architecture and demonstrated the potential of cyber diplomacy in strengthening collective resilience.

Sixth, the research indicates that despite significant progress, the EU still faces notable challenges. These include the need to eliminate fragmentation between national cybersecurity rules, invest more actively in cyber defence capabilities, expand public-

private partnerships, and strengthen protection of critical infrastructure from evolving threats. The war proved that operational flexibility, real-time information exchange, and strategic autonomy in the digital sphere are essential for Europe's long-term stability.

The concluding assessment of the study states that the full-scale invasion of Ukraine fundamentally reshaped the EU's approach to cybersecurity. Cyber threats are now viewed not only as technical challenges but as geopolitical and security priorities requiring coordinated, long-term strategies. The EU has moved toward forming a more unified cyber defence policy, integrating supranational mechanisms with national systems, and building deeper partnerships with states like Ukraine.

Overall, the findings of the research underline that cybersecurity in the context of the Russo-Ukrainian war is not merely a regional issue—it has become a defining factor of European security in the 21st century. The conflict accelerated institutional modernization within the EU, fostered unprecedented cooperation with Ukraine, and established new standards for collective cyber resilience. The lessons learned from this period will continue to influence European cyber policy well beyond the end of hostilities, shaping a more robust, cooperative, and adaptive cybersecurity architecture for the future.