КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023
DOI 10.28925/2663-4023.2024.24.133149
УДК 32:004.056:061.1 ЄС

Мужанова Тетяна Михайлівна
к.держ.упр., доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних
технологій, Київ, Україна
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Легомінова Світлана Володимирівна
д.е.н., професор, завідувач кафедри управління
інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних
технологій, Київ, Україна
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Щавінський Юрій Віталійович
к.т.н., доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних
технологій, Київ, Україна
ORCID ID: 0000-0002- 2319-8983
yushchavinsky@ukr.net

Якименко Юрій Михайлович
к.військ.н. доцент, доцент кафедри управління
інформаційною та кібернетичною безпекою
Державний університет інформаційно-комунікаційних
технологій, Київ, Україна
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Нестеренко Галина Петрівна
к.держ.упр., доцент, доцент кафедри публічного управління та
адміністрування Навчально-наукового інституту неперервної освіти
Національний авіаційний університет, Київ, Україна
ORCID ID: 0000-0002-1106-3790
halynanesterenko@gmail.com

ОСНОВНІ ПІДХОДИ Й НАПРЯМИ РОЗВИТКУ ПОЛІТИКИ КІБЕРБЕЗПЕКИ ЄВРОПЕЙСЬКОГО СОЮЗУ

Анотація. Впровадження цифрових технологій у всі сфери життєдіяльності суспільства поряд з багатьма перевагами викликало появу нових викликів безпеці, реагування на які вимагає гнучких, інноваційних і комплексних підходів, швидкої і злагодженої відповіді, об'єднання зусиль багатьох зацікавлених сторін. За останні роки значних результатів у розробці і впровадженні політики кібербезпеки досяг Європейський Союз, який завдяки об'єднанню інституційних можливостей на рівні спільноти, зусиль держав-членів, співпраці з бізнесом і міжнародними партнерами вже впроваджує низку узгоджених ініціатив у сфері кібербезпеки. Досвід ЄС щодо вирішення проблем безпечного цифрового розвитку може бути еталоном для інших держав, у тому числі України. У статті розглянуто розвиток основних підходів і напрямів політики кібербезпеки ЄС з кінця 90-х років минулого століття до сьогодні. Встановлено, що з початку 2000-х років Єврокомісія окреслила спільний підхід до політики кібербезпеки ЄС, який передбачав подальшу реалізацію заходів щодо: обґрунтування політики і вдосконалення нормативно-правової бази; створення європейської

системи попередження й інформування; підтримки й інвестування в технологічні рішення кібербезпеки; підвищення цифрової обізнаності; впровадження ринково-орієнтованої стандартизації і сертифікації; забезпечення безпеки інституцій ЄС і держав-членів; розвитку міжнародної співпраці в галузі кібербезпеки. Перелічені напрями загалом залишалися актуальними в ході подальшого розвитку й удосконалення політики ЄС у цій сфері. Дослідження показало, що наступні етапи еволюції політики кібербезпеки ЄС були пов'язані із прийняттям трьох стратегій кібербезпеки 2013, 2017 та 2020 років, які відображали тенденції розвитку цифрового середовища і потреби в реагуванні на нові виклики кібербезпеки. Аналіз положень зазначених стратегій свідчить, що політика кібербезпеки ЄС була і продовжує бути спрямованою на вирішення трьох ключових цілей: досягнення кіберстійкості Європейської спільноти, держави, організацій в умовах постійних кіберзагроз; забезпечення ефективного кіберстримування; просування безпечного і відкритого глобального кіберпростору. На виконання задекларованих цілей політики кібербезпеки впродовж 2022–2023 років Єврокомісія запропонувала низку важливих ініціатив, зокрема щодо підвищення рівня кібербезпеки в державах ЄС; встановлення спільних стандартів кібербезпеки для інституцій ЄС; впровадження вимог кібербезпеки для продуктів із цифровими елементами; посилення потужностей ЄС з метою виявлення, підготовки й реагування на загрози й інциденти кібербезпеки. Встановлено, що при розробці і впровадженні політики кібербезпеки ЄС зіткнувся з низкою проблем і викликів, серед яких недостатній рівень координації, підтримки й ресурсного забезпечення; відставання нормативно-правової бази кібербезпеки від розвитку сфери; труднощі транскордонної і міжнародної співпраці; потреба в проактивному підході й адаптації політики до динамічного кіберсередовища; необхідність дотримання балансу між відкритістю й безпекою тощо. Доведено, що політика кібербезпеки Євросоюзу, яка розвивається поступально й динамічно, передбачає впровадження нових рішень і підходів у відповідь на виклики цифрового середовища, є еталоном для інших держав, зокрема й України.

Ключові слова: кібербезпека; політика кібербезпеки Європейського Союзу; законодавство з кібербезпеки ЄС.

ВСТУП

Цифрова трансформація поряд з перевагами розширення можливостей доступу, використання й обміну інформації, впровадження інноваційних технологічних рішень і підходів, які оптимізують процеси у будь-якій сфері життєдіяльності суспільства, викликала появу й ускладнення багатьох видів кіберзагроз, поставила людство перед цілковито новими викликами безпеки стратегічного й нерідко глобального масштабу.

Вирішення зазначених проблем кібербезпеки вимагає адаптованих до динамічних реалій цифрового середовища, інноваційних і комплексних рішень, швидкої і злагодженої реакції, об'єднання зусиль багатьох зацікавлених сторін.

Постановка проблеми. Європейський Союз є одним із провідних міжнародних гравців з кібербезпеки, який постійно оновлює і вдосконалює підходи, спрямовані на забезпечення безпечної цифровізації. За останні понад 30 років політика кібербезпеки Євросоюзу пройшла послідовний шлях удосконалення й адаптації до динамічних умов і загроз цифрового середовища.

Об'єднання інституційних можливостей ЄС, зусиль держав-членів, співпраця з бізнесом і міжнародними партнерами дозволили досягти багатьох своєчасних і конструктивних рішень, які вже зараз знаходяться на етапі реалізації. З огляду на зазначене, досвід розробки і впровадження політики кібербезпеки ЄС може бути еталоном кращих практик для інших держав, в тому числі України, стати рушійною силою для впровадження нових ініціатив для вирішення проблем кібербезпеки на світовому рівні, а, отже, вимагає ретельного вивчення й аналізу його переваг і прогалин.

Аналіз останніх досліджень і публікацій. Слід відзначити, що питання розробки і впровадження політики кібербезпеки ЄС перебуває в центрі уваги українських науковців. Дослідженню питань розробки і впровадження політики кібербезпеки ЄС присвячені праці таких вчених, як Бойко В., Василенко М., Кухаренко С. [1], Грубінко А. [2], Кузнєцов О. [3], Федонюк С. [4] та інших. Ґрунтовні роботи щодо еволюції підходів до кібербезпеки і перспектив концептуалізації європейської політики у цій сфері представлені колективами авторів з країн ЄС [5] – [8]. Однак, зазначені публікації не висвітлюють останніх ініціатив з кібербезпеки ЄС 2022–2023 років, які небезпідставно вважаються кращими рішеннями з моменту започаткування європейської політики кібербезпеки; не дають широкого уявлення про здобутки і труднощі впровадження європейської політики кібербезпеки.

Мета статті — дослідити основні підходи й напрями розвитку політики кібербезпеки ЄС з моменту започаткування до сьогодні як потенційного зразка кращих практик для інших держав, у тому числі України.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ

Європейський Союз був і залишається зразком кращих практик розробки і впровадження спільної політики у різних сферах життєдіяльності як на рівні європейської спільноти, так і на рівні держав-членів. Формування політики кібербезпеки не є винятком. Однак, політика кібербезпеки ЄС пройшла нелегкий шлях вдосконалення й адаптації під умови мінливого цифрового середовища, ландшафту кіберзагроз і динамічних викликів новітніх технологій.

Розглянемо еволюцію політики кібербезпеки ЄС на основі аналізу нормативно-правових актів ЄС (табл. 1).

Таблиця 1

Основні нормативно-правові акти, що регламентують питання кібербезпеки ЄС

Рік	Назва нормативно-правового документа
1995	Директива про захист осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних
1999	Ініціатива «Електронна Європа» та План дій щодо її реалізації
2000	Спільна позиція про переговори щодо конвенції Ради Європи про кіберзлочинність
2001	Повідомлення щодо створення безпечного інформаційного суспільства
	Повідомлення щодо безпеки мереж та інформації (NIS)
	Конвенція про кіберзлочинність
	Регламент про захист осіб у зв'язку з обробкою персональних даних
2002	Резолюція щодо спільного підходу і конкретних дій у сфері NIS
2004	Регламент про створення ENISA
2005	Рамкове рішення щодо атак проти інформаційних систем
2006	Стратегія безпечного інформаційного суспільства
2009	Повідомлення про захист критичної інформаційної інфраструктури: захист від масштабних кібератак і збоїв через посилення готовності, безпеки і стійкості
2013	Стратегія кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір»
	Директива ЄС про атаки на інформаційні системи
2016	Глобальна стратегія із зовнішньої і безпекової політики ЄС
	Директива з безпеки мережевих та інформаційних систем NIS
	Загальний регламент про захист даних (GDPR)

2017	Стратегія кібербезпеки «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС»
2019	Регламент про ENISA і сертифікацію ІКТ в галузі кібербезпеки (Акт з кібербезпеки)
2020	Стратегія кібербезпеки ЄС для цифрового десятиліття
2022	Директива щодо заходів для забезпечення високого спільного рівня кібербезпеки в ЄС (NIS 2)
	Регламент щодо заходів для високого загального рівня кібербезпеки в органах ЄС
	Регламент щодо горизонтальних вимог кібербезпеки для продуктів із цифровими елементами (Акт про кіберстійкість) — *проєкт*
2023	Регламент щодо заходів посилення солідарності й потужностей ЄС з метою виявлення, підготовки та реагування на загрози й інциденти кібербезпеки (Акт про кіберсолідарність) — *проєкт*

Основи політики кібербезпеки ЄС були закладені у кінці 90-х років минулого століття. Реагуючи на виклики, пов'язані з розбудовою цифрового суспільства й упровадження ІКТ, керівництво ЄС акцентувало на важливості мережевої безпеки й боротьби з кіберзлочинністю, зокрема зробило низку кроків для боротьби зі шкідливим і незаконним контентом в Інтернеті, захисту інтелектуальної власності й персональних даних, сприяння електронній торгівлі та підвищення безпеки транзакцій.

Починаючи з початку 2000-х років, Європейська Комісія починає приділяти все більше уваги питанням кібербезпеки. Водночас, основні зусилля зосереджуються на питаннях удосконалення інформаційної інфраструктури, захисту даних і протидії комп'ютерній злочинності.

Слід відзначити, що саме в цей час у законодавстві ЄС почали використовувати термін «мережева та інформаційна безпека» (Network and Information Security, NIS), під якою розуміють здатність мережі або інформаційної системи протистояти випадковим подіям або зловмисним діям на заданому рівні довіри.

Також Єврокомісія окреслила спільний підхід до європейської політики NIS, який передбачав подальшу реалізацію заходів за такими напрямами: обґрунтування політики і вдосконалення нормативно-правової бази; створення європейської системи попередження та інформування; підтримка й інвестування в технологічні рішення NIS; підвищення обізнаності; підтримка ринково орієнтованої стандартизації та сертифікації; забезпечення безпеки інституцій ЄС і країн-членів; міжнародна співпраця [9]. Держави-члени ЄС отримали вказівки щодо впровадження відповідних рішень на національному рівні [10].

Варто зауважити, що подальша політика ЄС у сфері кібербезпеки загалом реалізувалася в межах вищезгаданого підходу.

Наступним важливим кроком у розбудові європейської політики кібербезпеки, зокрема її інституційної складової, стало створення у 2004 році Європейського агентства мережевої та інформаційної безпеки ENISA [11], яке відігравало і продовжує відігравати ключову роль у забезпеченні кібербезпеки Спільноти. На той час ENISA отримало повноваження щодо консультування інституцій ЄС з питань NIS, сприяння підвищенню обізнаності й обміну кращими практиками, посилення співпраці з усіма зацікавленими сторонами у цій сфері, а також відстеження розробки стандартів для продуктів і послуг NIS і управління кіберризиками.

Усвідомлюючи необхідність об'єднання зусиль державного і приватного секторів у подоланні спільних проблем кібербезпеки, Єврокомісія розпочала налагодження тісної співпраці з економічними гравцями, запросивши зацікавлених представників приватного сектора взяти участь у поширенні кращих практик безпеки; визначенні вимог безпеки для виробників ПЗ і провайдерів Інтернет-послуг; впровадженні навчальних програм з

безпеки для персоналу; здійсненні сертифікації безпеки для продуктів, процесів і послуг тощо [12].

У кінці першої декади 2000-х років з огляду на масштабні кібератаки і збої у роботі об'єктів критичної інфраструктури ЄС Єврокомісія зосередилася на вирішенні проблем забезпечення безпеки і стійкості критичних інформаційних інфраструктур (Critical Information Infrastructures, CIIs). З цією метою було встановлено такі завдання: усунути відмінності в національних підходах до забезпечення безпеки і стійкості CIIs; сформувати нову європейську модель управління CIIs; забезпечити раннє попередження й реагування на інциденти; налагодити ефективну міжнародну співпрацю [13].

Новий етап розвитку політики кібербезпеки ЄС ознаменувався прийняттям у 2013 році першої Стратегії кібербезпеки ЄС «Відкритий, надійний і безпечний кіберпростір», у якій кібербезпека була визнана новим окремим напрямом політики ЄС. Під кібербезпекою Стратегія розуміє заходи безпеки та дії, які можуть бути використані для захисту кіберсередовища, як у цивільній, так і у військовій сферах, від тих загроз, які пов'язані або можуть зашкодити його взаємозалежним мережам та інформаційній інфраструктурі. Метою кібербезпеки визначено збереження доступності й цілісності мереж та інфраструктури, а також конфіденційності даних, які в них містяться [14].

Відповідно до Стратегії принципами кібербезпеки є: застосування у кіберпросторі тих же цінностей, законів і норм, що і в фізичному світі; захист основних прав, свободи вираження поглядів, персональних даних і конфіденційності; забезпечення необмеженого і безпечного доступу до Інтернету для всіх; демократичне й ефективне багатостороннє управління Інтернетом; спільна відповідальність за кібербезпеку.

Стратегічними пріоритетами ЄС було визначено:

- *досягнення кіберстійкості*, яке передбачає розбудову можливостей держав-членів ЄС шляхом встановлення загальних мінімальних вимог до кібербезпеки на національному рівні, зокрема призначення національних компетентних органів, прийняття національної стратегії і плану дій з кібербезпеки, створення CERT; створення узгоджених механізмів запобігання, виявлення, пом'якшення та реагування у сфері кібербезпеки; підвищення готовності й залучення приватного сектору, а також зростання обізнаності користувачів з питань кібербезпеки;
- *значне скорочення кіберзлочинності*, яке має бути досягнене шляхом формування сильного й ефективного законодавства щодо протидії кіберправопорушенням; розширення й оновлення оперативного потенціалу для боротьби з кіберзлочинністю (застосування новітніх засобів і методів, збір і поширення передового досвіду подолання кіберзлочинності у співпраці з Європейським центром боротьби з кіберзлочинністю ЕС3 та Євроюстом); покращення координації зусиль з метою протидії кіберзлочинності на рівні ЄС;
- *розробку політики кіберзахисту*, що охоплює оцінювання оперативних вимог і розробку основ політики кіберзахисту ЄС, покращення можливостей освіти й навчання з кіберзахисту для військових, сприяння діалогу та координації між цивільними та військовими суб'єктами в ЄС щодо раннього попередження, реагування на інциденти, оцінювання ризиків тощо; забезпечення діалогу з міжнародними партнерами для забезпечення ефективного кіберзахисту;
- *розвиток промислових і технологічних ресурсів для кібербезпеки*, яке буде здійснюватися через розвиток єдиного ринку для продуктів кібербезпеки (з

одного боку, мотивування виробників і провайдерів послуг забезпечувати високі стандарти безпеки, з іншого — стимулювання ринкового попиту на «високо безпечні» продукти в ЄС, розробка галузевих стандартів і сприяння добровільній сертифікації з кібербезпеки, введення т.зв. «міток безпеки» для кращих компаній; інвестування в дослідження і сприяння інноваціям;

– *формування узгодженої міжнародної політики в кіберпросторі для ЄС та просування основних цінностей спільноти*, таких як людська гідність, свобода, демократія, рівність, верховенство права та повага до основних прав людини, що охоплюватиме зусилля ЄС зі сприяння відкритості та свободі Інтернету, розробки норм поведінки й застосування чинних міжнародних законів у кіберпросторі, усунення цифрового розриву і створення потенціалу кібербезпеки.

У цьому ж році зроблено низку важливих кроків щодо протидії кіберзлочинності, зокрема подальшого зближення кримінального законодавства держав-членів у цій сфері; створення Європейського центру боротьби з кіберзлочинністю ЕС3 як складової Європолу [15]; визначення знарядь вчинення правопорушень, до яких, зокрема, віднесено створення ботнетів; встановлення покарань за вчинення кіберзлочинів, зокрема термінів ув'язнення від 2-х років (від 5-ти років для злочинів, вчинених у рамках злочинної організації або проти СІІ) [16].

Прагнучи посилити безпеку і кіберстійкість мережевих та інформаційних систем на національному рівні, Єврокомісія у 2016 році зобов'язала держави ЄС схвалити національні закони з безпеки мережевих та інформаційних систем, створити компетентний національний орган (або органи) у цій сфері, визначити операторів основних послуг (Essential Services Providers), а також встановити вимоги щодо безпеки й оповіщення для операторів основних послуг і постачальників цифрових послуг. Також була створена Група співробітництва NIS, яка мала забезпечити стратегічну співпрацю й обмін інформацією між державами-членами з питань кібербезпеки, а також здійснювати координацію дій новоствореної мережі груп реагування на інциденти комп'ютерної безпеки CSIRT [17].

Наступною віхою розвитку політики кібербезпеки ЄС стало прийняття другої Стратегії кібербезпеки «Стійкість, стримування та захист: побудова міцної кібербезпеки для ЄС», яка була оприлюднена у вересні 2017 року [18].

Європейська Комісія наголосила у Стратегії, що з огляду на експоненціальне зростання ризиків кібербезпеки й обсягів деструктивного впливу кіберзлочинності на економіку ЄС, необхідним є застосування нового проактивного підходу, який передбачає участь ЄС, країн-членів, представників галузей економіки й окремих громадян для підвищення кіберстійкості та кращого реагування на кібератаки.

Документ демонструє остаточні зміни у підходах ЄС до питань кібербезпеки, зокрема зміщення акцентів з кібербезпеки як забезпечення захищеності об'єктів на кіберстійкість як здатність забезпечити стабільне функціонування Європейської спільноти, держави, організацій в умовах постійних кіберзагроз. Також визнано нагальну необхідність міжнародної співпраці для вирішення проблем безпеки кіберпростору з огляду на його глобальну і транскордонну природу.

Отже, оновлений підхід передбачає досягнення трьох основних цілей:

І. підвищення стійкості ЄС до кібератак, яке передбачає зміцнення ENISA; розбудову єдиного ринку кібербезпеки (стандартизація, сертифікація продуктів, послуг і процесів); впровадження ефективних практик управління ризиками й інформування про серйозні кіберінциденти для надавачів критичних і цифрових послуг; швидке реагування

на кібератаки через налаштування швидкого механізму обміну інформацією між усіма ключовими гравцями на національному й загальноєвропейському рівні; розбудову мережі центрів компетентностей кібербезпеки на чолі з Європейським центром досліджень і компетентностей кібербезпеки (ECCC), створеним у 2021 році; створення потужної бази кібернавичок ЄС шляхом розвитку освіти з кібербезпеки на всіх рівнях; сприяння кібергігієні й обізнаності громадян.

II. забезпечення ефективного кіберстримування, що охоплює підвищення результативності виявлення винних у кібератаках, зокрема шляхом ефективного розслідування й судового розгляду кіберзлочинів правоохоронними органами, посилення ролі ЕС3 у цих процесах; державно-приватна співпраця з метою подолання кіберзлочинності; розробку набору інструментів кібердипломатії (cyber diplomacy toolbox) [19] для дипломатичного реагування на зловмисну кібердіяльність, спрямовану проти інтересів ЄС; посилення можливостей кіберзахисту держав-членів через поєднання їхніх зусиль з діями інституцій ЄС, військових і цивільних суб'єктів.

III. посилення міжнародної співпраці з кібербезпеки шляхом підвищення ролі питань кібербезпеки у зовнішніх відносинах, розвитку спільних можливостей усіх держав запобігати кіберінцидентам і реагувати на них, розслідувати справи про кіберзлочини тощо.

Важливим здобутком ЄС у цей період стало досягнення політичної згоди щодо сертифікації ІКТ в галузі кібербезпеки. Так, з метою створення єдиного цифрового ринку для продуктів, послуг і процесів ІКТ, а також забезпечення високого рівня кібербезпеки, кіберстійкості й довіри в ЄС вирішено впровадити узгоджений загальносоюзний підхід до європейських схем сертифікації кібербезпеки. Сертифікація має гарантувати, що сертифіковані продукти, послуги та процеси ІКТ відповідають встановленим вимогам щодо захисту конфіденційності, цілісності, доступності й автентичності даних, функцій або послуг, які пропонуються або доступні через ці продукти, послуги та процеси протягом їх життєвого циклу [20].

У цьому контексті було також розширено повноваження ENISA, зокрема Агентство має брати участь у розробці та впровадженні політики і права ЄС з кібербезпеки; сприяти операційній співпраці за участю держав-членів, інституцій, органів, служб і агентств ЄС; надавати підтримку для груп реагування на інциденти комп'ютерної безпеки (загальноєвропейської CERT-EU та національних CSIRT); розробляти і впроваджувати політики ЄС щодо сертифікації продуктів, послуг і процесів ІКТ з кібербезпеки; сприяти розвитку освіти, підвищенню обізнаності й навчанню, дослідженням та інноваціям з кібербезпеки в ЄС, а також міжнародній співпраці у цій сфері.

Початком поточного етапу розвитку політики кібербезпеки ЄС стало прийняття у 2020 році Стратегії кібербезпеки ЄС на цифрове десятиліття [21]. Стратегія декларує прагнення ЄС щодо забезпечення глобального та відкритого Інтернету з надійними бар'єрами для усунення ризиків безпеці й основним європейським цінностям, і містить пропозиції щодо застосування трьох основних інструментів: регуляторних, інвестиційних і політичних, — для досягнення трьох цілей ЄС (рис. 1).

Як представлено на рис. 1 для досягнення зазначених цілей заплановано виконання низки завдань.

Рис. 1. Цілі й завдання Стратегії кібербезпеки ЄС на цифрове десятиліття

Порівняння положень Стратегій 2020 і 2017 років показало, що цілі практично накладаються: перша ціль має на меті забезпечення стійкості до кібератак; друга — стримування кіберзлочинності й кіберзахист; третя — об'єднання зусиль усіх зацікавлених сторін (як в ЄС, так і по всьому світу; державних, приватних, експертних організацій та громадян) для формування безпечного кіберпростору.

Натомість, для досягнення кожної з цілей у Стратегії 2020 року передбачено низка принципово нових конкретних завдань, які раніше не окреслювалися в основоположних нормативних документах ЄС.

Так, *забезпечення кіберстійкості, технологічного суверенітету й лідерства* має бути досягнуте, зокрема, шляхом:

- формування кіберстійких інфраструктури і критичних сервісів в результаті реформування вимог щодо безпеки і звітності про інциденти, національного нагляду та правозастосування для стратегічно важливих секторів, а також зміцнення кіберстійкості демократичних процесів та інституцій;
- розбудови єдиної мережі операційних центрів безпеки (SOC), щоб завдяки використанню штучного інтелекту й машинного навчання завчасно виявляти ознаки неминучих кібератак і вживати запобіжних заходів;
- розгортання надзахищеної квантової комунікаційної інфраструктури (QCI);
- захист 5G і наступних поколінь широкосмугових мобільних мереж;

- створення умов для Інтернету безпечних речей, зокрема через впровадження прозорих рішень безпеки й сертифікації;
- посилення кібербезпеки ланцюжка постачання технологій, включаючи дані та хмари, процесорні технології нового покоління, надбезпечне під'єднання та мережі 6G;
- формування кіберкваліфікованої робочої сили шляхом залучення, утримання, розвитку й підвищення кваліфікації спеціалістів із кібербезпеки, інвестування в дослідження та інновації світового класу, що має сприяти подальшому збільшенню навичок кібербезпеки та кіберзахисту на рівні ЄС;
- зміцнення глобальної безпеки в Інтернеті через розробку плану на випадок надзвичайних ситуацій (зловмисних кібератак, великих геополітичних і технічних інцидентів), які можуть вплинути на цілісність і доступність глобальної кореневої системи DNS, впровадження ключових стандартів Інтернету та безпеки мережі.

У рамках *розбудови операційної спроможності для запобігання, стримування та реагування на кіберінциденти* передбачено створення спільного кіберпідрозділу (Joint Cyber Unit), який має забезпечити оперативну й технічну координацію щодо протидії великим транскордонним кіберінцидентам і загрозам; посилення можливостей кіберзахисту шляхом розробки й використання технологій штучного інтелекту, шифрування та квантових обчислень, а також забезпечення синергії кіберзусиль між цивільною, оборонною і космічною галузями; впровадження набору інструментів кібердипломатії для посилення дипломатичної відповіді ЄС на дії у кіберпросторі, які несуть потенційну шкоду інтересам європейської спільноти.

Досягнення цілі з *просування глобального та відкритого кіберпростору* охоплює виконання завдань щодо стандартизації новітніх технологій (штучний інтелект, хмарні обчислення, квантові обчислення й комунікації); захисту правозахисників, громадянського суспільства й наукових кіл, які працюють над вирішенням проблем кібербезпеки, конфіденційності даних, стеження й онлайн-цензури.

Особливий акцент зроблено на посиленні співпраці та забезпечення захисту основних прав і свобод, зокрема права на гідність, приватне життя і свободу вираження поглядів та інформації у всесвітній мережі, а також пошуку моделі багатостороннього управління Інтернетом.

ЄС зобов'язався підтримувати цю Стратегію шляхом безпрецедентного рівня інвестицій у цифровий перехід ЄС протягом наступних 7-ми років, перевищивши попередні рівні фінансування кібербезпеки в чотири рази [21].

Упродовж 2022–2023 років Єврокомісія запропонувала низку важливих ініціатив, спрямованих на досягнення стратегічних цілей посилення кібербезпеки і кіберстійкості Європейського Союзу і держав-членів.

Так, для забезпечення високого спільного рівня кібербезпеки в ЄС Єврокомісія зобов'язала держави ЄС прийняти національні стратегії кібербезпеки та призначити або створити компетентні органи, органи управління кіберкризами, єдині контактні пункти з питань кібербезпеки і групи реагування на інциденти комп'ютерної безпеки CSIRT; підвищити рівень гармонізації вимог безпеки, забезпечити реалізацію заходів базового рівня з управління ризиками кібербезпеки і встановити зобов'язання щодо звітності для організацій критичних і важливих галузей; забезпечити виконання організаціями правил і зобов'язань щодо обміну інформацією у сфері кібербезпеки. За невиконання зазначених вимог передбачені штрафні санкції, обсяг яких залежить від тяжкості порушення і розміру організації. На виконання вказівок Єврокомісії була створена Європейська

мережа національних CSIRT і офіційно розпочала роботу мережа національних органів держав-членів, які відповідають за управління кіберкризами (European Cyber Crisis Liaison Organisation Network, EU-CyCLONe) [22].

З огляду на посилення ризиків кібербезпеки і зростання вразливості інституцій ЄС до кіберзагроз та інцидентів запроваджено загальні стандарти кібербезпеки щодо створення структур управління безпекою й оцінки ризиків, розробки планів удосконалення кібербезпеки; розширено можливості й фінансування CERT-EU, яка здійснює нагляд за станом кібербезпеки установ та організацій Євросоюзу; передбачено створення міжвідомчого органу з безпеки (Interinstitutional Cybersecurity Board), який стежитиме за реалізацією зазначених вимог. Також було узгоджено часові рамки для звітування про серйозні кіберінциденти [23].

Продовжуючи зусилля щодо розвитку безпечного й надійного єдиного цифрового ринку ЄС, у кінці 2022 року Єврокомісія внесла проєкт Регламенту щодо горизонтальних вимог кібербезпеки для продуктів із цифровими елементами (Акт про кіберстійкість, Cyber Resilience Act, CRA) [24], який спрямований на вирішення проблем неналежного рівня кібербезпеки цифрових продуктів, або неадекватного оновлення їхньої безпеки, а також відсутності у споживачів і компаній можливості визначити, які продукти є кіберзахищеними і вартими довіри.

Регламент вводить обов'язкові вимоги кібербезпеки протягом усього ланцюжка поставок і життєвого циклу апаратних і програмних продуктів (проєктування, розробки, виробництва та продажу), щоб уникнути дублювання вимог у різних нормативно-правових актах держав-членів ЄС, заповнити існуючі прогалини у чинному законодавстві про кібербезпеку ЄС і зробити його більш послідовним і узгодженим.

Відповідальність за дотримання нормативних вимог безпеки покладено на виробників, які зобов'язані проводити оцінку ризиків кібербезпеки для продуктів із цифровими елементами, доступними на ринку ЄС, декларувати дотримання відповідності та співпрацювати з відповідними компетентними органами ЄС. Також у Регламенті окреслено основні вимоги та зобов'язання виробників цифрових продуктів щодо процесів обробки кіберуразливостей, окреслено заходи щодо підвищення прозорості безпеки апаратних і програмних продуктів для споживачів і бізнес-користувачів, а також визначено структуру нагляду за ринком для забезпечення дотримання цих правил.

Слід відзначити, що проєкт Регламенту про кіберстійкість викликав широкий резонанс і бурхливу дискусію в експертних колах кібербезпеки, зокрема були висловлені побоювання щодо потенційного зловживання нормами закону про розкриття вразливостей [25] і створення серйозної загрози для майбутнього глобальної індустрії відкритого коду [26].

У листопаді 2023 року Рада ЄС і Європарламент досягли попередньої угоди щодо Регламенту про кіберстійкість, а в березні 2024 року Європарламент схвалив його зі змінами, внесеними за результатами дебатів. Щоб набути чинності, Регламент має бути офіційно прийнятий Радою ЄС [27].

Регламент про кіберстійкість стане першим у світі нормативним актом, який визначає вимоги безпеки для продуктів як перешкоду для входу на ринок. Обмеження почнуть діяти з 2027 року.

Реагуючи на виклики кібербезпеки та прагнучи посилити операційну спроможність ЄС із запобігання, стримування та реагування на кіберінциденти, у квітні 2023 року Єврокомісія внесла проєкт Регламенту щодо заходів посилення операційних можливостей ЄС з метою виявлення, підготовки та реагування на загрози й інциденти кібербезпеки (Акт про кіберсолідарність, Cyber Solidarity Act) [28].

Як передбачалося в останній Стратегії кібербезпеки ЄС, Регламент декларує створення Європейської системи оповіщення про кібербезпеку (European Cybersecurity Alert System) або Європейського кіберщита, що складається з операційних центрів безпеки (SOC) по всьому ЄС, об'єднаних у кілька платформ. Ці SOC використовують передові технології, такі як штучний інтелект і аналітику даних, щоб виявляти й ділитися попередженнями про кіберзагрози з органами влади інших країн-членів, а, отже, швидше й ефективніше реагувати на кіберзагрози.

Слід відзначити, що ще під час першого етапу, розпочатого в листопаді 2022 року, було обрано три консорціуми транскордонних SOC, які об'єднали державні органи з 17 держав-членів та Ісландії в рамках Програми цифрової Європи [29].

Також документ встановлює завдання щодо формування механізму реагування на надзвичайні кіберситуації (Cyber Emergency Mechanism), який забезпечить підвищення готовності й реагування на інциденти кібербезпеки, зокрема тестування на наявність потенційних вразливостей суб'єктів у важливих секторах (фінанси, енергетика та охорона здоров'я), створення резерву кібербезпеки ЄС у складі служб реагування на інциденти від надійних приватних постачальників послуг, взаємної допомоги між державами-членами ЄС.

Крім цього, Регламент запроваджує механізм перевірки інцидентів кібербезпеки. Так, на запит Єврокомісії або національних органів (мережі EU-CyCLONe або CSIRTs), ENISA перевірятиме значні й великомасштабні інциденти кібербезпеки з наданням звіту й рекомендацій щодо покращення реагування на конкретний вид кібератаки.

У березні 2024 року досягнуто попередньої угоди між Європейським парламентом і Радою щодо цього регламенту [30].

Як показало дослідження політика кібербезпеки Євросоюзу, яка зародилася в останній декаді XX ст., розвивалася поступально і досить динамічно, впроваджуючи нові рішення і підходи для пом'якшення проблем безпеки кіберпростору. За цей час Єврокомісія внесла низку важливих законодавчих ініціатив щодо посилення кібербезпеки і кіберстійкості Європейського Союзу і держав-членів, що було викликано розвитком ситуації у сфері кібербезпеки.

Водночас, у ході розробки і впровадження спільної політики кібербезпеки керівництво ЄС зіткнулося з низкою викликів і проблем (рис. 2).

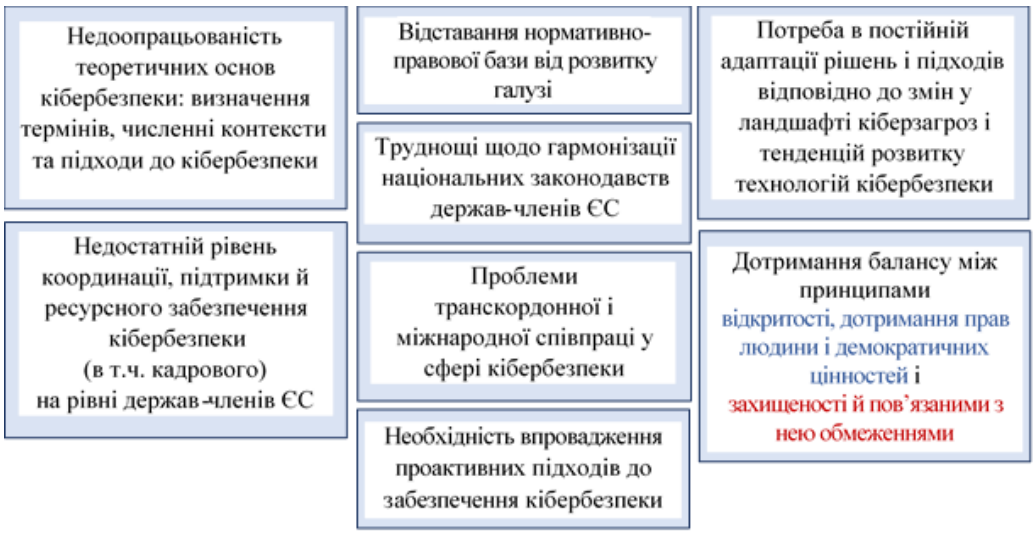

Рис. 2. Виклики і проблеми розробки і впровадження спільної політики кібербезпеки ЄС

Як бачимо, більшість проблем, пов'язані з недоліками управління ЄС і держав-членів (нормативно-правове, інституційне, кадрове забезпечення), труднощами координації зусиль і пошуку компромісів, оптимізації організаційних структур. Однак, викликами для ЄС стали також необхідність впровадження гнучких і проактивних підходів до забезпечення кібербезпеки, а також гарантування прав людини і демократичних цінностей в умовах обмежень, пов'язаних із забезпеченням захищеності кіберпростору.

Окремо слід відзначити, що в результаті розвитку політики кібербезпеки ЄС на порядку денному постало питання запровадження фундаментального права людини на кібербезпеку (безпечне цифрове життя) [31].

ВИСНОВКИ ТА ПЕРСПЕКТИВИ ПОДАЛЬШИХ ДОСЛІДЖЕНЬ

Дослідження показало, що впродовж останніх трьох десятиліть у відповідь на появу нових викликів цифрового середовища Європейський Союз досяг значних успіхів у розробці і впровадженні політики кібербезпеки. Об'єднання інституційних можливостей на рівні спільноти, зусиль держав-членів, співпраці з бізнесом і міжнародними партнерами забезпечило реалізацію ЄС низки узгоджених ініціатив у сфері кібербезпеки.

На початку 2000-х років визначено спільний підхід до політики кібербезпеки ЄС, який передбачав подальшу реалізацію заходів щодо: обґрунтування політики і вдосконалення нормативно-правової бази; створення європейської системи попередження й інформування; підтримки й інвестування в технологічні рішення кібербезпеки; підвищення цифрової обізнаності; впровадження ринково-орієнтованої стандартизації і сертифікації; забезпечення безпеки інституцій ЄС і держав-членів; посилення міжнародної співпраці в галузі кібербезпеки. У рамках перелічених напрямів загалом в подальшому відбувався розвиток і вдосконалення політики ЄС у цій сфері й надалі.

Встановлено, що ключову роль у еволюції сучасної політики кібербезпеки ЄС відіграли стратегії кібербезпеки 2013, 2017 та 2020 років, які відображали зміни у підходах до забезпечення кібербезпеки як реагування на зміни цифрового середовища.

Узагальнивши положення зазначених стратегій, слід зазначити, що політика кібербезпеки ЄС була і продовжує бути спрямованою на вирішення трьох ключових цілей: досягнення кіберстійкості як здатності забезпечити стабільне функціонування Європейської спільноти, держави, організацій в умовах постійних кіберзагроз; забезпечення ефективного кіберстримування (запобігання, стримування та реагування на кіберінциденти, протидія кіберзлочинності); просування безпечного і відкритого глобального кіберпростору з дотриманням прав людини, унормуванням поведінки й багатостороннім управлінням Інтернетом) через міжнародну співпрацю і провідну роль у ній ЄС.

На виконання задекларованих цілей політики кібербезпеки впродовж останніх років Єврокомісія запропонувала і впровадила низку важливих ініціатив, зокрема щодо підвищення рівня кібербезпеки в державах ЄС; встановлення спільних стандартів кібербезпеки для інституцій ЄС; впровадження вимог кібербезпеки для продуктів із цифровими елементами; посилення потужностей ЄС з метою виявлення, підготовки й реагування на загрози й інциденти кібербезпеки.

Водночас, у процесі розробки і впровадження політики кібербезпеки Євросоюз зіткнувся з низкою труднощів, серед яких недостатній рівень координації, підтримки й ресурсного забезпечення політики кібербезпеки; відставання нормативно-правової бази кібербезпеки від розвитку галузі; труднощі транскордонної і міжнародної співпраці; потреба

впровадження проактивного підходу й постійної адаптації політики до динамічного кіберсередовища; необхідність дотримання балансу між відкритістю й безпекою тощо.

Отже, політика кібербезпеки Євросоюзу, яка була започаткована в кінці XX ст., розвивається поступально і динамічно, передбачає впровадження нових рішень і підходів у відповідь на виклики цифрового середовища, може бути еталоном для інших держав, зокрема й України.

У перспективі планується дослідити особливості інституційного забезпечення як важливої складової розробки і впровадження політики кібербезпеки ЄС.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Бойко, В., Василенко, М., & Кухаренко, С. (2019). Кібербезпека в ЄС та країнах-членах: генезис та проблеми її підвищення. *Інформаційна безпека людини, суспільства, держави*, *3(27)*, 57–69.
2. Грубінко, А. (2021). Особливості формування політики кібербезпеки Європейського Союзу: правові аспекти. *Актуальні проблеми правознавства*, *1(25)*, 5–10.
3. Кузнєцов, О. (2021). Європейський досвід посилення спроможностей у сфері забезпечення кібербезпеки в сучасних умовах. *Інформація і право, 1(36),* 106–113. https://doi.org/10.37750/2616-6798.2021.1(36).238189
4. Федонюк, С. (2021). Політика ЄС в аспекті основних глобальних концепцій інформаційної (кібер) безпеки. Розділ II. *Суспільні комунікації та мовні універсалії*, *3(11),* 144–168. https://doi.org/10.29038/2524-2679-2021-03-144-168
5. Caspar, A., & Antonov, A. (2019). Towards Conceptualizing EU Cybersecurity Law. *ZEI Discussion Paper*.
6. Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. *The Ethics of Cybersecurity*, *21*, 97–115. https://doi.org/10.1007/978-3-030-29053-5_5
7. García Segura, L.A. (2020). European Cybersecurity: Future Challenges from a Human Rights Perspective. *Security and Defence in Europe*, 35–46. https://doi.org/10.1007/978-3-030-12293-5_3
8. Papakonstantinou, V. (2022). Cybersecurity as *praxis* and as a *state*: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review, 44.* https://doi.org/10.1016/j.clsr.2022.105653
9. *EUR-Lex - 52001DC0298 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298
10. *EUR-Lex - 32002G0216(02) - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216(02)
11. *EUR-Lex - 32004R0460 - EN*. (n. d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
12. *EUR-Lex - 52006DC0251 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0251
13. *EUR-Lex - 52009DC0149 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149
14. *EUR-Lex - 52013JC0001 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001
15. *European Cybercrime Centre - EC3 | Europol*. (n.d.). Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
16. *Directive - 2013/40 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040&qid=1709725652664
17. *Directive - 2016/1148 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148&qid=1709740990646
18. *EUR-Lex - 52017JC0450 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52017JC0450
19. *The EU Cyber Diplomacy Toolbox*. (n.d.). The EU Cyber Diplomacy Toolbox. https://www.cyber-diplomacy-toolbox.com/

20. *Regulation - 2019/881 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881&qid=1701413940571
21. *EUR-Lex - 52020JC0018 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020JC0018
22. *Directive - 2022/2555 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555&qid=1708526033822
23. *Regulation - EU - 2023/2841 - EN - EUR-Lex*. (n. d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2841&qid=1708541342208
24. *EUR-Lex - 52022PC0454 - EN - EUR-Lex*. (n. d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
25. Allan, K. (2023). *A mixed response on EU's new vulnerability disclosure rules*. Home of Cybersecurity News | Cyber Magazine. https://cybermagazine.com/articles/a-mixed-response-on-eus-new-vulnerability-disclosure-rules
26. Fox, B. (2023). *The Cyber Resilience Act Threatens the Future of Open Source.* Devops. https://devops.com/the-cyber-resilience-act-threatens-the-future-of-open-source/
27. *The European Cyber Resilience Act (CRA).* (2022). https://www.european-cyber-resilience-act.com/
28. *EUR-Lex - 52023PC0209 - EN - EUR-Lex*. (n. d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209
29. European Commission. (2022). *Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres* [Press release]. https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security
30. European Commission. (2024). *Commission welcomes political agreement on Cyber Solidarity Act* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332
31. Chiara, P. G. (2023). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review, 53.* https://doi.org/10.1016/j.clsr.2024.105961

КІБЕРБЕЗПЕКА: освіта, наука, техніка
CYBERSECURITY: EDUCATION, SCIENCE, TECHNIQUE
№ 4 (24), 2024
ISSN 2663 - 4023

Tetiana Muzhanova
PhD in Public Administration, Associate Professor, Associate Professor of
Information Security and Cyber Security Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-7435-0287
muzanovat@gmail.com

Svitlana Lehominova
Doctor of Economics, Professor, Head of Information Security
and Cyber Security Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-4433-5123
chiarasvitlana77@gmail.com

Yurii Shchavinsky
PhD in Technacal Science, Associate Professor, Associate Professor of
Information Security and Cyber Security Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-2319-8983
yushchavinsky@ukr.net

Yuriy Yakymenko
PhD in Military Science, Associate Professor, Associate Professor of
Information Security and Cyber Security Management Department
State University of Information and Communication Technologies, Kyiv, Ukraine
ORCID ID: 0000-0002-6848-852X
yakum14@ukr.net

Halyna Nesterenko
PhD in Public Administration, Associate Professor, Associate Professor of
Department of Public Management and Administration
The Educational and Scientific Institute of Continuing Education
National Aviation University, Kyiv, Ukraine
ORCID ID: 0000-0002-1106-3790
halynanesterenko@gmail.com

MAIN APPROACHES AND DIRECTIONS OF DEVELOPMENT OF EUROPEAN UNION CYBER SECURITY POLICY

Abstract. The implementation of digital technologies into all spheres of society's life, along with many advantages, has caused the emergence of new security challenges, the response to which requires flexible, innovative and complex approaches, a quick and coordinated reaction, and the consolidation of efforts of many stakeholders. In recent years, significant results in the development and realization of cybersecurity policy have been achieved by the European Union, which, thanks to the combination of institutional capabilities at the community level, efforts of member states, cooperation with business and international partners, is already implementing a number of coordinated initiatives in the field of cybersecurity. The experience of the EU in solving the problems of safe digital development can be a benchmark for other states, including Ukraine. The article examines the development of the main approaches and directions of the EU cyber security policy from the end of the 90s of the 20th century to the present day. It has been established that since the beginning of the 2000s, the European Commission outlined a common approach to the EU cyber security policy, which provided for the further implementation of measures related to: justification of the policy and improvement of the legal framework; creation of a European warning and information system; supporting and investing in cyber security technological solutions; increasing digital awareness; introduction of market oriented standardization and certification; ensuring the security of EU institutions and member states; international cooperation in the field of cyber security. The listed directions generally remained relevant during the further development and improvement of EU policy of cyber security. The study showed that the next stages of the evolution

of the EU cyber security policy were related with the adoption of three cyber security strategies of 2013, 2017 and 2020, which reflected the development trends of the digital environment and the need to respond to new cyber security challenges. The analysis of these strategies indicated that the EU cyber security policy was and continues to be aimed at solving three key goals: achieving cyber resilience of the European Community, the state, and organizations in the face of constant cyber threats; ensuring effective cyber resilience; promoting a safe and open global cyberspace. In order to fulfill the declared goals of the cyber security policy during 2022–2023, the European Commission proposed a number of important initiatives, in particular, to increase the level of cyber security in the EU states; establish common cyber security standards for EU institutions; implement cybersecurity requirements for products with digital elements; strengthen the EU's capabilities to identify, prepare for and respond to cyber security threats and incidents. It was established that during the development and implementation of the cyber security policy, the EU faced a number of problems and challenges, including an insufficient level of coordination, support and resource provision; lagging behind the regulatory and legal framework of cyber security from the development of the field; difficulties of cross-border and international cooperation; the need for a proactive approach and policy adaptation to the dynamic cyber environment; necessity to maintain a balance between openness and security, etc. It has been proven that the cyber security policy of the European Union, which is developing progressively and dynamically, involves the implementation of new approaches and solutions in response to the challenges of the digital environment, is a benchmark for other states, in particular Ukraine.

Keywords: cyber security; cyber security policy of the European Union; EU cyber security legislation.

REFERENCES (TRANSLATED AND TRANSLITERATED)

1. Boiko, V., Vasylenko, M., & Kuharenko, S. (2019). Cyber security in the EU and its member states: genesis and problems of its improvement. *Information security of a person, society, state, 3(27),* 57–69.
2. Grubinko, A. (2021). Peculiarities of the formation of the cyber security policy of the European Union: legal aspects. *Actual problems of jurisprudence, 1(25),* 5–10.
3. Kuznetsov, O. (2021). European experience of strengthening capabilities in the field of ensuring cyber security in modern conditions. *Information and law, 1(36),* 106–113. https://doi.org/10.37750/2616-6798.2021.1(36).238189
4. Fedonyuk, S. (2021). EU policy in the aspect of the main global concepts of information (cyber) security Section II. *Public communications and language universals, 3(11),* 144–168. https://doi.org/10.29038/2524-2679-2021-03-144-168
5. Caspar, A., & Antonov, A. (2019). Towards Conceptualizing EU Cybersecurity Law. *ZEI Discussion Paper*.
6. Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity Regulation in the European Union: The Digital, the Critical and Fundamental Rights. *The Ethics of Cybersecurity, 21,* 97–115. https://doi.org/10.1007/978-3-030-29053-5_5
7. García Segura, L.A. (2020). European Cybersecurity: Future Challenges from a Human Rights Perspective. *Security and Defence in Europe,* 35–46. https://doi.org/10.1007/978-3-030-12293-5_3
8. Papakonstantinou, V. (2022). Cybersecurity as *praxis* and as a *state*: The EU law path towards acknowledgement of a new right to cybersecurity? *Computer Law & Security Review, 44.* https://doi.org/10.1016/j.clsr.2022.105653
9. *EUR-Lex - 52001DC0298 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52001DC0298
10. *EUR-Lex - 32002G0216(02) - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32002G0216(02)
11. *EUR-Lex - 32004R0460 - EN*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32004R0460:EN:HTML
12. *EUR-Lex - 52006DC0251 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52006DC0251
13. *EUR-Lex - 52009DC0149 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:52009DC0149

14. *EUR-Lex - 52013JC0001 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52013JC0001
15. *European Cybercrime Centre - EC3 | Europol*. (n.d.). Europol. https://www.europol.europa.eu/about-europol/european-cybercrime-centre-ec3
16. *Directive - 2013/40 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32013L0040&qid=1709725652664
17. *Directive - 2016/1148 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L1148&qid=1709740990646
18. *EUR-Lex - 52017JC0450 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:52017JC0450
19. *The EU Cyber Diplomacy Toolbox*. (n.d.). The EU Cyber Diplomacy Toolbox. https://www.cyber-diplomacy-toolbox.com/
20. *Regulation - 2019/881 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32019R0881&qid=1701413940571
21. *EUR-Lex - 52020JC0018 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:52020JC0018
22. *Directive - 2022/2555 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555&qid=1708526033822
23. *Regulation - EU - 2023/2841 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32023R2841&qid=1708541342208
24. *EUR-Lex - 52022PC0454 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454
25. Allan, K. (2023). *A mixed response on EU's new vulnerability disclosure rules*. Home of Cybersecurity News | Cyber Magazine. https://cybermagazine.com/articles/a-mixed-response-on-eus-new-vulnerability-disclosure-rules
26. Fox, B. (2023). *The Cyber Resilience Act Threatens the Future of Open Source.* Devops. https://devops.com/the-cyber-resilience-act-threatens-the-future-of-open-source/
27. *The European Cyber Resilience Act (CRA).* (2022). https://www.european-cyber-resilience-act.com/
28. *EUR-Lex - 52023PC0209 - EN - EUR-Lex*. (n.d.). EUR-Lex — Access to European Union law — choose your language. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0209
29. European Commission. (2022). *Cybersecurity: EU launches first phase of deployment of the European infrastructure of cross-border security operations centres* [Press release]. https://digital-strategy.ec.europa.eu/en/news/cybersecurity-eu-launches-first-phase-deployment-european-infrastructure-cross-border-security
30. European Commission. (2024). *Commission welcomes political agreement on Cyber Solidarity Act* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_1332
31. Chiara, P. G. (2023). Towards a right to cybersecurity in EU law? The challenges ahead. *Computer Law & Security Review, 53.* https://doi.org/10.1016/j.clsr.2024.105961