ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

https://doi.org/10.58442/3041-1858-2025-32(61)-328-346
УДК 352/354: 681.004

Олійник Наталія Іванівна,
доктор наук з державного управління, професор,
професор кафедри публічного управління і
проектного менеджменту
Навчально-наукового інституту менеджменту та психології
ДЗВО «Університет менеджменту освіти».
Київ, Україна.
https://orcid.org/0000-0001-8489-4141
nataliyao888@gmail.com

Петроє Іван Костянтинович,
аспірант кафедри публічного управління і проектного менеджменту
Навчально-наукового інституту менеджменту та психології
ДЗВО «Університет менеджменту освіти».
Київ, Україна.
https://orcid.org/0009-0004-4382-2343
petroei@gmail.com

ЕВОЛЮЦІЯ ЄВРОПЕЙСЬКИХ НОРМАТИВНО-ПРАВОВИХ СТАНДАРТІВ ТА МЕХАНІЗМІВ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ В ОРГАНАХ ПУБЛІЧНОЇ ВЛАДИ В УМОВАХ ЦИФРОВИХ ТРАНСФОРМАЦІЙ

Анотація. У статті проаналізовано ключові фактори та основні загрози у сфері інформаційної та кібербезпеки на глобальному, європейському та національному рівні. Розкрито актуальність завдання удосконалення системи інформаційної безпеки в органах публічної влади України в умовах цифрових трансформацій, зростаючих глобальних та національних викликів, спричинених, з одного боку триваючою російською військовою агресією, а з другого, необхідністю виконання нашою країною євроінтеграційних зобов'язань як країни-кандидата на вступ до Європейського Союзу (ЄС). Обґрунтовано важливість імплементації європейських стандартів та механізмів управління інформаційною безпекою як умови ефективного забезпечення інформаційної безпеки в органах публічної влади України. Здійснено комплексний аналіз особливостей формування та еволюції нормативно-правових стандартів та механізмів управління інформаційною безпекою ЄС в умовах цифрових трансформацій. Виокремлено основні напрями політики ЄС у системі інформаційної безпеки: 1) захист персональних даних; 2) мережева та інформаційна безпека 3) стратегічне управління

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

кібербезпекою та гармонізація законодавства у сфері кібербезпеки. Встановлено тенденції розвитку інформаційної політики ЄС, ключовою серед яких є посилення ролі кібербезпеки в системі забезпечення інформаційної безпеки. Проаналізовано новітні нормативно-правові стандарти політики ЄС у сфері інформаційної та кібербезпеки, впровадження якої забезпечує комплекс механізмів з гармонізації законодавства ЄС і країн-членів через директиви, регламенти, стратегічні програми ЄС; розвиток співпраці між державами-членами; оптимізацію різних правових рамок установ та органів ЄС в цій сфері; впровадження заходів для високого загального рівня кібербезпеки в установах, органах, офісах та агентствах ЄС; створення жорстких єдиних стандартів безпечного обміну інформацією, обов'язкових до застосування всіма інституціями, органами та агентствами ЄС; забезпечення інституційної підтримки політики ЄС у цій сфері; встановлення вимог щодо дотримання мінімального набору правил інформаційної безпеки та кібербезпеки для всіх установ ЄС та органів публічної влади країн-членів у фізичному та цифровому середовищі; фінансування досліджень та інновацій у сфері кібербезпеки; підвищення цифрової грамотності громадян і бізнесу та ін.

Ключові слова: цифрові трансформації; інформаційна безпека; кібербезпека; органи публічної влади; ЄС; нормативно-правові стандарти; механізми управління.

ВСТУП / INTRODUCTION

Постановка проблеми / Statement of the problem. Актуальність теми дослідження зумовлена низкою причин. Згідно з висновками експертів «Global Cybersecurity Outlook 2025» Всесвітнього економічного форуму, кібербезпека вступає в епоху безпрецедентної складності, зростаючої палітри кіберландшафту, який має глибокі та далекосяжні наслідки для організацій і націй. Ця складність зумовлена комплексом факторів [1]:

Геополітична напруженість: зростання загроз кібершпигунства і втрати конфіденційної інформації внаслідок поточних глобальних конфліктів.

Штучний інтелект. Швидке впровадження нових технологій спричиняє появу нових кіберзагроз, кіберзлочинів.

Складність кіберзлочинності: генеративні інструменти ШІ змінюють ландшафт кіберзлочинності, дозволяючи злочинцям удосконалювати свої

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

методи, а також автоматизувати та персоналізувати свої методи фішингу, вішингу, дипфейку та інших атак соціальної інженерії.

Взаємозалежності ланцюгів постачання: труднощі з дотриманням стандартів безпеки та управлінням ризиками, пов'язаними зі складними ланцюгами постачання та залежністю від критичних постачальників.

Дефіцит кібернавичок: усі вказані проблеми посилюються через збільшення розриву в навичках, що робить їх надзвичайно складними для ефективного управління. Майже половина (49 %) респондентів публічного сектору вказали, що вони не мають необхідної робочої сили для досягнення своїх цілей у сфері кібербезпеки.

Нормативні вимоги: збільшення кількості регуляторних актів і дисгармонія між ними створює додаткові виклики та додаткові труднощі щодо забезпечення їх дотримання для організацій.

В аналітичному огляді «Enisa Threat Landscape 2024» за результатами вивчення ситуації в період з липня 2023 по червень 2024 р. представники Агентства Європейського Союзу з кібербезпеки (ENISA) визначили сім основних загроз кібербезпеці: 1) програми-вимагачі; 2) шкідливе програмне забезпечення; 3) соціальна інженерія; 4) загрози для даних; 5) загрози доступності: відмова в обслуговуванні; 6) маніпулювання інформацією та втручання; 7) атаки на ланцюги постачання [2]. У документі наголошено на значній ескалації атак на кібербезпеку в досліджуваний період, на нових параметрах як різноманітності, так і кількості кіберінцидентів, а також їх наслідків.

За даними «The Global Risks Report 2023» Світового економічного форуму, з початку повномасштабного вторгнення багаторазово збільшилися інтенсивність та масштаби інформаційних диверсій з боку країни-агресора проти України [3]. З огляду на існуючі та всезростаючі глобальні та національні виклики, невідкладним є завдання впровадження цілеспрямованого, послідовного та узгодженого підходу до забезпечення захисту органів публічної влади України від постійно зростаючих інформаційних та кіберзагроз.

Питання інформаційної безпеки в органах публічної влади набуває особливого значення в сучасних умовах цифрової трансформації та інтеграції України до Європейського Союзу. Статус країни-члена ЄС передбачає адаптацію національних стандартів та механізмів управління інформаційною безпекою до європейських норм, що є ключовим компонентом забезпечення ефективного публічного управління. Європейський Союз має розвинену нормативно-правову базу та інституційні механізми забезпечення кібербезпеки, які обґрунтовуються на принципах відкритості, довіри та міждержавної співпраці. Їх імплементація

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

в національне законодавство України створює передумови для підвищення інформаційної та кіберстійкості органів публічної влади.

Аналіз (основних) останніх досліджень і публікацій / Analysis of (major) recent research and publications. Тема інформаційної безпеки знайшла висвітлення у працях закордонних (G. Kambourakis, R. Neisse, & I. Nai-Fovino (2021) [4], C. Rupp (2024) [5]) та українських вчених (V. Ahmadov, N. Klietsova, K. Bieliakov etc. (2021) [6], A. Krupnova (2023) [7], A. Marushchak, S. Petrov, M. Romanov, & O. Balashova (2021) [8], Т. Ткачук, (2024) [9], M. Shevchuk (2024) [10] та ін. Разом з тим, тема нормативно-правового забезпечення інформаційної безпеки в органах публічної влади залишається недостатньо дослідженою.

У контексті євроінтеграційних завдань України на окрему увагу заслуговує дослідження механізмів наближення українського законодавства до законодавства та права ЄС [11]. Теоретико-методологічну основу даного дослідження складають тексти регуляторних документів ЄС, у яких визначено правові засади та механізми ЄС в питаннях інформаційної та кібербезпеки, в тому числі – в установах ЄС та органах публічної влади країн-членів ЄС.

МЕТА ТА ЗАВДАННЯ / AIM AND TASKS

Мета дослідження – теоретико-методологічне обґрунтування нормативно-правових стандартів ЄС у сфері управління інформаційною безпекою в умовах цифрових трансформацій та визначення основних механізмів їх впровадження в органах публічної влади.

На досягнення мети визначено та виконано такі ***завдання***:

- здійснено аналіз особливостей формування та еволюції нормативно-правових стандартів у сфері інформаційної безпеки ЄС;
- визначено комплекс механізмів забезпечення ефективної системи інформаційної та кібербезпеки в інституціях ЄС і органах публічної влади країн-членів ЄС в умовах цифрових трансформацій.

ТЕОРЕТИЧНІ ОСНОВИ / THEORETICAL FRAMEWORK

Дослідження ґрунтується на відборі, контент-аналізі та узагальненні положень основних європейських офіційних документів у сфері інформаційної безпеки. Поглибленому вивченню спеціальних європейських стандартів інформаційної безпеки в органах публічної влади сприяв аналіз положень таких основних нормативно-правових документів ЄС у цій сфері як «Директива ЄС про захист осіб у зв'язку з обробкою персональних даних і про вільне переміщення таких даних» (1995), «Резолюція про спільний підхід та

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

конкретні дії у сфері мережевої інформаційної безпеки» (2002), «Стратегія кібербезпеки Європейського Союзу: відкритий, безпечний і захищений кіберпростір» (2013), «Регламент ЄС про захист про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних» (2016), «Директива ЄС щодо заходів для високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі» (2016), «Стратегія кібербезпеки ЄС на цифрове десятиліття» (2021), «Регламент ЄС щодо вимог до горизонтальної кібербезпеки для продуктів із цифровими елементами» (2022), «Директива ЄС про заходи щодо високого загального рівня кібербезпеки в Союзі» (2022), «Європейський акт про захист від кібернетичної інформації» (2024) та ін.

МЕТОДИ ДОСЛІДЖЕННЯ / RESEARCH METHODS

Методологічну основу дослідження складає метод аналізу правових документів, що включає методи пошуку, відбору, аналізу, синтезу, узагальнення, історичний метод, порівняльний та структурно-функціональний методи вивчення документальних джерел – європейських нормативно-правових документів у сфері інформаційної та кібербезпеки. Окрема увага в дослідженні відведена аналізу нормативно-правових механізмів управління інформаційною безпекою в інституціях ЄС та органах публічної влади країн-членів ЄС в умовах цифрових трансформацій.

РЕЗУЛЬТАТИ ДОСЛІДЖЕННЯ / RESEARCH RESULTS

Запобігання інформаційним та кіберзагрозам і забезпечення інформаційної безпеки є всезростаючим викликом для органів публічної влади. Сучасне публічне управління стає вразливим без забезпечення належного рівня інформаційної безпеки. На думку авторів статті «Правові питання інформаційної безпеки органів державної влади в Україні та Європейському Союзі», високі темпи формування глобального інформаційного простору та інформатизації всіх сфер життєдіяльності суспільства створили передумови для інтенсивного використання інформаційних технологій для здійснення публічного управління, а разом з тим і для появи нових загроз інформаційній безпеці держав V. Ahmadov, N. Klietsova, K. Bieliakov, A. Klochko, & T. Kravtsova (2021) [6].

Інформаційні системи визнані ключовим елементом політичної, соціальної та економічної взаємодії в ЄС. Європейське суспільство все більше залежить від інформаційних, мережевих та кіберсистем. Відтак, їх безперебійна робота та інформаційна безпека в ЄС визнана життєво

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

важливою для розвитку внутрішнього ринку та конкурентоспроможної інноваційної економіки [12].

Основи формування політики інформаційної безпеки ЄС закладено в низці ключових стандартів, основні з яких представлено в табл. 1.

Таблиця 1

Еволюція європейських стандартів ЄС у сфері інформаційної та кібербезпеки

Рік	Назва документа
1995	Директива ЄС про захист осіб у зв'язку з обробкою персональних даних і про вільне переміщення таких даних [13]*
2002	Резолюція про спільний підхід та конкретні дії у сфері мережевої інформаційної безпеки» [14]
2013	Стратегія кібербезпеки Європейського Союзу: відкритий, безпечний і захищений кіберпростір [15]
2016	Регламент ЄС про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних (GDPR) [16]
2016	Директива ЄС щодо заходів для високого загального рівня безпеки мережевих та інформаційних систем у всьому Союзі [17]**
2019	Новий Стратегічний порядок денний 2019–2024 [18]
2021	Стратегія кібербезпеки ЄС на цифрове десятиліття [19]
2022	Пропозиції ЄК про Регламент ЄС щодо вимог до горизонтальної кібербезпеки для продуктів із цифровими елементами [20]
2022	Директива ЄС про заходи щодо високого загального рівня кібербезпеки в Союзі (NIS2) [21]***
2024	Європейський акт про захист від кібернетичної інформації [22] та ін.

*Скасована Загальним регламентом захисту даних GDPR, 2018.

***Скасована Директивою ЕС 2022/2555.*

****Замінює першу Директиву NIS 2016/1148.*

Джерело: Складено авторами на основі аналізу та узагальнення першоджерел

Контент-аналіз представлених у табл. 1 ключових стандартів ЄС у сфері інформаційної та кібербезпеки дає підстави для виокремлення таких основних напрямів політики ЄС у цій сфері: 1) захист персональних даних; 2) мережева та інформаційна безпека 3) стратегічне управління кібербезпекою та гармонізація законодавства у сфері кібербезпеки (табл. 2).

Результати аналізу європейських стандартів відображають тенденції розвитку інформаційної політики ЄС, ключовою серед яких є посилення ролі кібербезпеки в системі забезпечення інформаційної безпеки. Кібербезпека визнана одним із ключових викликів для ЄС: вона має

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

критичний вплив не лише на економіку ЄС, а й на демократію, а також на безпеку та здоров'я населення.

Таблиця 2

Основні напрями нормативно-правових стандартів ЄС у сфері інформаційної безпеки та кібербезпеки

Основні напрями формування і розвитку нормативно-правових стандартів ЄС у сфері інформаційної безпеки та кібербезпеки	
1	
№ з/п	Цілі і завдання нормативно-правових стандартів ЄС у сфері інформаційної безпеки та кібербезпеки
Захист персональних даних	
1	Забезпечення захисту персональних даних фізичних осіб, створення умов для транскордонного переміщення персональних даних між державами-членами ЄС [13]
2	Захист основних прав і свобод фізичних осіб, зокрема їхнього права на захист персональних даних. Забезпечення вільного руху таких даних в межах Європейського Союзу шляхом: гармонізації правил захисту даних, посилення прав суб'єктів даних, покладання відповідальності на контролерів та обробників даних; сприяння вільному потоку даних [16]
Мережева та інформаційна безпека	
1	Активізація зусиль щодо підвищення інформаційної безпеки, створення єдиного підходу до питання кібербезпеки, координація між державами-членами для захисту критично важливих інфраструктур і даних [14]
2	Підвищення загального рівня безпеки мережевих та інформаційних систем на території ЄС шляхом встановлення єдиних мінімальних стандартів кібербезпеки для критично важливих секторів економіки та суспільства, створення національних стратегій кібербезпеки, створення мережі співпраці між державами-членами ЄС, визначення секторів економіки, в яких оператори повинні відповідати вимогам кібербезпеки, встановлення вимог до постачальників цифрових послуг [17]
Стратегічне управління кібербезпекою та гармонізація законодавства у сфері кібербезпеки	
1	Упровадження системного підходу до забезпечення кібербезпеки в ЄС, посилення захищеності інформаційних систем та послуг, підвищення довіри до інтернет-середовища та зміцнення співпраці між державами-членами у сфері кібербезпеки [15]
2	Визначено пріоритетні напрями політики щодо забезпечення високого рівня кібербезпеки в ЄС для успішної цифрової трансформації суспільства та економіки шляхом створення стійкого та безпечного цифрового простору, посилення стійкості до кіберзагроз, підвищення кібербезпеки продуктів і послуг, посилення співпраці та обміну інформацією, розвитку кібердипломатії, підвищення рівня кіберграмотності [19]

ISBN 978-617-8335-49-6

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

Продовження табл. 2

1	
3	Підвищення рівня кібербезпеки в ЄС, гармонізація правил кібербезпеки шляхом встановлення єдиних правил кібербезпеки для продуктів з цифровими елементами в ЄС [20]
4	Досягнення високого спільного рівня кібербезпеки в ЄС шляхом встановлення більш суворих та деталізованих вимог, розширення сфери застосування Директиви, покращення стійкості до кіберзагроз, посилення співпраці між державами-членами ЄС та організаціями в галузі кібербезпеки, підвищення обізнаності співробітників з питань кібербезпеки [21]
5	Підвищення рівня кібербезпеки в ЄС шляхом підвищення безпеки продуктів з цифровими елементами, захисту споживачів і підприємств від кіберзагроз, які можуть призвести до фінансових втрат, порушення конфіденційності та інших негативних наслідків, гармонізація правил кібербезпеки в ЄС, створення єдиного ринку ЄС для безпечних цифрових продуктів [22]

Джерело: Складено авторами на основі першоджерел

Впровадження нормативно-правових стандартів ЄС у сфері інформаційної та кібербезпеки забезпечує комплекс механізмів щодо гармонізації законодавства через директиви та регламенти ЄС, розвиток співпраці між державами-членами, фінансування досліджень та інновацій у сфері кібербезпеки, підвищення цифрової грамотності громадян, бізнесу тощо. У 2013 році Європейська Комісія опублікувала першу Стратегію ЄС з кібербезпеки «Відкритий, безпечний та захищений кіберпростір» (2013) [15]. У 2016 році держави-члени ЄС та Європейський парламент прийняли перше в ЄС горизонтальне законодавство про кібербезпеку – «Директиву про мережеву та інформаційну безпеку» [17].

Підвищеною увагою ЄС до інформаційної та кібербезпеки позначилися останні роки, що об’єктивно спричинено зростанням кіберзлочинності внаслідок цифрових трансформацій та поширення цифрових інфраструктур, технологій штучного інтелекту, онлайн-систем комунікації та взаємодії [23]. Правову основу новітньої інформаційної політики в ЄС складають визначені в «Стратегічному порядку денному Європейської Ради на 2019–2024 роки» завдання захистити суспільство ЄС від зловмисної кіберактивності, гібридних загроз і дезінформації, що походять від ворожих державних і недержавних суб’єктів. У документі було обґрунтовано необхідність комплексного підходу до вирішення цього завдання – з більшою співпрацею, більшою координацією, більшими ресурсами та більшими технологічними можливостями розвивати і зміцнювати боротьбу з тероризмом і транскордонною злочинністю,

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

покращуючи співпрацю та обмін інформацією, а також розвиваючи спільні інструменти. У рамках цієї стратегії було заплановано створити мінімальний набір правил щодо інформаційної безпеки та кібербезпеки для всіх установ Союзу та органів у фізичному та цифровому середовищі, яка визначила 4 стратегічні пріоритети для дій на рівні ЄС [18]:

1. Перспективне середовище безпеки;
2. Боротьба із загрозами, що розвиваються;
3. Захист європейців від тероризму та організованої злочинності;
4. Сильна європейська екосистема безпеки.

У грудні 2020 р. ЄК виступила з ініціативою створення жорстких єдиних стандартів безпечного обміну інформацією, обов'язкових до застосування всіма інституціями, органами та агентствами ЄС [24]. У 2022 р. ЄК надала «Пропозиції щодо інформаційної безпеки в установах, органах, офісах та агентствах ЄС» [25], спрямовані на оптимізацію різних правових рамок установ та органів Союзу в цій сфері шляхом: встановлення гармонізованих і всеохопних категорій інформації, а також загальних правил поводження з нею для всіх установ і органів ЄС; створення схеми співробітництва з інформаційної безпеки між установами та органами ЄС; модернізація політик інформаційної безпеки на всіх рівнях класифікації/категоризації, для всіх установ та органів ЄС, з урахуванням цифрової трансформації та розвитку дистанційної роботи як структурної практики.

У відповідь на Пропозиції ЄК, у 2023 р. Було схвалено «Регламент ЄС, що встановлює заходи для високого загального рівня кібербезпеки в установах, органах, офісах та агентствах Союзу» [26], який передбачає: створення внутрішньої системи управління та контролю ризиків кібербезпеки для кожного суб'єкта ЄС; управління ризиками кібербезпеки, звітність та обмін інформацією; створення Міжвідомчої ради з кібербезпеки (IICB) та розширення мандату Служби кібербезпеки для установ, органів, офісів та агентств Союзу (CERT-EU); моніторинг виконання нормативно-правового акту.

Важлива роль у сфері інформаційної безпеки та кібербезпеки відведена механізмам забезпечення інституційної підтримки політики ЄС. З метою підвищення рівня мережевої та інформаційної безпеки в ЄС, розвитку культури мережевої та інформаційної безпеки в інтересах громадян, споживачів, бізнесу та організацій публічного сектору у 2004 р. в ЄС було засновано «Європейське агентство з мережевої та інформаційної безпеки», ENISA (2004) [27]. У 2019 р. це агентство було перейменовано на «Агентство ЄС з кібербезпеки» з наданням йому розширених повноважень та завдань сприяння кіберполітиці ЄС, підвищення надійності продуктів і послуг ІКТ, сертифікації у сфері кібербезпеки, співпраці з державами-

ISBN 978-617-8335-49-6

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

членами та органами ЄС, а також підготовки до кібервикликів завтрашнього дня [28].

ВИСНОВКИ / CONCLUSIONS

1. Результати проведеного дослідження підтверджують, що в умовах цифрової трансформації органи публічної влади стикаються з нарощуваними загрозами у сфері інформаційної та кібербезпеки, подолання яких вимагає удосконалення усього комплексу механізмів публічного управління у цій сфері, зокрема, нормативно-правових.

2. Правове забезпечення інформаційної безпеки в органах публічної влади є багатогранним процесом, що включає імплементацію міжнародних, і передусім європейських стандартів для удосконалення національного законодавства у сфері інформаційної безпеки. Аналіз політики ЄС у сфері інформаційної безпеки є фундаментальною передумовою для формування виваженої, структурованої та стійкої політики інформаційної безпеки в Україні. Завдання удосконалення національної політики інформаційної безпеки набуває особливого значення внаслідок зростання інформаційних загроз в умовах триваючої військової російської агресії. З іншого боку, імплементація та застосування законодавства ЄС у сфері інформаційної безпеки є умовою виконання Україною зобов'язань як країни-кандидата на вступ до ЄС. Комплексний підхід до цих аспектів сприятиме підвищенню рівня інформаційної безпеки та ефективності функціонування органів публічної влади в Україні. Впровадження європейських стандартів сприятиме зміцненню національної кібербезпеки України, підвищенню довіри до цифрових послуг та захисту критично важливих публічних інституцій.

3. За результатами дослідження, у ЄС розроблено і впроваджено багаторівневу нормативно-правову систему регулювання інформаційної безпеки, яка еволюціонувала від базових директив із захисту персональних даних до комплексних стратегій кібербезпеки. Контент-аналіз європейських нормативних стандартів свідчить, що основними напрямами розвитку системи інформаційної безпеки в ЄС є: 1) захист персональних даних; 2) Мережева та інформаційна безпека; 3) Стратегічне управління у сфері кібербезпеки та гармонізація законодавства ЄС і країн-членів.

4. Отримані результати можуть бути використані для формування та реалізації політики імплементації європейських стандартів у національне законодавство та інституційні політики органів публічної влади з удосконалення систем забезпечення інформаційної безпеки.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

Перспективи подальших досліджень у цьому напрямі / Prospects for further research in this direction. Перспективною для подальших досліджень є проблема забезпечення інформаційної безпеки в органах публічної влади в умовах динамічного та масштабного впровадження штучного інтелекту.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ / REFERENCES

[1] «Global Cybersecurity Outlook 2025», *World Economic Forum*. [Online]. Available: https://is.gd/w028PO Application date: February 05, 2025.

[2] «ENISA Threat Landscape 2024», *European Union Agency for Cybersecurity*, 2024. [Online]. Available: https://is.gd/r8HGDp Application date: February 05, 2025.

[3] «The Global Risks Report 2023. 18th Edition Insight Report», *World Economic Forum*, 2023. [Online]. Available: https://is.gd/rgaWeA Application date: February 05, 2025.

[4] G. Kambourakis, R. Neisse, and I. Nai-Fovino, «Information security in the age of EU Institutions digitalisation, a landscape analysis», *European Commission,* 2021. [Online]. Available: https://is.gd/D3zAuX Application date: February 05, 2025.

[5] C. Rupp, «Navigating the EU Cybersecurity Policy Ecosystem. A Comprehensive Overview of Legislation, Policies and Actors», *Interface*, 2024. [Online]. Available: https://is.gd/joj6yB Application date: February 05, 2025.

[6] V. Ahmadov, N. Klietsova, K. Bieliakov, A. Klochko, and T. Kravtsova, «Legal issues of information security of public authorities in Ukraine and the European Union: Experience and realities», *AD ALTA: Journal of Interdisciplinary Research*, vol. 11, is. 2, pp. 12–17, 2021. [Online]. Available: http://ep3.nuwm.edu.ua/id/eprint/21131 Application date: February 05, 2025.

[7] А. О. Крупнова, «правове регулювання сфери забезпечення інформаційної безпеки в Україні», *Аналітично-порівняльне правознавство*, № 5, с. 348–354, 2023. https://doi.org/10.24144/2788-6018.2023.05.62

[8] A. Marushchak, S. Petrov, M. Romanov, and O. Balashova, «The Problem of Legal Regulation of the Security of a Person, Society, State in the Formation of the Information Society in Ukraine», *European Journal of Transformation Studies*, vol. 9 No. 1, pp. 101–116, 2021. [Online]. Available: https://is.gd/ADJdq0 Application date: February 05, 2025.

[9] Т. Ю. Ткачук, *Забезпечення інформаційної безпеки в умовах євроінтеграції України: правовий вимір*. Київ, Україна : ТОВ «Видав. дім «АртЕк», 2018.

[10] М. Шевчук, «Особливості правового забезпечення інформаційної безпеки з урахуванням сучасних загроз національній безпеці», *Правовий часопис Донбасу*, № 1, с. 45–50, 2024. https://doi.org/10.32782/2523-4269-2024-86-45-50

[11] *«Рекомендації для українських органів державного управління щодо наближення до права ЄС».* Київ, Україна, 2018. [Електронний ресурс]. Доступно: https://is.gd/7oAI34 Дата звернення: Лют. 10, 2025.

[12] H. Carrapico, and B. Farrand, «Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics», *Journal of Common Market Studies*, vol. 62, is. S1, pp. 147–158, Sep. 2024. https://doi.org/10.1111/jcms.13654

[13] «Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data», *Official Journal of the European Union*, L 281, pp. 31–50, October 23, 1995. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 Application date: February 05, 2025.

[14] «Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security», *Official Journal of the European Union*, C 43, pp. 2–4, February 16, 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2002_043_R_0002_01 Application date: February 05, 2025.

[15] «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace», European Commission, *JOIN, 1 final,* February, 7, 2013. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 Application date: February 05, 2025.

[16] «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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)», *Official Journal of the European Union*, April 27, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng Application date: February 05, 2025.

[17] «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», *Official Journal of the European Union,* L 194, pp. 1–30, July 6, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148 Application date: February 05, 2025.

[18] «A new Strategic Agenda 2019–2024», *European Council*, June 20, 2019. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/ Application date: February 05, 2025.

[19] European Commission, «EU's Cybersecurity Strategy for the Digital Decade», Brussels, December 16, 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 Application date: February 05, 2025.

[20] European Commission. (2022, September 15). Cyber Resilience Act *«Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020».* [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454

[21] «Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)», *Official Journal of the European Union*, L 333, pp. 80–152, December 14, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 Application date: February 05, 2025.

[22] «Cyber Resilience Act», *European Commission,* 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act Application date: February 05, 2025.

[23] І. К. Петроє, «Новітня політика інформаційної безпеки в Європейському Союзі: правовий аспект», на *II Всеукр. наук.-практ. конф. Теоретико-прикладні аспекти розвитку цифрової держави в Україні*. Київ, 2024, т. 30, с. 27–31. [Електронний ресурс]. Доступно: https://duikt.edu.ua/uploads/p_2661_23355401.pdf Дата звернення: Лют. 10, 2025.

[24] «Information security – common rules for EU institutions, bodies and agencies», *European Commission*, 2020. [Online]. Available: https://is.gd/RU8YBE Application date: February 05, 2025.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

[25] «Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union», *European Commission*, 2022. [Online]. Available: https://is.gd/uruEnL Application date: February 05, 2025.
[26] «Cybersecurity at the European Union institutions, bodies, offices and agencies», *European Union*, 2023. [Online]. Available: https://is.gd/kahbBR Application date: February 05, 2025.
[27] «European Network and Information Security Agency (ENISA)», *European Union*, March 10, 2004. [Online]. Available: https://is.gd/OxO8GW Application date: February 05, 2025.
[28] «2024 Report on the state of cybersecurity in the Union», *European Union Agency for Cybersecurity*, 2024. [Online]. Available: https://is.gd/9KKITH Application date: February 05, 2025.

Матеріал надійшов до редакції 13.03.2025 р.

VOLUTION OF EUROPEAN LEGAL STANDARDS AND MECHANISMS FOR INFORMATION SECURITY GOVERNANCE IN PUBLIC AUTHORITIES AMIDST DIGITAL TRANSFORMATIONS

Nataliia Oliinyk,
Doctor of Science in Public Administration, Professor,
Professor of the Department of Public Administration and
Project Management Educational and Scientific Institute
of Management and Psychology of the
SIHE «University of Educational Management».
Kyiv, Ukraine.
https://orcid.org/0000-0001-8489-4141
nataliyao888@gmail.com

Ivan Petroie,
postgraduate student of the
Department of Public Administration and
Project Management, Educational and Scientific Institute
of Management and Psychology of the
SIHE «University of Educational Management».
Kyiv, Ukraine.
https://orcid.org/0009-0004-4382-2343
petroei@gmail.com

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

Abstract. This article analyses the key factors and major threats in information and cybersecurity at the global, European, and national levels. The article addresses the pressing need to enhance the information security system within Ukraine's public authorities amidst digital transformations and escalating global and national challenges. These challenges are exacerbated by the ongoing Russian military aggression and the imperative for Ukraine to fulfill its European integration commitments as an EU candidate country. The study underscores the significance of implementing European standards and mechanisms for information security governance as a prerequisite for effectively safeguarding information security in Ukraine's public authorities. The authors made a comprehensive analysis that examines the formation and evolution of EU legal standards and mechanisms for information security governance in the context of digital transformations. The analysis results delineate the EU's core policy directions in this domain, including 1) personal data protection; 2) network and information security; 3) strategic cybersecurity governance and legislative harmonization in cybersecurity. The trends in EU information policy, the key of them is the increasing role of cybersecurity within the information security framework, were identified. The article highlights the newest EU legal standards in information and cybersecurity, the implementation of which involves a suite of mechanisms designed to harmonize EU and member state legislation through directives, regulations, and strategic EU programs. These mechanisms include enhanced cooperation among member states, streamline diverse legal frameworks across EU institutions and bodies, implement measures for a high common level of cybersecurity across EU institutions, bodies, offices, and agencies, establish stringent unified standards for secure information exchange applicable to all EU institutions, bodies, and agencies, provide institutional support for EU policy in this area, set requirements for adherence to a minimum set of information and cybersecurity rules for all EU institutions and member state public authorities in physical and digital environments, fund cybersecurity research and innovation, and promote digital literacy among citizens and businesses, among other initiatives.

Keywords: Digital transformations; information security; cybersecurity; public authorities; EU; legal standards; governance mechanisms.

ISSN 3041-1858 (print) Ідентифікатор медіа: R30-05167
ISSN 3041-1866 (online) Media identifier: R30-05167
Вісник післядипломної освіти: збірник наукових праць. Серія «Соціальні та поведінкові науки; Управління та адміністрування». Вип. 32(61). Категорія «Б»
Bulletin of Postgraduate education: collection of scientific papers. Series Social and Behavioral Sciences; Management and Administration. Issue 32(61). Category «B»
https://doi.org/10.58442/3041-1858-2025-32(61)

ПЕРЕКЛАД, ТРАНСЛІТЕРАЦІЯ / TRANSLATED AND TRANSLITERATED

[1] «Global Cybersecurity Outlook 2025», World Economic Forum. [Online]. Available: https://is.gd/w028PO Application date: February 05, 2025. (in English).

[2] «ENISA Threat Landscape 2024», European Union Agency for Cybersecurity, 2024. [Online]. Available: https://is.gd/r8HGDp Application date: February 05, 2025. (in English).

[3] «The Global Risks Report 2023. 18th Edition Insight Report», World Economic Forum, 2023. [Online]. Available: https://is.gd/rgaWeA Application date: February 05, 2025. (in English).

[4] G. Kambourakis, R. Neisse, and I. Nai-Fovino, «Information security in the age of EU Institutions digitalisation, a landscape analysis», European Commission, 2021. [Online]. Available: https://is.gd/D3zAuX Application date: February 05, 2025. (in English).

[5] C. Rupp, «Navigating the EU Cybersecurity Policy Ecosystem. A Comprehensive Overview of Legislation, Policies and Actors», Interface, 2024. [Online]. Available: https://is.gd/joj6yB Application date: February 05, 2025. (in English).

[6] V. Ahmadov, N. Klietsova, K. Bieliakov, A. Klochko, and T. Kravtsova, «Legal issues of information security of public authorities in Ukraine and the European Union: Experience and realities», AD ALTA: Journal of Interdisciplinary Research, vol. 11, is. 2, pp. 12–17, 2021. [Online]. Available: http://ep3.nuwm.edu.ua/id/eprint/21131 Application date: February 05, 2025. (in English).

[7] A. O. Krupnova, «pravove rehuliuvannia sfery zabezpechennia informatsiinoi bezpeky v Ukraini», Analitychno-porivnialne pravoznavstvo, № 5, s. 348–354, 2023. https://doi.org/10.24144/2788-6018.2023.05.62 (in Ukrainian).

[8] A. Marushchak, S. Petrov, M. Romanov, and O. Balashova, «The Problem of Legal Regulation of the Security of a Person, Society, State in the Formation of the Information Society in Ukraine», European Journal of Transformation Studies, vol. 9 No. 1, pp. 101–116, 2021. [Online]. Available: https://is.gd/ADJdq0 Application date: February 05, 2025. (in English).

[9] T. Yu. Tkachuk, Zabezpechennia informatsiinoi bezpeky v umovakh yevrointehratsii Ukrainy: pravovyi vymir. Kyiv, Ukraina : TOV «Vydav. dim «ArtEk», 2018. (in Ukrainian).

[10] M. Shevchuk, «Osoblyvosti pravovoho zabezpechennia informatsiinoi bezpeky z urakhuvanniam suchasnykh zahroz natsionalnii bezpetsi», Pravovyi chasopys Donbasu, № 1, s. 45–50, 2024. https://doi.org/10.32782/2523-4269-2024-86-45-50 (in Ukrainian).

[11] «Rekomendatsii dlia ukrainskykh orhaniv derzhavnoho upravlinnia shchodo nablyzhennia do prava YeS». Kyiv, Ukraina, 2018. [Elektronnyi resurs]. Dostupno: https://is.gd/7oAI34 Data zvernennia: Liut. 10, 2025. (in Ukrainian).

[12] H. Carrapico, and B. Farrand, «Cybersecurity Trends in the European Union: Regulatory Mercantilism and the Digitalisation of Geopolitics», *Journal of Common Market Studies*, vol. 62, is. S1, pp. 147–158, Sep. 2024. https://doi.org/10.1111/jcms.13654 (in English).

[13] «Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data», Official Journal of the European Union, L 281, pp. 31–50, October 23, 1995. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 Application date: February 05, 2025. (in English).

[14] «Council Resolution of 28 January 2002 on a common approach and specific actions in the area of network and information security», Official Journal of the European Union, C 43, pp. 2–4, February 16, 2002. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=oj:JOC_2002_043_R_0002_01 Application date: February 05, 2025. (in English).

[15] «Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace», European Commission, JOIN, 1 final, February, 7, 2013. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52013JC0001 Application date: February 05, 2025. (in English).

[16] «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, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)», Official Journal of the European Union, April 27, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng Application date: February 05, 2025. (in English).

[17] «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», Official Journal of the European Union, L 194, pp. 1–30, July 6, 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016L1148 Application date: February 05, 2025. (in English).

[18] «A new Strategic Agenda 2019–2024», European Council, June 20, 2019. [Online]. Available: https://www.consilium.europa.eu/en/press/press-releases/2019/06/20/a-new-strategic-agenda-2019-2024/ Application date: February 05, 2025. (in English).

[19] European Commission, «EU's Cybersecurity Strategy for the Digital Decade», Brussels, December 16, 2020. [Online]. Available: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 Application date: February 05, 2025. (in English).

[20] European Commission. (2022, September 15). Cyber Resilience Act «Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020». [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0454 (in English).

[21] «Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)», Official Journal of the European Union, L 333, pp. 80–152, December 14, 2022. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555 Application date: February 05, 2025. (in English).

[22] «Cyber Resilience Act», European Commission, 2024. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act Application date: February 05, 2025. (in English).

[23] I. K. Petroie, «Novitnia polityka informatsiinoi bezpeky v Yevropeiskomu Soiuzi: pravovyi aspekt», na II Vseukr. nauk.-prakt. konf. Teoretyko-prykladni aspekty rozvytku tsyfrovoi derzhavy v Ukraini. Kyiv, 2024, t. 30, s. 27–31. [Elektronnyi resurs]. Dostupno: https://duikt.edu.ua/uploads/p_2661_23355401.pdf Data zvernennia: Liut. 10, 2025. (in Ukrainian).

[24] «Information security – common rules for EU institutions, bodies and agencies», European Commission, 2020. [Online]. Available: https://is.gd/RU8YBE Application date: February 05, 2025. (in English).
[25] «Proposal for a Regulation of the European Parliament and of the Council on information security in the institutions, bodies, offices and agencies of the Union», *European Commission*, 2022. [Online]. Available: https://is.gd/uruEnL Application date: February 05, 2025. (in English).
[26] «Cybersecurity at the European Union institutions, bodies, offices and agencies», European Union, 2023. [Online]. Available: https://is.gd/kahbBR Application date: February 05, 2025. (in English).
[27] «European Network and Information Security Agency (ENISA)», European Union, March 10, 2004. [Online]. Available: https://is.gd/OxO8GW Application date: February 05, 2025. (in English).
[28] «2024 Report on the state of cybersecurity in the Union», European Union Agency for Cybersecurity, 2024. [Online]. Available: https://is.gd/9KKITH Application date: February 05, 2025. (in English).

Reviewed April 20, 2025
Published May 22, 2025