УДК 35-049.5:004](100)
DOI: https://doi.org/10.31470/2786-6246-2025-12-141-147

Стельмах Андрій, *кандидат наук з державного управління, викладач кафедри публічного управління та адміністрування Університету Григорія Сковороди в Переяславі*

Stelmakh Andriy, *Candidate of Science in Public Administration, Lecturer at the Department of Public Management and Administration at Hryhorii Skovoroda University in Pereiaslav*

ORCID ID: https://orcid.org/0000-0003-3721-5593

СУЧАСНІ АСПЕКТИ РОЗВИТКУ ЦИФРОВІЗАЦІЇ У СИСТЕМІ НАЦІОНАЛЬНОЇ БЕЗПЕКИ: ЗАКОРДОННИЙ ДОСВІД

MODERN ASPECTS OF DIGITALIZATION DEVELOPMENT IN THE NATIONAL SECURITY SYSTEM: FOREIGN EXPERIENCE

Анотація. У статті проаналізовані основні аспекти цифровізації національної безпеки за кордоном. Аналіз закордонного досвіду, зокрема таких країн, як США, Велика Британія, Ізраїль, Канада, Австралія, країни ЄС та Балтії, показує, що основою ефективної цифрової безпеки є стратегічна координація між державним та приватним секторами, розвиток технологічної інфраструктури, нормативна адаптивність та підвищення цифрової грамотності всіх учасників безпекового середовища.

Запропоновані основні аспекти запровадження світового досвіду щодо цифровізації національної безпеки в Україні. Зазначено, що імплементація закордонного досвіду має спиратися на кілька ключових напрямів: по-перше, розробка Національної стратегії цифрової безпеки з урахуванням ризиків кібервійни, гібридних загроз та інформаційних атак; по-друге, масштабна цифровізація сектору безпеки та оборони, включаючи побудову центрів кібероперацій, розгортання хмарних рішень на захищених серверах, використання автоматизованих систем моніторингу; по-третє, створення кіберрезерву – мережі цивільних фахівців, здатних долучатися до протидії атакам; по-четверте, інтеграція українських структур у міжнародні платформи співпраці в галузі кібербезпеки (ENISA, CISA, NCSC тощо); по-п'яте, розвиток освіти та цифрової грамотності, у тому числі для службовців сектору безпеки, з акцентом на практичні навички та адаптивні цифрові компетенції; по-шосте, забезпечення технологічного суверенітету, зокрема шляхом підтримки вітчизняних IT-рішень, локалізації критичних даних та зменшення залежності від зовнішніх цифрових платформ.

Зазначено, що цифровізація системи національної безпеки України має стати пріоритетом державної політики, спрямованим не лише на зміцнення обороноздатності, але й на побудову стійкої, адаптивної, інноваційної моделі управління безпековими ризиками в умовах сучасного світу. Імплементація перевірених міжнародних практик з одночасним урахуванням українських реалій здатна суттєво підвищити ефективність державної реакції на сучасні загрози.

Ключові слова: національна безпека, цифровізація національної безпеки, інформаційна безпека, кібербезпека, інституційні механізми цифровізації національної безпеки, гібридні загрози, інформаційні загрози.

Abstract. The article analyzes the main aspects of the digitalization of national security abroad. An analysis of foreign experience – in particular, of countries such as the USA, Great Britain, Israel, Canada, Australia, the EU and the Baltic countries – shows that the basis of effective digital security is strategic coordination between the public and private sectors, the development of technological infrastructure, regulatory adaptability and increasing the digital literacy of all participants in the security environment.

The author proposes the main aspects of implementing world experience in the digitalization of national security in Ukraine. It is noted that the implementation of foreign experience should be based on several key areas: first, the development of a National Digital Security Strategy taking into account the risks of cyberwar, hybrid threats and information attacks; second, large-scale digitalization of the security and defense sector, including the construction of cyber operations centers, the deployment of cloud solutions on secure servers, and the use of automated monitoring systems; third, the creation of a cyber reserve – a network of civilian specialists capable of participating in countering attacks; fourth, the integration of Ukrainian structures into international cooperation platforms in the field of cybersecurity (ENISA, CISA, NCSC, etc.); fifth, the development of education and digital literacy, including for security sector employees, with an emphasis on practical skills and adaptive digital competencies; sixth, ensuring technological sovereignty, in particular by supporting domestic IT solutions, localizing critical data, and reducing dependence on external digital platforms.

The digitalization of Ukraine's national security system should become a priority of state policy, aimed not only at strengthening defense capabilities, but also at building a sustainable, adaptive, innovative model of security risk management in the modern world. The implementation of proven international practices while taking into account Ukrainian realities can significantly increase the effectiveness of the state's response to modern threats.

Keywords: national security, digitalization of national security, information security, cybersecurity, institutional mechanisms for digitalization of national security, hybrid threats, information threats.

Постановка проблеми. Актуальність дослідження сучасних аспектів розвитку цифровізації у системі національної безпеки зумовлена глибокими трансформаціями безпекового середовища, що відбуваються у світі під впливом інформаційно-комунікаційних технологій. У XXI ст. цифрові загрози стають не менш серйозними, ніж традиційні військові виклики. Кібератаки, інформаційні війни, маніпуляції у соціальних мережах, технології штучного інтелекту – усе це є інструментами новітніх конфліктів, до яких держави змушені адаптувати свої системи безпеки. Саме тому цифровізація національної безпеки є не лише питанням інноваційного розвитку, а й фактором державної стійкості та виживання.

Актуальність цього напряму вивчення зростає і для України, яка фактично перебуває в умовах гібридної війни. Для держави надзвичайно важливо не лише переймати міжнародний досвід, а й формувати власну модель цифрової безпеки, адаптовану до унікального спектру викликів – від кібератак і пропагандистських кампаній до захисту критичної інфраструктури та цифрових реєстрів у період воєнного стану.

Аналіз останніх досліджень і публікацій. Певні аспекти цифровізації публічного управління, публічної служби, економічних процесів, сфер життєдіяльності суспільства аналізують багато науковців. Водночас, у контексті національної безпеки є предметом дослідження деяких науковців, зокрема: Ю. Завгородня, Л. Кормич, Т. Краснопольська, О. Мазурук, В. Новіков, Н. Новікова, Я. Самусевич, Г. Ситник, М. Ткач, Т. Яровой та ін.

Метою статті є обґрунтування імплементації світового досвіду щодо розвитку цифровізації у системі національної безпеки в сучасну національну безпеку України.

Виклад основного матеріалу. Закордонний досвід переконливо свідчить про те, що найбільш успішні у протидії гібридним загрозам держави активно інвестують у цифрові рішення для безпеки. У США одним із ключових органів, що здійснює управління в сфері цифрової безпеки, є Агентство з кібербезпеки та безпеки інфраструктури (Cybersecurity and Infrastructure Security Agency – CISA) [1], яке функціонує в структурі Міністерства внутрішньої безпеки (Department of Homeland Security). Створене у 2018 р., CISA відіграє центральну роль у забезпеченні національної стійкості до цифрових загроз, особливо у сфері критично важливої інфраструктури, що охоплює енергетичний сектор, транспорт, фінансову систему, медичні заклади, водопостачання, телекомунікації, державне управління та інші об’єкти, від яких залежить життєдіяльність суспільства.

Одна з основних функцій CISA [1] – координація діяльності федеральних, регіональних та місцевих органів влади, а також приватних компаній у запобіганні, виявленні та реагуванні на кіберзагрози. Агентство здійснює безперервний моніторинг кіберпростору через спеціалізовані платформи раннього попередження, які аналізують мільйони подій у режимі реального часу, використовуючи штучний інтелект, алгоритми машинного навчання та аналітику великих даних. Такі системи дозволяють своєчасно виявляти кібератаки, фішингові кампанії, витоки даних та інші інциденти, що можуть загрожувати національній безпеці.

CISA також реалізує ініціативу «Shield Up!» [1], що спрямована на підвищення рівня готовності організацій до кіберінцидентів. У межах цієї програми надаються рекомендації, методичні матеріали, інструкції щодо кібергігієни, інструменти для оцінки ризиків і вразливостей систем. Агентство виступає посередником між державою і приватним сектором, створюючи партнерства з технологічними компаніями, операторами критичної інфраструктури, банками та освітніми установами. Такий формат співпраці ґрунтується на обміні інформацією про кіберзагрози, спільному моделюванні сценаріїв атак, проведенні тренувань і симуляцій.

Особливе значення має підхід CISA до кібербезпеки як до питання загальнонаціональної безпеки, що охоплює не лише технологічний аспект, а й людський фактор [1]. Агентство проводить освітні кампанії серед громадян і службовців, розвиває систему підвищення цифрової грамотності та надає технічну підтримку організаціям, які не мають достатніх власних ресурсів для забезпечення кіберзахисту.

Окрему увагу CISA приділяє забезпеченню безпеки виборчого процесу, захисту державних реєстрів, урядових вебресурсів, а також реагуванню на масштабні загрози, наприклад, кібератаки з боку держав-противників або транснаціональних хакерських угруповань [1]. Для цього агентство співпрацює з Федеральним бюро розслідувань (FBI), Агентством національної безпеки (NSA), а також міжнародними партнерами в рамках обміну досвідом та оперативними даними.

Таким чином, діяльність CISA у США є прикладом комплексного та багаторівневого підходу до цифрової безпеки, який поєднує сучасні технології, міжвідомчу та міжсекторальну співпрацю, стратегічне планування та відкритість до інновацій. Цей досвід демонструє, як системна цифровізація безпекових механізмів може суттєво підвищити захищеність держави в умовах динамічного технологічного середовища та глобальних кіберзагроз.

У Європейському Союзі ключовим інституційним органом, відповідальним за координацію політик у сфері цифрової безпеки, є Європейське агентство з кібербезпеки (ENISA) – European Union Agency for Cybersecurity [2]. Створене у 2004 р., агентство посідає центральне місце у зміцненні кіберстійкості ЄС, формуванні спільного безпекового простору в цифровій сфері та сприянні імплементації політик з кібербезпеки в країнах-членах.

ENISA виконує низку критично важливих функцій. Зокрема, воно забезпечує методологічну підтримку урядам країн ЄС у розробці та реалізації національних стратегій цифрової безпеки, проводить аудити кіберстійкості цифрових систем, аналізує ризики та загрози, бере участь у розслідуванні кіберінцидентів і координує транскордонну взаємодію між органами влади, приватними компаніями та структурами критичної інфраструктури. Агентство також організовує масштабні навчання – такі як Cyber Europe – в яких беруть участь сотні установ, що імітують реагування на масштабні кібератаки [2].

ENISA тісно співпрацює з Європейською комісією, Європейською службою зовнішніх дій, національними центрами реагування на інциденти кібербезпеки (CSIRT) та іншими структурами, щоб забезпечити єдині стандарти безпеки, спільні механізми моніторингу загроз і оперативне реагування на них [2]. У 2019 р. ЄС затвердив Регламент про кібербезпеку, який значно розширив мандат ENISA і закріпив за агентством координуючу роль у створенні Європейської рамки сертифікації кібербезпеки (EU Cybersecurity Certification Framework).

Особливу увагу в політиці кібербезпеки ЄС приділено концепції «цифрового суверенітету» [3]. Вона передбачає прагнення держав-членів до збереження контролю над національними цифровими ресурсами, зокрема, над персональними даними громадян, критично важливою

інфраструктурою, державними сервісами та стратегічними технологіями. У межах цієї концепції активно розвивається ініціатива GAIA-X, яка має на меті створення європейської федеративної хмарної інфраструктури, незалежної від глобальних гігантів, таких як Amazon, Google чи Microsoft.

Стратегічна мета ЄС полягає не лише в захисті від зовнішніх загроз, а й у підвищенні автономності в розробці та використанні цифрових технологій [4]. Цей підхід включає підтримку європейських інноваційних екосистем, стартапів і компаній, що працюють у сфері штучного інтелекту, IoT, хмарних обчислень, блокчейну та інших критичних напрямів цифрової трансформації. Програми Horizon Europe, Digital Europe Programme, European Defence Fund передбачають мільярдні інвестиції у розвиток таких технологій з урахуванням високих стандартів кібербезпеки.

Крім того, ENISA [3] реалізує широку просвітницьку діяльність, спрямовану на підвищення обізнаності громадян, службовців і бізнесу у питаннях цифрової гігієни, кіберзахисту, відповідального використання даних. Усі ці заходи мають на меті формування культури кібербезпеки як невід'ємного елементу європейської безпекової політики та економічної самостійності.

Проведений аналіз дає підстави зазначити, що цифрова безпека в Європейському Союзі є складовою ширшого стратегічного бачення – захисту демократії, економіки та суверенітету у цифрову епоху. ENISA та національні органи з кібербезпеки виступають гарантом реалізації цього курсу, орієнтуючись на прозорість, довіру, інновації та солідарність між державами-членами.

У країнах Балтії, зокрема в Естонії, цифровізація системи національної безпеки стала ключовим чинником підвищення стійкості держави до зовнішніх загроз і гібридних викликів. Естонія, яка ще з початку 2000-х рр. активно інвестувала у створення електронної держави (e-Estonia), стала одним із перших у світі прикладів інтегрованого підходу до цифрового урядування та безпеки [5]. Сучасні технології пронизують усі рівні функціонування держави – від обміну даними між відомствами до участі громадян у виборах онлайн, а кібербезпека розглядається як складова національної оборонної доктрини.

Одним із важливих елементів цієї системи є електронне управління в умовах криз, яке дозволяє органам влади швидко ухвалювати рішення, координувати дії між структурами, вести документообіг у цифровому форматі та забезпечувати безперервність державного управління навіть у разі кіберінцидентів або фізичної дестабілізації [6]. Централізована інфраструктура даних, заснована на платформі X-Road, дозволяє безпечно обмінюватися інформацією між державними установами та реагувати на надзвичайні ситуації в режимі реального часу.

Окрему роль відіграє створення так званого «кіберрезерву» – мережі добровольців і професійних фахівців з IT-сфери, які можуть бути оперативно мобілізовані у випадку загроз національній кібербезпеці. Цей механізм функціонує за підтримки Кібероборони Естонії (Estonian Defence League's Cyber Unit [7]), що є частиною сил територіальної оборони. До кіберрезерву входять програмісти, аналітики, інженери, які діють у тісній співпраці з урядовими структурами, Службою інформації та безпеки Естонії (KAPO), а також міжнародними партнерами по НАТО.

Населення Естонії демонструє високий рівень цифрової грамотності, що є результатом довготривалої освітньої політики, орієнтованої на впровадження IT у шкільну та університетську підготовку, а також національних кампаній з підвищення обізнаності про кіберризики. Це дозволяє не лише зменшити кількість кіберінцидентів, пов'язаних з людським фактором, але й підвищити готовність суспільства до участі в забезпеченні цифрової безпеки країни.

Інтеграція великих баз даних, інтелектуальний аналіз ризиків і автоматизоване виявлення загроз стали невід'ємною частиною роботи силових і безпекових структур. Естонські установи використовують алгоритми машинного навчання та штучного інтелекту для аналізу аномальної активності в інформаційних системах, прогнозування потенційних атак, а також для забезпечення безпеки державних сервісів, включаючи охорону персональних даних, фінансових транзакцій, е-охорони здоров'я та е-правосуддя.

Важливою складовою безпекової політики є тісна інтеграція Естонії в євроатлантичні безпекові структури, включаючи співпрацю з НАТО Cooperative Cyber Defence Centre of Excellence (CCDCOE) [8], що розташований у Таллінні. Цей центр є провідним міжнародним осередком досліджень та навчання в галузі кібероборони.

Досвід Естонії демонструє, що цифрова трансформація системи національної безпеки може бути не лише інструментом технічного оновлення, але й основою для створення нової філософії оборони – відкритої, гнучкої, технологічної та орієнтованої на активну участь суспільства.

Особливу увагу цифровізації системи національної безпеки приділяють такі високотехнологічні держави, як Ізраїль, Велика Британія, Канада та Австралія. Ці країни демонструють комплексний підхід до впровадження цифрових інновацій у сферу безпеки, поєднуючи технологічний розвиток з нормативно-правовим регулюванням, міжнародною кооперацією та системною модернізацією державних інституцій. Одним із ключових напрямів є інтеграція передових технологій, зокрема, predictive analytics (аналітики на основі прогнозування), blockchain, квантового шифрування (quantum encryption), систем штучного інтелекту та машинного навчання.

В Ізраїлі цифрова безпека – це частина національної стратегії виживання, враховуючи складне геополітичне положення держави. Основний акцент робиться на проактивному виявленні загроз через системи прогнозної аналітики, що базуються на великих обсягах даних. Ці системи дозволяють виявляти підозрілу активність задовго до того, як вона переросте у повномасштабний інцидент. Ізраїль також є одним із лідерів у використанні блокчейн-технологій для захисту урядових баз даних, що забезпечує децентралізований контроль, прозорість доступу до інформації та підвищену стійкість до кібервтручання. Крім того, в країні активно розвиваються інструменти кібервоєнної стратегії – як оборонні, так і наступальні – у рамках діяльності таких підрозділів, як Unit 8200 [9].

У Великій Британії діє Національний центр кібербезпеки (NCSC) [10], який виступає основною структурою, що координує зусилля уряду, приватного сектору та наукової спільноти у сфері цифрової безпеки. У рамках проєктів з кіберстійкості активно впроваджуються технології квантового шифрування, що забезпечують захист каналів зв'язку від перехоплення та декодування в умовах розвитку квантових обчислювальних потужностей. Британські урядові структури також експериментують із використанням predictive analytics у протидії тероризму та кіберзлочинності, де моделі машинного навчання використовуються для аналізу поведінкових шаблонів, виявлення ризиків у цифровому середовищі та моделювання сценаріїв реагування.

У Канаді цифрова безпека органічно поєднується з концепцією публічної прозорості та захисту прав громадян, що створює виклик для балансування між ефективністю та етикою. Уряд Канади інвестує значні ресурси у створення інфраструктури даних на базі blockchain для захисту ідентичності, ведення державного реєстру та забезпечення незмінності інформації. Також реалізуються проєкти у сфері штучного інтелекту для виявлення фейкових новин, пропаганди та дезінформації, що особливо актуально в умовах гібридних загроз. Стратегія «Canada's National Cyber Security Strategy» [11] включає елементи співпраці із приватним сектором, розвиток науково-дослідних центрів і підготовку кадрів нового покоління.

В Австралії цифрова трансформація системи національної безпеки реалізується через Australian Signals Directorate (ASD) [12], яке відіграє провідну роль у розробці інструментів цифрової оборони. Країна інтенсивно впроваджує кіберрозвідку, побудовану на принципах прогнозного моделювання, аналізу кіберповедінки та оцінювання вразливостей цифрової інфраструктури. Австралійський уряд інвестує в національні дослідницькі програми у сфері квантових технологій, зокрема створення центрів квантового шифрування для захисту державної інформації від майбутніх загроз з боку суперкомп'ютерів. Значна увага приділяється міжнародній співпраці, зокрема в рамках Five Eyes – альянсу розвідслужб, що включає також США, Великобританію, Канаду та Нову Зеландію.

Таким чином, досвід цих країн свідчить про перехід до нової парадигми цифрової безпеки, де ключовими стають не лише реактивні, а й проактивні методи. Інтеграція новітніх технологій, посилення партнерства між державою та бізнесом, розвиток людського капіталу й постійне оновлення нормативно-правової бази є основою ефективної кіберполітики в умовах нової технологічної реальності. Україна може використати ці підходи для формування власної цифрової стратегії в системі національної безпеки.

Висновки. Сучасні аспекти розвитку цифровізації у системі національної безпеки свідчать про стрімку трансформацію традиційних підходів до забезпечення безпеки, яка базується на використанні інноваційних цифрових технологій, таких як штучний інтелект, прогнозна аналітика, квантове шифрування, blockchain та інтеграція великих даних. Аналіз зарубіжного досвіду, зокрема, таких країн, як США, Велика Британія, Ізраїль, Канада, Австралія, країни ЄС та Балтії показує, що основою ефективної цифрової безпеки є стратегічна координація між державним та приватним секторами, розвиток технологічної інфраструктури, нормативна адаптивність та підвищення цифрової грамотності всіх учасників безпекового середовища.

У США, ЄС та країнах Балтії запроваджено розвинені моделі цифрової кібероборони, які базуються на проактивному виявленні загроз, захисті критичної інфраструктури та побудові кіберрезервів. Велика Британія та Ізраїль демонструють передові приклади використання штучного інтелекту та технологій прогнозування для запобігання інцидентам. Канада та Австралія фокусуються на етичному використанні цифрових інструментів, кіберрозвідці та підвищенні кіберстійкості систем державного управління.

Для України впровадження цих підходів має критичне значення з огляду на триваючу військову агресію та необхідність забезпечення функціонування ключових інституцій у цифровому форматі. Імплементація закордонного досвіду має спиратися на кілька ключових напрямів: по-перше, розробка Національної стратегії цифрової безпеки з урахуванням ризиків кібервійни, гібридних загроз та інформаційних атак; по-друге, масштабна цифровізація сектору безпеки та оборони, включаючи побудову центрів кібероперацій, розгортання хмарних рішень на захищених серверах, використання автоматизованих систем моніторингу; по-третє, створення кіберрезерву – мережі цивільних фахівців, здатних долучатися до протидії атакам; по-четверте, інтеграція українських структур у міжнародні платформи співпраці в галузі кібербезпеки (ENISA, CISA, NCSC тощо); по-п'яте, розвиток освіти та цифрової грамотності, у тому числі для службовців сектору безпеки, з акцентом на практичні навички та адаптивні цифрові компетенції; по-шосте, забезпечення технологічного суверенітету, зокрема шляхом підтримки вітчизняних IT-рішень, локалізації критичних даних та зменшення залежності від зовнішніх цифрових платформ.

У підсумку, цифровізація системи національної безпеки України має стати пріоритетом державної політики, спрямованим не лише на зміцнення обороноздатності, але й на побудову стійкої, адаптивної, інноваційної моделі управління безпековими ризиками в умовах сучасного світу. Імплементація перевірених міжнародних практик з одночасним урахуванням українських реалій здатна суттєво підвищити ефективність державної реакції на сучасні загрози.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Cybersecurity and Infrastructure Security Agency. URL: https://www.cisa.gov/ (дата звернення: 24.03.2025).
2. European Union Agency for Cybersecurity (ENISA). URL: https://www.enisa.europa.eu/ (дата звернення: 24.03.2025).
3. Christakis T. (2020). European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence/ Grenoble Alpes Data Institute. URL: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098 (дата звернення: 24.03.2025).
4. Crespi, F., Caravellla, S., Menghini, M., Salvatori, Ch. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. Intereconomics. *Review of European Economic Policy*,

56(6), p. 348–354. URL: https://www.econstor.eu/bit-stream/10419/247773/1/10.1007_s10272-021-1013-6.pdf (дата звернення: 24.03.2025).
5. e-Estonia. URL: https://e-estonia.com/ (дата звернення: 24.03.2025).
6. Case study e-Estonia: digital society & open data. URL: https://urbact.eu/sites/default/files/2024-07/E-Estonia%20Case%20Study.pdf (дата звернення: 24.03.2025).
7. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. URL: https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/ (дата звернення: 24.03.2025).
8. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. URL: https://ccdcoe.org/ (дата звернення: 24.03.2025).
9. Unit 8200: Israel's Information Warfare Unit. URL: https://greydynamics.com/unit-8200-israels-information-warfare-unit/ (дата звернення: 24.03.2025).
10. The National Cyber Security Centre(NCSC). URL: https://www.ncsc.gov.uk/ (дата звернення: 24.03.2025).
11. Canada's National Cyber Security Strategy. URL: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx (дата звернення: 24.03.2025).
12. Australian Signals Directorate (ASD)**.** URL: https://www.asd.gov.au/ (дата звернення: 24.03.2025).

REFERENCES

1. Cybersecurity and Infrastructure Security Agency. *www.cisa.gov.* Retrieved from https://www.cisa.gov/ [in English].
2. European Union Agency for Cybersecurity **(ENISA). *www.enisa.europa.eu*.** Retrieved from https://www.enisa.europa.eu/ [in English].
3. Christakis, T. (2020). European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy. Multidisciplinary Institute on Artificial Intelligence/ Grenoble Alpes Data Institute. *papers.ssrn.com.* Retrieved from https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3748098 [in English].
4. Crespi, F., Caravellla, S., Menghini, M., & Salvatori, Ch. (2021). European Technological Sovereignty: An Emerging Framework for Policy Strategy. Intereconomics. *Review of European Economic Policy*, *56(6),* 348–354. Retrieved from https://www.econstor.eu/bit-stream/10419/247773/1/10.1007_s10272-021-1013-6.pdf [in English].
5. e-Estonia. *e-estonia.com*. Retrieved from https://e-estonia.com/ [in English].
6. Case study e-Estonia: digital society & open data. *urbact.eu.* Retrieved from https://urbact.eu/sites/default/files/2024-07/E-Estonia%20Case%20Study.pdf [in English].
7. The Cyber Defence Unit of the Estonian Defence League: Legal, Policy and Organisational Analysis. *ccdcoe.org.* Retrieved from https://ccdcoe.org/library/publications/the-cyber-defence-unit-of-the-estonian-defence-league-legal-policy-and-organisational-analysis/ [in English].
8. The NATO Cooperative Cyber Defence Centre of Excellence is a multinational and interdisciplinary cyber defence hub. *ccdcoe.org.* Retrieved from https://ccdcoe.org/ [in English].
9. Unit 8200: Israel's Information Warfare Unit. *greydynamics.com.* Retrieved from https://greydynamics.com/unit-8200-israels-information-warfare-unit/ [in English].
10. The National Cyber Security Centre(NCSC). *www.ncsc.gov.uk.* Retrieved from https://www.ncsc.gov.uk/ [in English].
11. Canada's National Cyber Security Strategy. *www.publicsafety.gc.ca.* Retrieved from https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/ntnl-cbr-scrt-strtg-2025/index-en.aspx [in English].
12. Australian Signals Directorate (ASD). *www.asd.gov.au***.** Retrieved from https://www.asd.gov.au/ [in English].

Подано до редакції 24.03.25 р.
Прийнято до друку 25.04.25 р.