

Логвиненко С. В.

<https://orcid.org/0009-0000-9186-4944>

Київський національний університет імені Тараса Шевченка

ЦИФРОВІ ПЛАТФОРМИ В СИСТЕМІ ЕКОНОМІЧНОЇ БЕЗПЕКИ: ФУНКЦІОНАЛЬНА КЛАСИФІКАЦІЯ ІНСТРУМЕНТІВ ТА ДОСВІД ЄС І США

Стаття присвячена порівняльному аналізу цифрових технологічних архітектур механізмів реагування Європейського Союзу (ЄС) і Сполучених Штатів Америки (США) на глобальні загрози в економічній сфері. Встановлено, що технологічна архітектура є невід'ємним контуром будь-якої сучасної системи реагування, без якого нормативно-правова рамка залишається функціонально неповноцінною. Проаналізовано ключові технологічні платформи європейської архітектури: Агентство ЄС з кібербезпеки (European Union Agency for Cybersecurity, ENISA), Гельсінський центр передового досвіду з питань гібридних загроз (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE), цифрова платформа скринінгу прямих іноземних інвестицій (ППІ), Єдиний консолідований санкційний список ЄС, Регламент про штучний інтелект (AI Act) 2024/1689. Виявлено три структурні характеристики європейської технологічної архітектури: спеціалізована платформізація, нормативна впорядкованість і захисна орієнтованість. Досліджено американські технологічні платформи: Мережа з протидії фінансовим злочинам (FinCEN), Об'єднана міжвідомча кіберслідча група (National Cyber Investigative Joint Task Force, NCJTF), Агентство з кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA), систему автоматизованого санкційного скринінгу Управління з контролю за іноземними активами (Office of Foreign Assets Control, OFAC) і Основи управління ризиками штучного інтелекту (AI RMF) Національного інституту стандартів і технологій (National Institute of Standards and Technology, NIST). Запропоновано авторську функціональну класифікацію цифрових інструментів механізмів реагування за п'ятьма категоріями: інструменти моніторингу, аналізу, підтримки прийняття рішень, імплементації та адаптації. Виявлено спільний патерн обох систем: інструменти моніторингу і аналізу є найбільш розвиненими, тоді як інструменти адаптації залишаються найбільш фрагментованими. Встановлено три структурних відмінності між моделями: архітектура даних, регуляторна філософія щодо автоматизованих рішень, механізми технологічного співробітництва. Визначено чотири ризики цифровізації без інституційної реформи і сформульовано п'ять принципів продуктивного технологічного розвитку безпекової функції, що є методологічним орієнтиром для формування технологічного компонента системи реагування України, що кореспондує з цілями Стратегії економічної безпеки України [3].

Ключові слова: цифрові технології; механізми державного реагування; глобальні загрози в економічній сфері; ENISA; FinCEN; CISA; штучний інтелект; AI Act; кібербезпека; FDI-скринінг; Україна.

Постановка проблеми. Нормативно-правова архітектура механізмів реагування, якими б досконалими не були її принципи і яким би розгалуженим не був її інституційний дизайн, потребує технологічного контуру для оперативної реалізації. Без систем збору і обробки даних, автоматизованого скринінгу, аналітичних платформ і інструментів підтримки рішень нормативна рамка залишається набором юридичних зобов'язань без

операційного наповнення. Цей технологічний вимір, довгий час недооцінюваний у порівняльному дослідженні систем економічної безпеки, набув стратегічного значення у контексті прискорення обороту загроз і масштабування їх транскордонного характеру [6; 16; 21].

Аналіз останніх досліджень і публікацій. Цифровий вимір механізмів реагування вивчається у кількох перетинних напрямках. Х. Карра-

піко і Б. Фарранд досліджують роль приватного сектора у формуванні кібербезпечових норм [10]. Е. Брав аналізує технологічні аспекти протидії сірозонним загрозам [11]. Т. Рюлінг досліджує технологічне суперництво ЄС і Китаю [25]. В. Маєр-Шьонбергер і Т. Рамге аналізують роль великих даних у трансформації регуляторних моделей [24]. Г. Кіссінджер, Е. Шмідт і Д. Гаттенлохер оцінюють стратегічні наслідки штучного інтелекту для систем безпеки [21]. У вітчизняній науці Г. Ситник [4] і В. Горбулін та А. Качинський [5] формують методологічний фундамент для аналізу управлінських механізмів. Важливим підґрунтям є і власний досвід автора у дослідженні цифрових технологій в системі управління економічною безпекою [6]. Попри значний масив публікацій, функціональна класифікація цифрових інструментів з порівняльним охопленням модей ЄС і США залишається недостатньо розробленою в науці публічного управління.

Постановка завдання. Мета статті полягає у порівняльному аналізі технологічних архітектур механізмів реагування ЄС і США на глобальні загрози в економічній сфері, розробці функціональної класифікації цифрових інструментів і формулюванні принципів їх адаптивного запозичення для реформування відповідної системи в Україні.

Виклад основного матеріалу. Технологічна архітектура ЄС. Європейська технологічна архітектура реагування на глобальні загрози в економічній сфері формувалась як паралельний контур до нормативно-правової рамки: якщо директиви і регламенти визначають, що є об'єктом регулювання, технологічні платформи визначають, як це регулювання реалізується. Агентство ЄС з кібербезпеки (European Union Agency for Cybersecurity, ENISA) у Афінах є ключовим цифровим хабом кібербезпекової архітектури. У межах Директиви NIS2 (Network and Information Security, NIS2) [8] ENISA веде єдину таксономію кіберінцидентів і координує мережу CSIRT (Computer Security Incident Response Teams) усіх держав-членів. Щорічний звіт ENISA про ландшафт кіберзагроз охоплює понад десять категорій загроз і слугує аналітичним підґрунтям для регуляторних ініціатив [13].

Гельсінський центр передового досвіду з питань гібридних загроз (European Centre of Excellence for Countering Hybrid Threats, Hybrid CoE) і Підрозділ з гібридного синтезу (EU Hybrid Fusion Cell) Служби зовнішніх зв'язків ЄС (European External Action Service, EEAS) становлять аналітичні платформи гібридного реагування.

Hybrid CoE, до якого входять 33 держави-члени і партнери з НАТО, виконує функцію синтезу аналітики, проведення навчань з гібридного реагування і підготовки рекомендацій для органів ЄС і держав-членів. Принципово важливим є те, що ці платформи є публічно-приватними: поряд з державними органами в їх аналітичному контурі задіяні університетські центри досліджень і технологічні компанії [10; 12].

Цифрова платформа скринінгу ПШ, що функціонує в межах Регламенту (ЄС) 2019/452 [7], забезпечує захищений обмін нотифікаціями між 27 державами-членами і Єврокомісією в режимі реального часу. Платформа стандартизує формат нотифікацій і дозволяє автоматично ідентифікувати транзакції, що підпадають під обов'язковий або добровільний розгляд. Станом на 2024 р. платформою проведено перевірку понад 1800 угод [12]. Єдина консолідована санкційна база даних ЄС (EU Consolidated List of Sanctioned Persons, Groups and Entities) надає доступ до актуальних санкційних списків для фінансових інституцій і регуляторів у форматі відкритих даних. Регламент (ЄС) 2024/1689 щодо штучного інтелекту (AI Act) [9] є першим у світі всеохопним регуляторним актом щодо ПШ-систем, що класифікує їх за рівнем ризику і встановлює жорсткі вимоги до систем, що використовуються в безпековій сфері.

Аналіз виявляє три структурні характеристики європейської технологічної архітектури. Перша: спеціалізована платформізація: кожен регуляторний інструмент отримує власну цифрову платформу з вузьким функціональним фокусом. Друга: нормативна впорядкованість: технологічні рішення розгортаються в межах і на виконання нормативно встановлених вимог, і впровадження нових цифрових інструментів завжди передувало або супроводжує нормативний акт. Третя: захисна орієнтованість: технологічний акцент є на захисті від загроз, а не на проєктному розширенні технологічних можливостей [10; 25].

Технологічна архітектура США. Американська технологічна архітектура формувалась у логіці, відмінній від європейської: США розгортали цифрові платформи до прийняття нормативних рамок або одночасно з ними, тоді як ЄС будував технологію слідом за правовою нормою. Мережа з протидії фінансовим злочинам Міністерства США (Financial Crimes Enforcement Network, FinCEN) є ключовою технологічною платформою фінансово-економічного моніторингу. Заснована у 1990 р., FinCEN веде найбільшу у світі базу даних повідомлень про підозрілі транзакції і застосовує машинне

навчання для ідентифікації патернів ухилення від санкцій та відмивання грошей. Річний звіт FinCEN за 2023 рік фіксує понад 3,6 млн повідомлень про підозрілу активність [15].

Об'єднана міжвідомча кіберслідча група (National Cyber Investigative Joint Task Force, NCIJTF), керована Федеральним бюро розслідувань (Federal Bureau of Investigation, FBI), координує діяльність понад тридцяти федеральних відомств і спецслужб у сфері кіберзагроз. Агентство з кібербезпеки та захисту інфраструктури (Cybersecurity and Infrastructure Security Agency, CISA) у складі Міністерства внутрішньої безпеки виконує функцію цифрового хабу захисту 16 секторів критичної інфраструктури. CISA веде систему збору повідомлень про кіберінциденти, забезпечує сканування мережевих уразливостей і підтримує Систему автоматизованого індикаторного обміну (Automated Indicator Sharing, AIS) між державними органами і операторами приватної критичної інфраструктури [14].

Система автоматизованого санкційного скринінгу Управління з контролю за іноземними активами (Office of Foreign Assets Control, OFAC) автоматично перевіряє контрагентів на відповідність актуальному Списку спеціально визначених суб'єктів і заблокованих осіб (Specially Designated Nationals and Blocked Persons, SDN List) у режимі реального часу. Технологічна інтеграція з базами даних Бюро з питань промисловості і безпеки (Bureau of Industry and Security, BIS) і Комітету зі скринінгу іноземних інвестицій (Committee on Foreign Investment in the United States, CFIUS) дозволяє OFAC застосовувати комплексний ризик-профіль при оцінці транзакцій [6; 17].

Національний інститут стандартів і технологій (National Institute of Standards and Technology, NIST) разом з Управлінням наукової і технологічної політики (Office of Science and Technology Policy, OSTP) при Президенті виконують функцію стандартизаційного регулятора в технологічній сфері. Основи управління ризиками штучного інтелекту (Artificial Intelligence Risk Management Framework, AI RMF 1.0) [18] є ключовим документом, що формує принципи відповідального використання ШІ в державному управлінні. Принципово важливою структурною характеристикою американської архітектури є інтегрованість систем агентств з масивами даних, що формуються в межах їх регуляторних мандатів: CFIUS має доступ до баз даних BIS, OFAC, Міністерства оборони, що дозволяє формувати комплексний ризик-профіль угоди замість вузького відомчого аналізу [6; 14].

Функціональна класифікація цифрових інструментів. Незважаючи на принципові архітектурні відмінності, аналіз виявляє конвергенцію: обидві системи застосовують цифрові інструменти для виконання одного і того ж обмеженого набору управлінських функцій. Пропонуємо класифікацію за п'ятьма категоріями. Перша: інструменти моніторингу: системи раннього попередження, автоматизовані тригери, моніторингові інтерфейси. Приклади: ENISA CSIRT Network (ЄС), CISA AIS та Система захищеного виявлення Einstein (США). Друга: інструменти аналізу: платформи синтезу даних, системи ШІ-аналітики, прогностичні моделі. Приклади: Hybrid CoE і EU Hybrid Fusion Cell (ЄС), FinCEN аналітика і NCIJTF (США). Третя: інструменти підтримки прийняття рішень: системи симуляції сценаріїв, інтерактивні дашборди, структуровані альтернативи. Четверта: інструменти імплементації: автоматизований compliance-моніторинг, цифрові санкційні реєстри, платформи ліцензування. Приклади: EU Consolidated Sanctions List і FDI Screening Platform (ЄС), OFAC automated screening і BIS Entity List (США). П'ята: інструменти адаптації: системи зворотного зв'язку, платформи інституційної пам'яті. Ця категорія є найбільш фрагментованою в обох системах [10; 19; 20].

Структурні відмінності між моделями. Перший вимір відмінностей: архітектура даних. Європейська модель опирається на принцип спеціалізованих платформ з обмеженими каналами міжплатформового обміну, що знижує ризик системних збоїв і витоку даних, але обмежує можливості інтегрованого аналізу. Американська модель характеризується значно ширшою міжагентською інтеграцією даних через системи розвідувальних архівів, що забезпечує глибший аналіз, але створює більші ризики системних збоїв і несанкціонованого доступу [6; 11]. Другий вимір: регуляторна філософія щодо автоматизованих рішень. Європейський AI Act [9] закріплює принцип людського нагляду (human oversight) над будь-якою ШІ-системою в безпековій сфері. Американський підхід за AI RMF NIST [18] є більш гнучким і спирається на принцип оцінки ризику, а не на категоричний обов'язок нагляду. Третій вимір: механізми технологічного співробітництва. ЄС організує його через Cyber Cooperation Group, CSIRT Network і спільні стресові тести в межах DORA (Regulation 2022/2554). США реалізують його через двосторонні угоди в межах Ради з торгівлі і технологій ЄС і США (EU-US Trade and Technology Council, TTC) [17; 23].

Практика спільного реагування і ризику цифровізації. Особливої аналітичної уваги заслуговує практика спільного реагування ЄС і США на гібридні загрози після 2022 р. Обидві системи оперативно скоординували санкційні переліки після повномасштабного вторгнення Росії в Україну, причому технологічне узгодження санкційних баз даних відбувалося паралельно з нормативним узгодженням переліків [12; 17]. Водночас цифровізація механізмів реагування несе чотири структурних ризику. Перший: перевантаження непрацюючих процесів: моніторингова система, що генерує сигнали без операційного носія реагування, стає джерелом аналітичного паралічу. Другий: нові вразливості через технологічну залежність: чим більш автоматизованою є система, тим руйнівнішою є потенційна недоступність інфраструктури внаслідок кібератаки. Третій: культура делегування рішень алгоритму з втратою управлінської відповідальності. Четвертий: структурна асиметрія між державою і технологічно розвиненим приватним сектором [22; 24].

Принципи продуктивної цифровізації для України. Зіставлення зарубіжного досвіду з українським контекстом виявляє різний рівень готовності за функціональними підсистемами. Технічна готовність у підсистемі моніторингу є середньою: інфраструктура «Трембіта» і «Дія» формують технологічний базис, але не покривають повного спектра потреб. У підсистемі аналізу готовність є середньо-високою: вітчизняний IT-сектор достатньо кваліфікований для розробки аналітичних ШІ-систем. У підсистемі імплементації готовність є найвищою: «Дія» і «Трембіта» забезпечують інфраструктуру для автоматизованого compliance-моніторингу і цифрових санкційних реєстрів. Методологічний висновок: технологія, не вбудована в інституційну реформу, перетворюється на самоціль, а не на засіб підвищення ефективності. Для України це означає пріоритет кількох принципів: 1) інституційне передування технологічному; 2) технологія слідує за функцією; 3) інтегральний підхід замість острівкової автоматизації; 4) кібербезпека як базова умова, а не опція; 5) публічно-приватне партнерство в аналітичному контурі [1; 2; 16; 20].

Роль штучного інтелекту у трансформації моніторингових систем. Спільна тенденція обох систем полягає в переході від ручної обробки сигналів загроз до автоматизованих платформ, що застосовують алгоритми машинного навчання. Ця тенденція є особливо виразною в підсистемі фінансового моніторингу: FinCEN у США і профільні

підрозділи Єврокомісії застосовують алгоритми виявлення аномалій у транзакційних масивах, що дозволяє ідентифікувати схеми ухилення від санкцій, невидимі при ручному аудиті. Впровадження AI Act [9] у ЄС створює нову регуляторну реальність: системи штучного інтелекту (ШІ), що беруть участь в ухваленні безпекових рішень, підпадають під категорію систем із високим ризиком і потребують спеціальних протоколів безпеки, документування і людського нагляду. США за основами управління ризиками ШІ (AI RMF) NIST [18] обрали більш гнучкий підхід: рамковий документ надає принципи, а не жорсткі вимоги. Обидва підходи є функціонально виправданими, але відображають принципово різні регуляторні філософії [21; 22].

EU-US TTC як механізм технологічної координації. Принципово новим елементом у порівняльній картині є механізм Ради з торгівлі і технологій (EU-US Trade and Technology Council, TTC), заснованої у 2021 р. Рада є першою формалізованою платформою технологічної координації між двома регуляторними архітектурами і включає десять робочих груп, три з яких безпосередньо пов'язані з технологіями безпеки. Спільна заява шостого міністерського засідання TTC у Лейвені 2024 р. [17] зафіксувала синхронізацію підходів до контролю над технологіями ШІ, квантовими технологіями і спільний список технологій подвійного використання. Для України, яка прагне членства в ЄС і підтримує стратегічне партнерство зі США, TTC є потенційною інституційною рамкою для участі в координації технологічних стандартів безпеки ще до повноправного членства [6; 19; 23].

Готовність України до цифрової трансформації безпекового управління. Українська система державного управління має диференційовану технологічну готовність до адаптації зарубіжних цифрових рішень. Розгортання таких платформ, як «Дія» і «Трембіта», засвідчує спроможність до масштабної цифровізації публічних послуг. Однак безпекова сфера потребує рішень іншого класу: не орієнтованих на зручність користувача, а критично залежних від захищеності, відмовостійкості і реального часу обробки. Адаптація підходів CISA до захисту критичної інфраструктури і ENISA до стандартизації кіберінцидентів є методологічно першочерговим завданням. У підсистемі імплементації наявна інфраструктура уже достатня для запровадження цифрових санкційних реєстрів і автоматизованого compliance-моніторингу. У підсистемах аналізу і адаптації потрібні цілеспрямовані інвестиції в людський капітал і нормативну

базу: технічна компетентність є, але регуляторних рамок для ШІ-асистованих аналітичних рішень у безпековій сфері ще немає [1; 2; 3; 16].

Висновки. Цифровий вимір є принциповою точкою конвергенції між ЄС і США, попри всі архітектурні відмінності. По-перше, обидві системи рухаються до дедалі ширшого використання штучного інтелекту і машинного навчання як інструментів аналітичної підтримки управлінських рішень, залишаючи за людиною функцію кінцевого вибору. По-друге, запропонована функціональна класифікація за п'ятьма категоріями (моні-

торинг, аналіз, рішення, імплементація, адаптація) є практичним діагностичним інструментом для оцінки технологічної зрілості будь-якої національної системи. По-третє, ключовим висновком для практики є визначення принципу інституційного передування: цифрова технологія є множителем ефективної системи реагування, але не заміником її відсутності. Перспективи подальших досліджень включають розробку методики оцінювання технологічної зрілості безпекових систем та аналіз практики технологічного партнерства в межах EU-US ТТС як механізму координації.

Список літератури:

1. Про національну безпеку України: Закон України від 21.06.2018 № 2469-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2469-19>
2. Про основні засади забезпечення кібербезпеки України: Закон України від 05.10.2017 № 2163-VIII. URL: <https://zakon.rada.gov.ua/laws/show/2163-19>
3. Про рішення Ради національної безпеки і оборони України «Про Стратегію економічної безпеки України»: Указ Президента України від 11.08.2021 № 347/2021. URL: <https://zakon.rada.gov.ua/laws/show/347/2021>
4. Ситник Г. П. Державне управління у сфері національної безпеки: підручник. Київ: НАДУ, 2012. 544 с.
5. Горбулін В. П., Качинський А. Б. Стратегічне планування: вирішення проблем національної безпеки. Київ: НІСД, 2010. 288 с.
6. Logvynenko S., Krivonosov L., Zhurba O., Kulin I., Pynda Yu. Digital Technologies in the System of State Economic Security Management. *Periodicals of Engineering and Natural Sciences*. 2026. Vol. 14. No. 1. P. 141–166. DOI: 10.21533/pen.v14.i1.1527
7. Regulation (EU) 2019/452 of the European Parliament and of the Council establishing a framework for the screening of foreign direct investments into the Union. *Official Journal of the European Union*. 2019. L 79I. P. 1–14.
8. Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). *Official Journal of the European Union*. 2022. L 333. P. 80–152.
9. Regulation (EU) 2024/1689 laying down harmonised rules on artificial intelligence (AI Act). *Official Journal of the European Union*. 2024. L series.
10. Carrapico H., Farrand B. Dialogue, Partnership and Empowerment for Network and Information Security: The Changing Role of the Private Sector. *Crime, Law and Social Change*. 2017. Vol. 67. No. 3. P. 245–263.
11. Braw E. The Defender's Dilemma: Identifying and Deterring Gray-Zone Aggression. Washington, D.C.: American Enterprise Institute, 2022. 156 p.
12. European Commission. Investment Screening: Annual Report 2023 on the Implementation of Regulation (EU) 2019/452. Brussels: DG TRADE, 2024. 62 p.
13. European Union Agency for Cybersecurity (ENISA). ENISA Threat Landscape 2024. Athens: ENISA, 2024. 156 p.
14. Cybersecurity and Infrastructure Security Agency (CISA). CISA Strategic Plan 2023–2025. Washington, D.C.: U.S. Department of Homeland Security, 2023. 36 p.
15. Financial Crimes Enforcement Network (FinCEN). FinCEN Year in Review for Fiscal Year 2023. Washington, D.C.: U.S. Department of the Treasury, 2024. 28 p.
16. World Economic Forum. The Global Risks Report 2025. 20th Edition. Geneva: World Economic Forum, 2025. 124 p.
17. EU–US Trade and Technology Council. Joint Statement of the Sixth Ministerial Meeting. Leuven, Belgium, 4–5 April 2024. Brussels–Washington, D.C., 2024. 18 p.
18. National Institute of Standards and Technology (NIST). Artificial Intelligence Risk Management Framework (AI RMF 1.0). NIST AI 100-1. Gaithersburg, MD: NIST, 2023. 48 p.
19. Chatham House. US–EU Strategic Alignment on Economic Security: Gaps and Opportunities. Research Paper. London: Royal Institute of International Affairs, 2023. 48 p.

20. Center for Strategic and International Studies (CSIS). Assessing the Economic Security Landscape: Benchmarks and Gaps. Washington, D.C.: CSIS, 2023. 64 p.
21. Kissinger H. A., Schmidt E., Huttenlocher D. The Age of AI and Our Human Future. New York: Little, Brown and Company, 2021. 272 p.
22. Brundage M., Avin S., Clark J., Toner H., Eckersley P. et al. The Malicious Use of Artificial Intelligence: Forecasting, Prevention, and Mitigation. Oxford: Future of Humanity Institute, 2018. 100 p.
23. Acharya P. Artificial Intelligence in National Security: Strategic Approaches. Journal of Strategic Security. 2023. Vol. 16. No. 2. P. 89–112.
24. Mayer-Schonberger V., Ramge T. Reinventing Capitalism in the Age of Big Data. New York: Basic Books, 2018. 256 p.
25. Ruhlig T. N. EU–China Tech Competition: How Europe Can Sharpen Its Approach. Policy Brief. Stockholm: Swedish Institute of International Affairs, 2023. 12 p.

**Logvynenko S. V. DIGITAL PLATFORMS IN THE ECONOMIC SECURITY SYSTEM:
FUNCTIONAL CLASSIFICATION OF INSTRUMENTS AND EU–US EXPERIENCE**

This article provides a comparative analysis of the digital technological architectures of European Union (EU) and United States (US) mechanisms for responding to global threats in the economic sphere. It is established that the technological architecture is an indispensable circuit of any modern response system, without which the regulatory framework remains functionally incomplete. The key technological platforms of the European architecture are analyzed: the European Union Agency for Cybersecurity (ENISA), the European Centre of Excellence for Countering Hybrid Threats (Hybrid CoE) in Helsinki, the digital Foreign Direct Investment (FDI) Screening Platform, the EU Consolidated Sanctions List, and the Artificial Intelligence Act (AI Act) Regulation 2024/1689. Three structural characteristics of the European technological architecture are identified: specialized platformization, regulatory orderliness, and defensive orientation. The key American technological platforms are examined: the Financial Crimes Enforcement Network (FinCEN), the National Cyber Investigative Joint Task Force (NCIJTF), the Cybersecurity and Infrastructure Security Agency (CISA), the Office of Foreign Assets Control (OFAC) automated sanctions screening system, and the National Institute of Standards and Technology (NIST) Artificial Intelligence Risk Management Framework (AI RMF). An original functional classification of digital instruments of response mechanisms is proposed, comprising five categories: monitoring tools, analysis tools, decision-support tools, implementation tools, and adaptation tools. A common pattern of both systems is identified: monitoring and analysis tools are most developed, while adaptation tools remain most fragmented. Three structural differences between the models are established: data architecture, regulatory philosophy regarding automated decisions, and mechanisms of technological cooperation. Four risks of digitalization without institutional reform are identified, and five principles of productive technological development of the security function are formulated.

Keywords: digital technologies; state response mechanisms; global threats in the economic sphere; ENISA; FinCEN; CISA; artificial intelligence; AI Act; cybersecurity; FDI screening; Ukraine.

Дата першого надходження статті до видання: 09.07.2026

Дата прийняття статті до друку після рецензування: 24.07.2026

Дата публікації (оприлюднення) статті: 15.10.2026