

УДК 347.73:342.9:342.7:004.056

DOI <https://doi.org/10.24144/2788-6018.2024.04.47>

ЗАХИСТ ЦИФРОВОЇ ІНФРАСТРУКТУРИ У МИТНО-АДМІНІСТРАТИВНИХ ПОСЛУГАХ: ВИКЛИКИ ТА СУЧАСНІ ПІДХОДИ ДО КІБЕРБЕЗПЕКИ

Біленець Д.А.,*кандидат юридичних наук, доцент,**доцент кафедри цивільно-правових дисциплін**Чернівецького навчально-наукового юридичного інституту**НУ «Одеська юридична академія»**ORCID: 0000-0003-0866-0698*

Біленець Д.А. Захист цифрової інфраструктури у митно-адміністративних послугах: виклики та сучасні підходи до кібербезпеки.

У сучасному світі цифрові технології проникають у всі сфери життя, і митно-адміністративні послуги не є винятком. Розвиток цифрових інфраструктур у цій галузі сприяє підвищенню ефективності, прозорості та швидкості обробки митних операцій. Цифровізація охоплює впровадження сучасних технологій та рішень, які дозволяють автоматизувати та оптимізувати багато аспектів роботи митних органів, що в свою чергу позитивно впливає на весь процес митного контролю та обслуговування. Одним з основних напрямів цифровізації є автоматизація процесів обробки митних документів. Використання електронних систем декларування значно скорочує час, необхідний для перевірки та обробки документів, що дозволяє швидше оформлювати вантажі та знижує ризик помилок, пов'язаних з людським фактором.

Одним з ключових аспектів забезпечення кібербезпеки в митно-адміністративній сфері є впровадження сучасних систем захисту даних. Це включає в себе використання надійного шифрування, багаторівневих систем аутентифікації та регулярний моніторинг мереж на наявність потенційних загроз. Також важливою є розробка та впровадження протоколів реагування на інциденти, що дозволяють швидко і ефективно нейтралізувати кіберзагрози та мінімізувати їх вплив на роботу митних органів.

Крім того, велике значення має підвищення обізнаності працівників митних органів щодо основних принципів кібербезпеки. Регулярні тренінги та навчання допомагають працівникам вчасно виявляти ознаки можливих кібератак та дотримуватися заходів безпеки при роботі з інформаційними системами. Важливою складовою є також співпраця з міжнародними організаціями та обмін досвідом з іншими країнами, які впроваджують передові практики в галузі кібербезпеки.

Розвиток цифрових технологій не лише підвищує ризики, але й відкриває нові можливості для оптимізації митних процесів. Впровадження систем штучного інтелекту може допомогти у виявленні потенційних, використання блокчейн-технологій забезпечує більшу прозорість та надійність ланцюжків постачання, що сприяє запобіганню шахрайству та підвищенню довіри між учасниками зовнішньоекономічної діяльності.

Ключові слова: митниця, цифровізація, кібербезпека, цифрова інфраструктура, митні послуги, адміністративні послуги, митні документи, митне оформлення.

Bilenets D. Protection of digital infrastructure in customs-administrative services: challenges and modern approaches to cybersecurity.

In the modern world, digital technologies penetrate all spheres of life, and customs-administrative services are no exception. The development of digital infrastructures in this field contributes to increasing the efficiency, transparency, and speed of customs operations. Digitalization encompasses the implementation of modern technologies and solutions that allow for the automation and optimization of many aspects of customs authorities' work, which in turn positively impacts the entire customs control and service process. One of the main directions of digitalization is the automation of customs document processing. The use of electronic declaration systems significantly reduces the time required for document verification and processing, enabling faster clearance of goods and reducing the risk of errors related to human factors.

One of the key aspects of ensuring cybersecurity in the customs-administrative sphere is the implementation of modern data protection systems. This includes the use of reliable encryption, multi-level authentication systems, and regular network monitoring for potential threats. The development

and implementation of incident response protocols are also important, as they allow for quick and effective neutralization of cyber threats and minimization of their impact on the operation of customs authorities.

In addition, raising the awareness of customs officials about the basic principles of cybersecurity is of great importance. Regular training and education help employees timely identify signs of possible cyber-attacks and adhere to security measures when working with information systems. An essential component is also cooperation with international organizations and the exchange of experiences with other countries that implement advanced practices in the field of cybersecurity.

The development of digital technologies not only increases risks but also opens new opportunities for optimizing customs processes. The implementation of artificial intelligence systems can assist in identifying potential risks, and the use of blockchain technologies ensures greater transparency and reliability of supply chains, helping to prevent fraud and increase trust among participants in foreign economic activity.

Key words: customs, digitalization, cybersecurity, digital infrastructure, customs services, administrative services, customs documents, customs clearance.

Постановка проблеми. Митні органи оперують великими обсягами конфіденційної інформації, включаючи дані про товари, транспортні засоби та учасників зовнішньоекономічної діяльності. Несанкціонований доступ до цієї інформації, її викрадення або маніпулювання можуть мати серйозні наслідки для національної безпеки, економіки та міжнародної торгівлі. Зростаюча кількість та складність кібератак, а також використання новітніх технологій злочинцями, вимагають від митних органів впровадження ефективних засобів захисту цифрових систем.

Однією з головних проблем є недостатня інтеграція сучасних засобів кіберзахисту в існуючі системи митних органів. Багато з них досі використовують застарілі технології, які не відповідають сучасним вимогам кібербезпеки. Крім того, існує проблема браку кваліфікованих фахівців у сфері кібербезпеки, здатних ефективно протистояти новітнім загрозам.

Метою дослідження є виявлення загроз, що можуть впливати на цифрові інфраструктури митних органів, проведення аналізу існуючих заходів та технологій захисту, що використовуються митними органами, та визначити їх ефективність у контексті сучасних кіберзагроз.

Проблематика захисту цифрових інфраструктур митних органів є актуальною як на міжнародному, так і на національному рівні. В

Україні дослідження у цій сфері здійснюють провідні вчені та експерти, що працюють над вирішенням проблем інформаційного простору та кібербезпеки в контексті адміністративного права та митної політики держави.

Виклад основного матеріалу. Діяльність ДМС України спрямована на забезпечення економічного зростання, добробуту країни, розвитку зовнішньої торгівлі, якісного надання адміністративних послуг, на досягнення інших стратегічних цілей, передбачених нормативними документами. Доцільно зазначити двоїстий характер надання адміністративних послуг. У результаті здійснення митної діяльності формуються особливі умови для захисту економічних інтересів, забезпечення економічної безпеки України, задоволення економічних потреб учасників зовнішньоекономічної діяльності. У наукових дослідженнях характерною класифікаційною ознакою адміністративних послуг є суб'єкт, який надає певний перелік послуг. Переважна більшість вчених виділяють комерційні та державні митні послуги, що зумовлено відмінностями суб'єктів, які надають послугу. Вказана обставина є основоположною при дослідженні сфери державних і комерційних адміністративних послуг. Сфера митних послуг включає сектор державних адміністративних послуг, сектор послуг, що надаються суб'єктами господарської діяльності – прибутковими організаціями [1; с. 106].

Митні органи відіграють ключову роль у забезпеченні економічної та національної безпеки держави, контролюючи перетин товарів через кордон. Важливою складовою їх діяльності є надання різноманітних адміністративних послуг, які забезпечують ефективно і прозоре виконання митних процедур.

Основною послугою митних органів є прийом, обробка та контроль митних декларацій. Ця процедура включає перевірку правильності заповнення декларацій, відповідність товарів заявленим у документах характеристикам та нарахування митних платежів. Ефективне виконання цієї функції сприяє прискоренню товарообігу і зниженню ризиків контрабанди та порушення митних правил.

Одним з найважливіших та найскладніших етапів здійснення зовнішньоекономічних операцій є процедура митного оформлення товарів і транспортних засобів комерційного призначення, що переміщуються через митний кордон України, в якій основна роль належить декларуванню, яке виконує функцію забезпечення митного оформлення. Без здійснення декларування, в результаті якого митному органу повідомляються відомості про товари, транспортні засоби, що переміщуються через митний кордон України, мету, режим такого переміщення тощо, неможливим є закріплення результатів митного

контролю, тобто здійснення необхідних митних процедур. При цьому, норми законодавства, якими врегульовано цей важливий правовий інститут є досить складними та специфічними, що суттєво заважає їх сприйняттю та реалізації [2; с. 107].

Вступ України в світовий простір призвів до зростання обсягу товарів і транспортних засобів, які перетинають митний кордон. В умовах скорочення часу на здійснення поточного митного контролю зросли ризики ввезення товарів із порушенням митного законодавства. Для виявлення та припинення адміністративних правопорушень і кримінальних злочинів підрозділи митних органів проводять митний контроль. Цей контроль, як інструмент реалізації митних послуг, охоплює різноманітні види, форми, принципи та заходи, що забезпечують ефективне виконання митних процедур.

Аналіз нормативно-правових наукових джерел дав змогу комплексно визначити наявні види митних послуг, які надаються митними органами і комерційними організаціями. Крім того, цей аналіз дозволив розширити класифікацію митних послуг, враховуючи нові кваліфікаційні критерії, такі як терміни надання, форми реалізації, вартість і типи надання митних послуг. Розроблена класифікація може бути ефективно використана для підвищення якості та ефективності митних послуг, а також при розробці стратегічних документів у цій галузі. Наприклад, при створенні Концепції розвитку системи управління якістю митних послуг до 2030 року і уніфікації митного законодавства.

Система управління якістю митних послуг доволі складна, тому, реалізуючи механізм управління її якістю, важливо враховувати вплив різних підсистем, що постійно взаємодіють між собою. Мета управління якістю митних послуг у митних органах полягає у забезпеченні єдиної дії всіх працівників митних органів для вирішення поставлених перед ними завдань щодо задоволення потреб учасників ЗЕД, за умови дотримання принципів забезпечення економічної безпеки держави [3; с. 91].

Митні органи активно співпрацюють з міжнародними організаціями та митними службами інших країн для обміну інформацією та досвідом, координації дій у боротьбі з контрабандою і порушеннями митного законодавства. Таке співробітництво сприяє гармонізації митних процедур і підвищенню ефективності митного контролю на міжнародному рівні [4].

Ця взаємодія включає участь у спільних навчаннях та семінарах, розробку та впровадження спільних проєктів, а також використання сучасних технологій для покращення моніторингу та аналізу митних операцій. Наприклад, впровадження єдиних електронних систем декларуван-

ня та обміну даними дозволяє швидше і точніше перевіряти вантажі, що перетинають кордони.

Крім того, митні органи активно співпрацюють у сфері підвищення безпеки ланцюгів постачання, що включає заходи проти тероризму та інших загроз. Спільні дії з партнерами сприяють створенню більш безпечного і прозорого міжнародного торговельного середовища. Міжнародні стандарти та рекомендації, розроблені у співпраці з такими організаціями, як Всесвітня митна організація, допомагають уніфікувати процедури та вимоги, що знижує ризики і забезпечує більш ефективне виконання митних функцій.

Таким чином, міжнародне співробітництво митних органів не лише покращує обмін інформацією і досвідом, але й сприяє розвитку глобальної системи митного контролю, яка є більш ефективною, безпечною і прозорою. Це, в свою чергу, сприяє зростанню міжнародної торгівлі та економічному розвитку, забезпечуючи належний баланс між сприянням торгівлі та захистом національних інтересів. Всі ці послуги забезпечують належне функціонування митної системи, сприяють розвитку зовнішньоекономічної діяльності та захисту національних інтересів. Ефективне виконання митними органами своїх обов'язків є запорукою економічної стабільності та безпеки країни.

Будь-яка компрометація цифрової інфраструктури Державної митної служби може мати серйозні наслідки, включаючи економічні втрати, підрив національної безпеки та шкоду міжнародній репутації. Тому захист інформаційних систем митних органів стає пріоритетним завданням.

В 2023 році Єврокомісія анонсувала масштабні зміни – найбільшу реформу за час існування Митного союзу з моменту його створення в 1968 році. У березні 2024 року Європейський парламент підтримав пропозиції у першому читанні. Далі вони розглядатимуться новим парламентом, вибори якого відбулися на початку червня. Основою реформи є створення нового Митного органу ЄС (EU Customs Authority) та Центру митних даних ЄС (EU Customs Data Hub), який поступово замінить наявну у країнах-членах ЄС митну ІТ-інфраструктуру. Усі держави-члени матимуть доступ до даних у реальному часі, а штучний інтелект аналізуватиме дані та прогнозуватиме проблеми ще до відвантаження товарів у ЄС. Це сприятиме прозорій взаємодії у ланцюгу митниця-трейдер-споживач та зекономить час і ресурси для всіх учасників ринку. За попередніми оцінками Єврокомісії, понад 2 млрд євро на рік митні органи ЄС зможуть заощадити тільки на операційних витратах.

Таким чином, реформа має на меті досягнення двох основних цілей:

– зменшення витрат для бізнесу та митних органів шляхом спрощення процедур;

– надання можливості митним органам краще захищати інтереси ЄС на основі спільного управління ризиками та більш гармонізованого контролю.

Митна реформа ЄС передбачає нове партнерство між бізнесом та митними органами. Зокрема, концепція «Trust and Check traders» ґрунтується на поточній програмі Авторизованих економічних операторів і передбачає її розвиток. Як і для статусу АЕО, для отримання статусу «Trust and Check Traders» підприємства повинні будуть відповідати ряду критеріїв, спрямованих на те, щоб гарантувати їх надійність, таким як чиста юридична історія, високий рівень контролю над своїми операціями та ланцюгом поставок, а також фінансова спроможність.

У квітні 2024 року Україна успішно перейшла на NCTS Фаза 5, навіть випередивши багато європейських країн. Водночас зростання кількості українських компаній, що отримали статус АЕО, має динаміку, схожу з більшістю країн ЄС у перші роки впровадження програми, а подекуди її перевищує. Це свідчить про те, що Україна вже готова до інтеграції концепції «Trust and Check traders», адже українські трейдери діями заявили про свою надійність, а митниця - про технічну готовність.

Державна митна служба України продовжує процес цифровізації та створює ІТ-рішення, які потенційно можуть інтегруватися в Центр митних даних ЄС. Водночас українська митниця працює над актуалізацією діючих інструментів з управління ризиками, адже саме завдяки ризикорієнтованому підходу можна гарантувати, що ринок буде захищений від небезпечних або незаконних товарів, не перешкоджаючи стабільному товаропотоку [5].

У рішеннях Європейського Союзу "Електронна митниця" є базою для створення "єдиного вікна", яке зобов'язані використовувати інші відомства, що задіяні у митній справі. Тому і на митні органи України мають бути покладені додаткові обов'язки з координації дій міністерств та відомств в цьому напрямку, затверджених відповідними рішеннями уряду. Об'єднуючий стрижень митної служби – це інформаційні механізми. Ця система має бути створена на нових інформаційних технологіях та, відповідно, на сучасній матеріальній базі, яка дасть можливість побудувати модернізовану багаторівневу систему із застосуванням телекомунікаційних технологій, забезпеченою комплексною системою захисту інформації, що потребує тривалого часу та значних капіталовкладень [6, с. 56].

Основними викликами є зростаюча складність кіберзагроз, високий рівень автоматизації, необхідність забезпечення безперервності бізнесу

та міжнародний характер діяльності. Кібератаки стають все більш складними і витонченими, використовуючи нові методи та технології для обходу захисних механізмів. Збільшення кількості автоматизованих систем та ІТ-пристроїв створює нові вразливості, які можуть бути використані зловмисниками. Критичні системи митних служб повинні функціонувати безперебійно, що ускладнює проведення регулярних оновлень та тестувань безпеки. Митні органи взаємодіють з різними міжнародними структурами, що потребує узгодження стандартів та підходів до кібербезпеки на міжнародному рівні.

Сучасні підходи до безпеки митної інформаційної системи включають інтеграцію кібербезпеки на всіх рівнях, використання штучного інтелекту та машинного навчання, постійне навчання персоналу та співпрацю і обмін інформацією. Використання багаторівневих систем захисту, що включають мережевий захист, захист даних, контроль доступу та моніторинг активності, є необхідним. Штучний інтелект та машинне навчання дозволяють виявляти аномалії та підозрілу активність в режимі реального часу, що допомагає швидко реагувати на потенційні загрози. Людський фактор залишається однією з основних вразливостей, тому регулярні тренінги та підвищення обізнаності працівників є критично важливими. Взаємодія з іншими державними та міжнародними організаціями для обміну досвідом та інформацією про кіберзагрози також є ключовим елементом захисту.

Захист цифрової інфраструктури у митно-адміністративних послугах є надзвичайно актуальним питанням у сучасному світі. Підвищення рівня кібербезпеки вимагає комплексного підходу, який включає як технологічні рішення, так і організаційні заходи. Лише постійна адаптація до нових викликів та впровадження передових практик зможе забезпечити надійний захист критично важливих систем та інформаційних ресурсів митних органів.

Система забезпечення митної безпеки – єдність, цілісність закономірно розташованих і взаємопов'язаних цільового, об'єктного, суб'єктно-організаційного й результативного компонентів. Системотвірним складником цієї системи є мета - реалізація економічних і безпосередньо митних інтересів і нівелювання відповідних загроз і небезпек. Елементами об'єктного компонента є: предмет – митні інтереси; суб'єкти / носії митних інтересів; загрози й небезпеки митним інтересам, які охоплюють джерела й носіїв загроз. Суб'єктно-організаційний компонент охоплює організаційно-інституційний та організаційно-функціональний елементи. Досягнутий результат функціонування системи забезпечення митної безпеки має корелювати з метою та дозволяє встановити рівень дієвості,

ефективності всієї системи й визначити напрямки її удосконалення. Система забезпечення митної безпеки є відкритою та динамічною, тобто реагує на зміни в зовнішньому середовищі, а її розвиток детермінується відповідними чинниками [7, с. 63].

ІТ-технології дійсно реалізували в повному обсязі поняття «інформаційний вік». У розвинутих країнах світу митниця трансформувалася в одну з найбільш прогресивних державних служб. Так, якщо в інших сферах дані процеси тільки набирають оберти, то митниця вже стала цифровою. Цифрова митниця означає використання цифрових систем для збору і захисту митних зборів, контролю за потоками товарів, людей, транспортних засобів та грошей, а також для захисту транскордонної торгівлі від злочинності, включаючи міжнародний тероризм [8].

Поєднання цифровізації та кібербезпеки є необхідним для забезпечення стабільної та ефективної роботи митних органів у сучасному світі. Інноваційні технології мають величезний потенціал для покращення якості митних послуг, але їх впровадження повинно супроводжуватися комплексними заходами захисту від кіберзагроз, щоб забезпечити надійність та безпеку всієї системи.

Однією з ключових переваг цифровізації є можливість автоматизації рутинних процесів, що значно зменшує час, необхідний для обробки митних документів та перевірки вантажів. Впровадження електронних систем обміну даними дозволяє митним органам більш ефективно взаємодіяти з іншими державними службами та учасниками зовнішньоекономічної діяльності. Це не лише спрощує процедури митного оформлення, але й підвищує прозорість та зменшує можливості для корупції.

Водночас, підвищення рівня цифровізації вимагає серйозної уваги до питань кібербезпеки. Це включає регулярні аудити безпеки, оновлення програмного забезпечення, використання сучасних засобів захисту від вірусів та інших шкідливих програм, а також навчання персоналу основам кібергігієни. Важливо також забезпечити резервне копіювання критичних даних і розробити плани на випадок надзвичайних ситуацій.

Забезпечення кібербезпеки також включає співпрацю з національними та міжнародними організаціями у сфері кіберзахисту. Це дозволяє отримувати актуальну інформацію про нові загрози та методи їх нейтралізації, а також брати участь у спільних тренуваннях та навчаннях, що сприяє підвищенню кваліфікації працівників.

Таким чином, інтеграція інноваційних технологій у роботу митних органів разом з комплексним підходом до кібербезпеки забезпечує їхню ефективність, прозорість та надійність. Це спри-

яє розвитку міжнародної торгівлі, забезпечуючи належний рівень захисту як для держави, так і для бізнесу, що бере участь у зовнішньоекономічній діяльності.

Висновки. Захист цифрової інфраструктури у митно-адміністративних послугах є критично важливим аспектом, що забезпечує стабільність та ефективність функціонування митних органів в умовах сучасного світу. З огляду на активну цифровізацію митних процесів, питання кібербезпеки набули першорядного значення. Впровадження нових технологій створює нові можливості для оптимізації митних процедур, але одночасно збільшує ризики кібератак та несанкціонованого доступу до конфіденційної інформації.

Серед основних викликів у сфері захисту цифрової інфраструктури митних органів можна виділити зростаючу складність кіберзагроз, брак кваліфікованих кадрів у сфері кібербезпеки, а також недостатню інтеграцію сучасних засобів захисту в існуючі системи. Постійно змінюючийся характер кіберзагроз вимагає від митних органів швидкої адаптації та впровадження нових підходів до захисту.

Для ефективного захисту цифрової інфраструктури митних органів необхідно впроваджувати багаторівневі системи кіберзахисту, що включають використання сучасних засобів шифрування, аутентифікації та моніторингу мереж. Важливо також проводити регулярні аудити безпеки та навчання персоналу, щоб підвищити їх обізнаність щодо кіберзагроз та методів їхньої нейтралізації.

Співпраця з міжнародними організаціями та митними службами інших країн є ключовим елементом у забезпеченні ефективної кібербезпеки. Обмін інформацією, досвідом та найкращими практиками сприяє гармонізації підходів до захисту цифрової інфраструктури на глобальному рівні. Важливим аспектом є підвищення рівня обізнаності працівників митних органів про кібербезпеку. Регулярні тренінги та навчання допомагають створити культуру безпеки, що значно зменшує ризики успішних кібератак. Використання новітніх технологій, таких як штучний інтелект та машинне навчання, дозволяє значно покращити процеси виявлення та нейтралізації кіберзагроз. Інноваційні підходи до аналізу даних та прогнозування потенційних атак стають невід'ємною частиною сучасної стратегії кібербезпеки.

Таким чином, ефективний захист цифрової інфраструктури митно-адміністративних послуг вимагає комплексного підходу, що поєднує сучасні технологічні рішення, постійне навчання персоналу та міжнародне співробітництво. Лише в таких умовах можна забезпечити стабільну та безпечну роботу митних органів у цифровому

просторі, сприяючи розвитку міжнародної торгівлі та економічному зростанню.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ:

1. Шляховський О.А., Сиймовський Р.М., Ковалів М.В., Єсімов С.С. Зміст адміністративних послуг, що надаються митними органами. *Наукові записки Львівського університету бізнесу та права. Серія економічна. Серія юридична*. 2021. Випуск 30. С. 104–110.
2. Коваль, Н.О. *Форми митного декларування та порядок їх застосування LexPortus 2018 № 3, С. 106–118.*
3. Руда М.В., Пукас Ю.А. Ключові аспекти застосування інструментарію оцінювання якості митних послуг на засадах маркетингу *Менеджмент та підприємництво в Україні: етапи становлення та проблеми розвитку 2023 № 1 (9) С. 91–107*
4. Міжнародна конвенція про спрощення і гармонізацію митних процедур URL: https://zakon.rada.gov.ua/laws/show/995_643#Text (дата звернення 07.07.2024 р.)
5. Звягінцев С.Б. Реалізація реформи у наступні кілька десятиліть створить безпечний та конкурентний ринок у єдиній цифровій екосистемі. URL: <https://customs.gov.ua/news/zagalne-20/post/ukrayina-bude-gotova-povnotsinno-stati-chastinoiuevropeiskoyi-mitnoyi-infrastrukturi-domomentu-realizatsiyi-mitnoyi-reformi-uesergii-zviagintsev-1638> (дата звернення 02.07.2024 р.)
6. Микуляк О.В., Стефанишин Р.І. Впровадження інформаційних технологій у митну практику України *Податки і фіскальна політика 2019 № 4(61) С. 53–66.*
7. Рябовол Л.Т. Система забезпечення митної безпеки в Україні *Юридичний вісник 2020 № 4 С. 58–65.*
8. Мацедонська Н., Коваленко В., Штефан Л. Модернізація митної діяльності з використанням інформаційних технологій. *Економіка та суспільство*. 2021, № 27.