

аналітична записка

# «РОЗУМНІ КОРДОНИ» В УКРАЇНІ

Ірина Сушко

травень 2025

---

Аналітична записка підготовлена в рамках проекту ICMPD “EU4IBM-Стійкість”, що фінансується Європейським Союзом.

Відповідальність за зміст публікації несе виключно автор. Позиція ICMPD може не збігатися з висновками, викладеними в цьому документі.



<b>Вступ</b> .....	<b>2</b>
<b>Ключові висновки</b> .....	<b>2</b>
<b>Визначення «Розумних кордонів»</b> .....	<b>3</b>
<b>Функції та перспективи «розумних кордонів»</b> .....	<b>5</b>
<b>Штучний інтелект у контексті «розумних кордонів»</b> .....	<b>7</b>
<b>Ризики «розумних кордонів»</b> .....	<b>8</b>
Вразливість технологій .....	8
Порушення прав людини .....	9
Захист даних .....	10
<b>Міжвідомча та міжнародна координація</b> .....	<b>11</b>
<b>Пропозиції</b> .....	<b>12</b>
<b>Додаток</b> .....	<b>13</b>



## Вступ

Україна з 2022 року є країною-кандидатом на членство в Європейському Союзі, а 8 листопада 2023 року Європейська Комісія рекомендувала ЄС розпочати переговори про вступ з Україною. З точки зору управління кордонами це означає, що Україна отримала перспективу приєднання до загальноєвропейської системи безпеки та управління. Це також означає, що Україна повинна привести свою систему інтегрованого управління кордонами (ІУК) у відповідність до вимог ЄС, з одного боку, а з іншого – адаптувати її до унікальних викликів, відповідей на які може не бути у регуляціях ЄС. З грудня 2024 року, профільні органи влади, дотичні до управління кордоном розпочали роботу над розробкою нової Стратегії інтегрованого управління державним кордоном України.

Запропонована структура Стратегії міститиме цілі, що відповідають компонентам інтегрованого підходу в управлінні кордонами ЄС. Окремі з них повністю зосереджені на розвитку систем автоматизованого контролю на кордонах та відповідають завданням, передбаченим у «Пакеті розумних кордонів ЄС»<sup>1</sup>. Запровадження в українській Стратегії нових стратегічних цілей базованих на підході «розумних кордонів» (далі – РК) потребує вивчення. Хоч в українському контексті вже застосовувались окремі елементи РК, однак у сфері управління кордонами цей термін не набув широкого вжитку та має різні трактування. По-перше, важливо розглянути поняття РК та практику його застосування в різних країнах, але з акцентом на Європейський Союз і Україну. Також важливо дати відповідь, які саме компоненти РК вже застосовувались в управлінні кордонами України, а які потрібно запровадити з урахуванням руху України до членства в ЄС. Разом з цим, важливо надати проміжний аналіз переваг та ризиків, пов'язаних із застосуванням компонентів РК в нову Стратегію ІУК.

## Ключові висновки

Вжиток терміну «розумні кордони» протягом останніх 20-ти років еволюціонував від широкого розуміння як належного управління кордонами в цілому до належного управління кордонами через цифровізацію та автоматизацію, або навіть до ще вужчого розуміння як конкретних проєктів (smart border package).

Тут РК визначено як *політики та техніки швидшого здійснення контролю руху людей і товарів, зі збереженням або підвищенням рівня безпеки та дотриманням прав людини, завдяки цифровізації та автоматизації контрольних процедур, збору й обробці великих обсягів даних, розширенню часових і просторових меж збору цих даних.*

---

<sup>1</sup> Smart Borders - European Commission



Концепція РК тісно пов'язана з розвитком технологій штучного інтелекту. Оскільки ЄС визначає ШІ як критично важливу технологію, імовірно, розвиток концепції РК може отримати політичну підтримку та інвестиції з боку структур ЄС і країн-членів ЄС в контексті руху України до членства.

Велика кількість програм і проєктів, які можна вважати елементами РК, вже присутні на українському кордоні, однак є ті, які очікують свого впровадження в контексті євроінтеграції України.

Нові стратегічні цілі Стратегії ІУК міститимуть компоненти РК, зокрема компонент 10 «Використання сучасної технології, включаючи великі інформаційні системи» та компонент 15 «Дослідження та інновації».

Згадані стратегічні цілі мають бути узгоджені зі Стратегією цифрового розвитку інноваційної діяльності України на період до 2030 року<sup>2</sup> та корелюватись з завданнями європейської інтеграції у сфері інноваційної діяльності.

Подальше застосування та розвиток концепцій РК повинно зважати на такі критичні ризики, як вразливість технологій, ризик порушення прав людини, ризики витоку даних та проблеми належної міжнародної і міжвідомчої взаємодії.

## Визначення «Розумних кордонів»

«Розумні кордони (smart borders)» (далі – також РК) є інтуїтивним контекстуальним терміном, значення якого відрізняється залежно від часу, географії та системи управління кордонами, в якій його застосовують.

Так, коли у 2001 році **США та Канада** підписали Декларацію розумних кордонів, План заходів до цієї Декларації містив 30 пунктів щодо такого широкого кола питань як запровадження біометричної ідентифікації, обмін попередньою інформацією про пасажирів (API/PNR), обмін даними, вдосконалення інфраструктури, координація та спільне навчання<sup>3</sup> – перелік, великою мірою подібний до сфери охоплення сучасною концепцією Інтегрованого управління кордонами в ЄС.

Сьогодні ж Канадська агенція служб кордону (CBSA), яка поєднує функції прикордонної, митної, міграційної служб та служби контролю споживчих товарів, зараховує до РК вже лише «нові цифрові інструменти та технології, покликані вдосконалити та пришвидшити контроль і пропуск мандрівників без шкоди для безпеки», такі як біометричні кіоски самообслуговування та eGate в

---

<sup>2</sup> Розпорядження КМУ від 31.12.2024 №1351 «Про схвалення Стратегії цифрового розвитку інноваційної діяльності України на період до 2030 року»

<sup>3</sup> U.S. - Canada Smart Border/30 Point Action Plan Update

аеропортах, механізми попереднього декларування, чи додаток CanBorder, який дозволяє оцінити час очікування на конкретному пункті пропуску<sup>4</sup>.

В **Європейському Союзі** концепція РК сьогодні присутня передусім у «Пакеті розумних кордонів<sup>5</sup>», зосередженому на розвитку систем автоматизованого контролю на кордонах (ABC, automated border control), таких як Entry-Exit System (EES) і European Travel Information and Authorisation System (ETIAS).

В чинній *багаторічній стратегічній політиці у сфері ІУК*, схваленій рішенням Єврокомісії на 2023-2027 роки<sup>6</sup>, термін РК прямо не фігурує, проте два з 15 визначених цим документом компонентів ІУК безпосередньо стосуються теми РК. *Компонент 10 «Використання сучасної технології, включаючи великі інформаційні системи»*, постулює, що європейське ІУК, «особливо перевірки на кордоні та спостереження на кордоні», має здійснюватися з застосуванням найсучасніших технічних систем і рішень. *Компонент 15, «Дослідження та інновації»*, покликаний забезпечити умови для появи та підтримки таких технологій і рішень. Прикметно, що серед стратегічних засад цих двох компонентів значну увагу приділено питанням захисту персональних даних, дотриманню фундаментальних прав та зменшенню залежності в технологіях від третіх країн.

На інституційному рівні в ЄС в рамках підготовки «пакету розумних кордонів» діє профільна робоча група – *Комітет розумних кордонів*, до якого входять представники поліції, міністерств внутрішніх справ чи прикордонних служб країн-членів, і які з'ясовують конкретні питання підготовки до впровадження EES, ETIAS і не тільки, під час регулярних зустрічей<sup>7</sup>.

В **українському контексті** термін РК використовували для позначення облаштування східного кордону системами відеоспостереження та сейсмічними датчиками у 2017 році<sup>8</sup>. Проте в чинній Стратегії ІУК впровадження принципів РК згадується вже в контексті вдосконалення контролю на пунктах пропуску, а не охорони «зеленого кордону». РК в Стратегії ІУК семантично пов'язаний з концепціями «кращих європейських практик», «сучасних технологій» і «ІТ рішень», «спрощення формальностей» і «підвищення безпеки», а також «обміну даними»<sup>9</sup>. Попри те, що РК в Стратегії ІУК згаданий у розділі «Контроль у пунктах пропуску», багато інших цілей, заходів і проєктів в різних сферах ІУК можуть бути віднесені до РК – *від автоматичного розпізнавання номерних знаків до NCTS та AEO, і від електронної черги до систем аналізу ризиків*.

Базуючись на наявній практиці вжитку терміну РК, можна дійти до висновку, що станом на сьогодні він еволюціонував від первісного широкого значення належної організації управління кордоном до вузького розуміння як *політики та техніки швидшого здійснення контролю руху людей і товарів, зі збереженням або підвищенням рівня безпеки та дотриманням прав людини, завдяки*

<sup>4</sup> Government of Canada, Canada Border Services Agency. *Smart and Secure Border Tools for Travel and Trade*

<sup>5</sup> *Smart Borders Package - European Commission*

<sup>6</sup> *Communication From The Commission To The European Parliament And The Council establishing the multiannual strategic policy for European integrated border management*

<sup>7</sup> *European Commission. Smart Borders Committee (EES, ETIAS, VIS)*

<sup>8</sup> *Радіо Свобода. Інтелектуальна електронна система охоронятиме кордон України з Росією – бідило*

<sup>9</sup> *Розпорядження КМУ від 24.07.2019 «Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 року»*

*цифровізації та автоматизації контрольних процедур, збору й обробці великих обсягів даних, розширенню часових і просторових меж збору цих даних.*

При цьому варто відзначити дві багатозначності у вжитку цього терміну. Перша полягає в тому, що РК можуть позначати як конкретні проекти цифровізації й автоматизації на кордоні (наприклад, smart borders package в ЄС або згаданий вище проєкт облаштування східного кордону в Україні), так і наскрізний принцип управління кордонами (як у чинній Стратегії ІУК). Друга багатозначність охоплює сферу застосування – це можуть бути або контроль на кордоні, в пунктах пропуску, або спостереження на (зеленому) кордоні. Подальше використання цього терміну в сфері ІУК повинне керуватися свідомим і осмисленим вибором між цими альтернативними значеннями, або так само свідомим їх поєднанням.

## Функції та перспективи «розумних кордонів»

Так як концепція РК є дуже широкою, створити вичерпний перелік функцій РК складно. Найчастіше їх вбачають у тому, щоб:

- Пришвидшити контроль в умовах збільшення трафіку
- Підвищити безпеку без збільшення тривалості перевірок
- Усунути людський фактор (упередженість, корупція)

На думку аналітиків FRONTEX, технології РК можуть застосовуватися для:

- Поліпшення ситуаційної обізнаності через обробку великих масивів даних спостережень
- Управління інформацією, у тому числі, розпізнавання образів і патернів, обробка природної мови, предикативний аналіз тощо
- Комунікації, як-от чат боти
- Виявлення, ідентифікації та автентифікації людей і об'єктів
- Навчання та тренінгів персоналу<sup>10</sup>

Наприклад, у рамках проєкту **D4Fly** (виявлення підробок документів та ідентифікація під час польоту)<sup>11</sup> за участі академічних установ, бізнесу та відповідних служб Великої Британії, Нідерландів, Литви та Греції тестували та вивчали такі технології:

- *Унікальний паттерн подорожі* – автоматичне сканування всіх віз і відміток про перетин кордону, яке дозволяє побудувати паттерн подорожі конкретного мандрівника і виявити можливі аномалії.
- *Історія перевірок документів* – фіксація за допомогою блокчейну всіх попередніх перевірок конкретного документа, що дозволяє прикордоннику переглянути всі попередні перевірки.

---

<sup>10</sup> FRONTEX. *Artificial intelligence-based capabilities for the EU border and coast guard final report*

<sup>11</sup> *Detecting document fraud*

- *Генерація альтернативних зображень* – моделювання за допомогою ШІ на основі фото в паспорті альтернативних зображень, зокрема інших кутів та «старіння» мандрівника
- *Постійна автентифікація* – розробка додатків, які б проводили постійну автентифікацію особи на підставі даних вже існуючих сенсорів у смартфоні, таких як гіроскоп, акселерометр, магнітометр тощо, порівнюючи дані про типові рухи (поведінкова біометрія) користувача з зафіксованими раніше. З метою захисту даних такий додаток міг би активуватися лише в «коридорі біометричної верифікації» та передавати лише висновок про верифікацію особи. Це потенційно може дозволити проводити ідентифікацію мандрівника під час руху, одночасно зберігаючи час на кордоні та підвищуючи якість перевірки.
- *Біометрична ідентифікація на відстані* – ідентифікація на відстані за типом тілобудови на основі 2Д зображень звичайних камер спостереження<sup>12</sup>.

Проект **AI-ARC** створив Віртуальну Контрольну Кімнату для підвищення ситуаційної обізнаності суб'єктів, які діють в арктичних водах, на основі обробки даних всіх учасників трафіку, прогнозування руху айсбергів, створення єдиної комунікаційної платформи тощо<sup>13</sup>.

Багато проектів у діяльності **суб'єктів ІУК на українському кордоні** також підпадає під визначення РК. Наприклад, єЧерга, яка діє на наземних ПП, оперує великими обсягами даних в режимі реального часу. Державна прикордонна служба користується програмами розпізнавання обличчя від американської Clearview AI<sup>14</sup> та технологією машинного зору для спостереження на кордоні від української Compass Engineering, зокрема, для бойової роботи<sup>15</sup>. Державна митна служба автоматизує процеси в рамках проектів на зразок «Розумний пункт пропуску». Зокрема, триває робота з розроблення ІТ-рішення організації роботи автоматизованої системи митного оформлення «Інспектор» у міжнародному електропоїзді «Інтерсіті+». У рамках міжнародно-технічної допомоги (МТД) отримано програмний Комплекс Криптографічного захисту інформації «QUANT 2.0», який є обов'язковою технічною передумовою запровадження механізму взаємодії інформаційних систем (захід 2 підпункту 1 завдання 1 Стратегічної цілі 1 Стратегії ІУК, Держмитслужба). У серпні 2024 року запрацювала нова система автоматизованого митного оформлення, інтегрована з системами ДПСУ та єЧергою<sup>16</sup>.

Прикметно, що під час семінару високого рівня на тему «Митні адміністрації в контексті забезпечення безпеки та захисту в умовах глобальних змін», організованого Національною податковою адміністрацією Польщі за погодженням з Європейською комісією, представники

---

<sup>12</sup> Multidisciplinary Digital Publishing Institute

<sup>13</sup> Artificial Intelligence based virtual control room for the Arctic

<sup>14</sup> Укрінформ. Завдяки програмі розпізнавання обличчя встановили 10 тисяч російських воєнних злочинів

<sup>15</sup> АДПСУ. Прикордонники тестують технології з машинним зором

<sup>16</sup> Державна митна служба України. Суттєвий крок митниці у напрямку ЄС: перехід на нову автоматизовану систему дозволить скоротити час оформлення транспортних засобів до 35%

української митниці зазначали про необхідність налагодження автоматизованого обміну попередньою митною інформацією між ЄС та третіми країнами в контексті безпеки<sup>17</sup>.

Також керівництвом Державної митної служби зазначалось про застосування цифрових технологій з метою протидії сучасним викликам та для аналізу даних у сфері міжнародної співпраці. Автоматизований обмін попередньою митною інформацією розглядається як ефективний механізм, що сприяє подоланню транскордонної злочинності<sup>18</sup>.

Для забезпечення планування та контролю з впровадження заходів щодо цифрової трансформації процесів Держмитслужба розробила Стратегічний план цифрового розвитку, цифрових трансформацій і цифровізації Державної митної служби України та її територіальних підрозділів. План затверджено Комітетом з управління інформаційними технологіями у системі управління державними фінансами та реалізований наказом Міністерства фінансів України від 15.12.2022 № 435 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами»<sup>19</sup>.

Серед поточних завдань Держмитслужби є імплементація ключових напрямків багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C) до цілей Стратегії ІУК. Зокрема, йдеться про гармонізацію інтерфейсу з ЄС та Єдиного вікна для міжнародної торгівлі, створення технічної специфікації системи та створення специфікацій для інтеграції з зовнішніми системами.

## Штучний інтелект у контексті «розумних кордонів»

Хоча запропоноване тут визначення РК ширше за прийняте в ЄС розуміння штучного інтелекту («застосування комп'ютерних систем, які аналізують їхнє середовище та ухвалюють рішення з певним ступенем автономії»<sup>20</sup>), РК неможливий без його застосування. Вага ШІ в цифровізації контролю та спостереження на кордоні, імовірно, лише зростатиме з часом<sup>21</sup>. У Європейському Союзі технологія штучного інтелекту наразі належить до 4-х найпріоритетніших з 10 критичних технологій для економічної безпеки, визначених Європейською комісією у 2023 році<sup>22</sup>.

---

<sup>17</sup> Урядовий портал. Митні органи країн ЄС, України та Молдови готуються до викликів, спричинених «торговою війною»

<sup>18</sup> Там само.

<sup>19</sup> Наказ Мінфіну від 09.02.2024 № 63 «Про реалізацію рішення Комітету з управління інформаційними технологіями у системі управління державними фінансами»

<sup>20</sup> FRONTEX. Artificial intelligence-based capabilities for the EU border and coast guard final report

<sup>21</sup> European Commission. Europe fit for the Digital Age: Commission proposes new rules and actions for excellence and trust in Artificial Intelligence. 2021

<sup>22</sup> European Commission. Commission recommendation of 3.10.2023 on critical technology areas for the EU's economic security for further risk assessment with Member States



Нещодавні заяви президента США Трампа про плани інвестувати в проєкт розвитку ШІ Stargate 500 млрд доларів та публікація Китаєм чатботу DeepSeek<sup>23</sup>, який обвалив акції американських конкурентів, свідчать про гонку технологій ШІ між основними глобальними суб'єктами, яка, імовірно, змусить ще більше активізувати зусилля в цьому напрямку і Європейський Союз. Хоча загальний обсяг інвестицій в розвиток ШІ в ЄС безперервно зростає щонайменше з 2016 року, сягнувши 16 млрд євро у 2022 р, Європейська аудиторська палата в опублікованому в 2024 році дійшла висновку що такий обсяг не є достатнім, до того ж, країнам ЄС у цьому питанні бракує координації та партнерства з приватним капіталом<sup>24</sup>.

У сфері законодавчого врегулювання ШІ ЄС, навпаки, є глобальним лідером, ухваливши перший комплексний Акт про ШІ<sup>25</sup>, хоча такий регуляторний підхід, на думку деяких аналітиків, знижує конкурентність ЄС у цій сфері<sup>26</sup>.

Викладене вище приводить до двох висновків в контексті РК. По-перше, оскільки сфера ШІ визнана в ЄС критичною технологією, з максимально високим пріоритетом, проєкти розвитку ШІ, у тому числі, у рамках РК, мають високі шанси залучити як політичну підтримку, так і інвестиції з боку структур ЄС, або окремих держав-членів.

По-друге, враховуючи перспективу членства України в ЄС, в розробку систем РК необхідно заздалегідь закладати засади використання ШІ, описані в Акті про ШІ.

## Ризики «розумних кордонів»

Цифровізація та використання ШІ на кордоні мають специфічні ризики, на які вказують професіонали у сфері ІУК, правозахисники або академічні дослідники. Це *ризики функціональної вразливості, порушення прав людини, захисту даних, браку міжвідомчої та міжнародної взаємодії*. Наведений перелік може бути доповнений.

### Вразливість технологій

З усуненням завдяки цифровізації фізичних «пляшкових горлечок» у пунктах пропуску фактично створюється одне віртуальне «пляшкове горлечко», яке може, теоретично, призвести до повного паралічу пропускових операцій внаслідок аварії або диверсії.

---

<sup>23</sup> Forbes Ukraine. Трамп оголосив про запуск проєкту «Зоряна брама» із розвитку ШІ з інвестиціями \$500 млрд

<sup>24</sup> European Court Of Auditors. Special report 08/2024: EU Artificial intelligence ambition

<sup>25</sup> Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act) (Text with EEA relevance)

<sup>26</sup> Science Business. EU is 'losing the narrative battle' over AI Act, says UN adviser



Вразливість щораз більше цифровізованого кордону до кібератак визнають і у FRONTEX<sup>27</sup>. У Стратегічному аналізі ризиків до 2034 року FRONTEX розглядає як найгірший сценарій розвитку подій, у якому прикордонний контроль чимраз більше цифровізується через падіння привабливості роботи в прикордонних службах, надмірну вартість праці та брак людських ресурсів. Це створює суттєві вразливості в процесі управління кордонами, оскільки просунуті технологічні системи зазнають атак з боку організованої злочинності та афілійованих з державами ворожих груп, що може включати хакерські атаки та атаки на фізичну інфраструктуру<sup>28</sup>.

Однією з можливих відповідей на цей виклик може бути певний дублюючий алгоритм роботи пунктів пропуску, який міг би функціонувати навіть у разі глобального виходу з ладу цифрової інфраструктури. Закладення принципу нецифрового дублювання у концепцію РК дозволить підвищити безпеку використання новітніх технологій. Проте підтримка функціональності такої схеми вимагатиме додаткової витрати ресурсів, наприклад, на проведення тренувань та навчання персоналу роботи в «цифровому» та «безцифровому» режимі.

### **Порушення прав людини**

Застосування систем оцінки ризиків і профайлінг на основі ШІ, системи визначення емоцій та поведінкової біометрії, віддалена ідентифікації можуть нести ризики суттєвих порушень прав людини, дискримінації та порушення права на притулок (наприклад, через автоматичне винесення рішення про відмову в перетині кордону на підставі походження або попередньої історії мандрівника)<sup>29</sup>.

Хоча ступінь занепокоєння цими технологіями може бути надмірним, увага до прав людини є неодмінною рисою європейського ІУК. Запобіжники від порушень прав людини закладаються як на рівні стратегічних документів, так і інституційно. Зокрема, управлінню кордонами регулярно приділяє увагу Європейська агенція фундаментальних прав, у Frontex існує посада офіцера з фундаментальних прав, а окремі масштабні проекти РК на зразок ETIAS мають власну моніторингову Раду з питань фундаментальних прав<sup>30</sup>. *Інституційні механізми моніторингу дотримання основних прав людини мають бути частиною концепції розвитку РК.*

Так само у розвитку РК мають бути враховані положення Європейської декларації про цифрові права та принципи<sup>31</sup>, а також запобіжники та регуляції Акту про ШІ<sup>32</sup>:

- Судження про людей мають базуватися на їхній фактичній поведінці, і ніколи не повинні базуватися виключно на передбаченнях ШІ, заснованих на профайлінгу чи певних характеристиках, як-от громадянство, місце народження чи тип автомобіля;

---

<sup>27</sup> FRONTEX. *A Strengthened European Border and Coast Guard Built on Trust to Protect and Connect Europe*

<sup>28</sup> FRONTEX. *The Strategic Risk Analysis 2024 Report*

<sup>29</sup> *Joint statement: The EU AI Act must protect people on the move*

<sup>30</sup> FRONTEX. *ETIAS Fundamental Rights Guidance. Annual report Board 2023*

<sup>31</sup> *European Commission. Europe's Digital Decade: digital targets for 2030*

<sup>32</sup> *EU Artificial Intelligence Act*

- ШІ-системи прикордонних служб належать до високоризикових, оскільки їхня робота може вплинути на долю людей в особливо вразливих ситуаціях, і тому потребують додаткового контролю;
- Високоризикові ШІ-системи повинні бути розроблені таким чином, щоб людина могла здійснювати нагляд за їхньою роботою та її відповідністю до засадничих принципів;

### Захист даних

Презентація «Пакету розумних кордонів» Європейською комісією ще 2013 року викликала хвилю критики та занепокоєння від членів Європейського парламенту щодо збору біометрії та збереження даних в проекті ЄК щодо запровадження Entry/Exit System або EES – системи автоматичної реєстрації в'їзду та виїзду громадян третіх країн до країн Шенгенської зони. У ній мають фіксуватись дані про мандрівника – скільки днів в Шенгені він провів, місце в'їзду/виїзду, та які були причини відмови у в'їзді<sup>33</sup>.

Саме ця система EES має застосовуватись для громадян третіх країн, що мають безвізовий режим, в переліку яких знаходиться і Україна. Комітет із громадянських свобод, юстиції та внутрішніх справ Європейського парламенту (LIBE) вказував на проблеми, пов'язуючи їх із ризиками стеження та порушення конфіденційності. Також доповідачі від LIBE акцентували на необхідності укладення контрактів на створення системи EES лише з компаніями, які надають системи з гарантіями високих стандартів безпеки та конфіденційності. Тривала дискусія про належний захист даних та необхідність обґрунтування Комісією доказів потреби та пропорційності заходів систем ЄС відклала впровадження EES майже на 10 років.

Про ризики витоку даних та проблем їх захисту було наголошено також у промові Європейського інспектора із захисту даних (EDPS)<sup>34</sup> під час дискусій у Європейській Комісії. Зокрема, Європейський інспектор вказував на ризики доступу правоохоронних органів до даних, які могли їх використовувати з метою запобігання та виявлення терористичних злочинів. Саме тому його головною рекомендацією було видалити усі статті та формулювання, пов'язані з невинуватою метою правоохоронних органів користування даними, оскільки заходи не є ані необхідними, ані пропорційними. Загалом визначалось, що збір біометричних ідентифікаторів має бути обмеженим, а зберігання даних має відбуватись за принципом подрібнення даних або їх зашифрованого зберігання, що дало би можливість уникнути створення єдиної масивної бази даних.

У випадку, якщо доступ для правоохоронних органів виявиться необхідним (на підставі вагомих доказів), необхідні надати факти про підозру щодо конкретної особи.

---

<sup>33</sup> Статті 11 і 12 Пропозиції Регламенту Європейського Парламенту та Ради про створення системи в'їзду/виїзду (EES) для реєстрації даних про в'їзд і виїзд громадян третіх країн, які перетинають зовнішні кордони держав членів Європейського Союзу

<sup>34</sup> A Data Protection perspective on the Smart Borders Package - focusing on the possibility of law enforcement authorities' access to border data



## Міжвідомча та міжнародна координація

Взаємодія профільних органів влади, залучених у процес управління кордонами та співпраця з суміжною стороною і міжнародними партнерами є ключовим принципом ІУК<sup>35</sup>. Поточна Стратегія ІУК належним чином відображає принцип горизонтальної взаємодії та містить окрему ціль щодо запровадження механізмів координації суб'єктів ІУК, що забезпечує їх ефективну співпрацю та міжнародне співробітництво для розвитку ІУК в Україні. Водночас, співпраця з профільними службами по іншу сторону кордону все ще не є ефективною. Наприклад, такий елемент РК як e-Черга впроваджена лише на українській частині кордону, а взаємодія між службами, що реалізують цей проект не завжди злагоджена<sup>36</sup>. Повільно запроваджується спільний митно-прикордонний контроль, що базується на взаємодії між профільними службами по обидва боки кордону. Разом з цим, застосування підходу РК вимагатиме ще більш інтенсивного розвитку співпраці, зокрема між митницями та прикордонною службою як зі суміжною стороною, так і загалом з іншими країнами. Профільні служби мають поділяти інноваційне мислення та ресурсно бути готовим до обміну даними, розвитку цифровізації державних послуг, застосування штучного інтелекту, великих даних, хмарних обчислень та інших технологій для автоматичного збору, ідентифікації та порівняння отриманої інформації, онлайн моніторингів, тощо.

Для уникнення проблем із взаємодією необхідно мати нормативну та ресурсну базу, довіру до партнерів, що дозволить здійснювати обмін інформацією, скоординоване управління прикордонних та митних служб через спільний внесок, спільні переваги та підтримку інфраструктури прикордонного і митного контролю та його системне програмне забезпечення.

---

<sup>35</sup> European Commission. *Guidelines for Integrated Border Management in European Commission External Cooperation*

<sup>36</sup> ГО «Європа без бар'єрів». Аналітичний бриф «Чи сприяють цифрові рішення прозорості та запобіганні корупції на кордоні»



## Пропозиції

Стратегічні документи у сфері інтегрованого управління державним кордоном мають розвивати діючі компоненти РК, що вже застосовуються профільними службами на кордоні. При цьому, такі автоматизовані та цифрові рішення мають рухатись в напрямку сумісності з технічними системами ЄС.

Для цього, важливо провести аналіз готовності української ІТ системи у сфері управління кордоном до поступового приєднання автоматизованих систем з такими системами ЄС як EES, ETIAS, SIS, VIS, EURODAC, тощо.

Має бути розроблений чіткий алгоритм дій, що буде відображений у плані заходів Стратегії ІУК з адаптації систем контролю ЄС, зокрема шенгенських.

«Цифровізований діалог» з ЄС має сприяти цілісному сприйняттю профільними органами влади можливостей використання сучасних технологій з метою покращення обміну даними, превентивних відповідей на загрози, зокрема ефективного реагування на подолання транскордонної злочинності.

При цьому, важливо, щоб завдання у сфері ІУК узгоджувалися зі Стратегією цифрового розвитку інноваційної діяльності України на період до 2030 року та корелюватись з завданнями європейської інтеграції у сфері інноваційної діяльності.

Важливо імплементувати ключові напрямки багаторічного стратегічного плану електронної митниці ЄС (Multi-annual strategic plan for electronic customs, MASP-C) до завдань плану заходів нової Стратегії ІУК.

Оскільки інновації тісно пов'язані з дослідженнями, важливо посилити науковий підхід в обґрунтуванні застосувань нових технологій у сфері управління кордону. Критично важливим є вивчення можливостей застосування штучного інтелекту суб'єктами ІУК у своїй діяльності.

Враховуючи перспективу членства України в ЄС, в розробку систем РК необхідно заздалегідь закладати засади використання ШІ, описані в Акті про ШІ.

Щоб зменшити критичний ризик, пов'язаний з вразливістю технологій в процесі управління кордонами, можна запроваджувати дублюючий алгоритм роботи пунктів пропуску, що функціонуватиме навіть у разі глобального виходу з ладу цифрової інфраструктури. Закладення принципу нецифрового дублювання у концепцію РК дозволить підвищити безпеку використання новітніх технологій.

## Додаток

### Компоненти РК, що вже впроваджені в систему управління кордону або можуть бути запроваджені

№	Компоненти	Може включати (але не виключно)
1	<p><b>Електронний обмін даними</b> – електронний обмін торговими даними між підприємствами та митними органами для полегшення обробки та оформлення товарів до прибуття</p>	<ul style="list-style-type: none"> <li>• удосконалення механізму “Єдиного вікна для міжнародної торгівлі, в т. ч. гармонізація інтерфейсу з ЄС</li> <li>• розвиток служби підтримки бізнесу (Help Desk)</li> <li>• запровадження обміну попередньою інформацією про товари та транспортні засоби з державами-членами ЄС</li> <li>• взаємне визнання митного контролю митними службами України та суміжних держав</li> <li>• розробка автоматизованої системи митного оформлення «Центр» (АСМО.Центр)</li> <li>• оновлення національної системи гарантій (GMS-UA)</li> <li>• впровадження системи прийняття митних рішень (CDS)</li> </ul>
2	<p><b>Автоматизовані системи митного оформлення</b> – використання автоматизації, штучного інтелекту та машинного навчання для спрощення митних процедур, зменшення паперової роботи та прискорення процесу оформлення</p>	<ul style="list-style-type: none"> <li>• збільшення кількості One-Stop Border Posts («Спільний контроль№)</li> <li>• застосування NCTS 5, 6</li> <li>• розробка IT-платформи Customs Decision Making для АЕО</li> <li>• пріоритетний пропуск вантажів NCTS, АЕО</li> <li>• функціонування програмно-аналітичних модулів для автоматизації митних формальностей</li> <li>• автоматизація контролю правильності класифікації товарів та виявлення порушень, пов’язаних із наданням недостовірних відомостей про код товарів згідно з УКТ ЗЕД</li> </ul>
3	<p><b>Системи управління ризиками</b> – впровадження систем цілеспрямованого аналізу ризиків для ідентифікації високоризикових вантажів для подальшої перевірки, дозволяючи швидко пропускати вантажі з низьким ризиком</p>	<ul style="list-style-type: none"> <li>• приведення процедури проведення аналізу ризиків у відповідність з європейською моделлю CIRAM 2.1</li> <li>• розвиток спроможностей підрозділів з аналізу та оцінки ризиків, включаючи IT-системи для покращення обміну інформацією між стейкхолдерами ПП</li> <li>• запровадження IT-рішень для забезпечення автоматизації процесу аналізу і профілювання ризиків</li> </ul>

		<ul style="list-style-type: none"> <li>• запровадження системи боротьби з підробкою та піратством (COPIS)</li> </ul>
4	<p><b>Технології відстеження і контролю</b> – використання таких технологій, як RFID, GPS і блокчейн для відстеження руху товарів у режимі реального часу, підвищуючи видимість і безпеку в ланцюгу постачання</p>	<ul style="list-style-type: none"> <li>• вдосконалення Черги перетину кордону</li> <li>• функціонування Автоматичного розпізнавання номерних знаків у ПП</li> <li>• встановлення GPS-трекерів на транспортні засоби</li> <li>• забезпечення посадових осіб Держмитслужби індивідуальними портативними відеокамерами</li> </ul>
5	<p><b>Передові технології обробки зображень і сканування</b> – розгортання рентгенівських сканерів, сканерів гамма-променів та інших технологій обробки зображень для безконтактної перевірки товарів на контрабанду або незаконні предмети</p>	<ul style="list-style-type: none"> <li>• забезпечення ПП стаціонарними сканерами</li> <li>• забезпечення митниць мобільними скануючими системами</li> <li>• створення центральної бази зображень, отриманих зі скануючих систем стаціонарного та мобільного типу.</li> </ul>
6	<p><b>Інтегровані інформаційні системи</b> – інтеграція різних джерел даних та систем для забезпечення безперервного обміну інформацією між митними органами, прикордонними службами та іншими зацікавленими сторонами</p>	<ul style="list-style-type: none"> <li>• спільне використання контролюючими службами електронних даних у ПП</li> <li>• впровадження Єдиної інформаційної системи митних органів</li> <li>• модернізація інтегрованої міжвідомчої інформаційно-комунікаційної системи “Аркан” та відомчих ІТ-систем, забезпечення інтероперабельності систем та опрацювання регламентів взаємодії між стейкхолдерами.</li> </ul>
7	<p><b>Платформи для співпраці</b> – створення платформ для обміну інформацією та співпраці між урядовими установами, приватним сектором та міжнародними партнерами для сприяння торгівлі та безпеці кордонів</p>	<ul style="list-style-type: none"> <li>• функціонування платформ: Українсько-румунська робоча група з митних та інфраструктурних питань, Координаційний центр ІУК, Міжвідомча робоча група з питань координації ІУК, тощо.</li> <li>• розробка Стратегії розвитку та розбудови прикордонної інфраструктури</li> <li>• моделі управління ПП, зокрема можливості для державно-приватного партнерства.</li> </ul>