ПУБЛІЧНЕ УПРАВЛІННЯ У СФЕРІ ДЕРЖАВНОЇ БЕЗПЕКИ ТА ОХОРОНИ ГРОМАДСЬКОГО ПОРЯДКУ

УДК 351.746.1
DOI https://doi.org/10.32838/TNU-2663-6468/2021.5/09

Віхтюк А.В.
Державна прикордонна служба України

НАУКОВО-ПРАКТИЧНІ ПІДХОДИ ДО АВТОМАТИЗАЦІЇ ПРОЦЕСІВ ІНФОРМАЦІЙНОГО СПІВРОБІТНИЦТВА В ІНТЕГРОВАНОМУ УПРАВЛІННІ КОРДОНАМИ

В умовах динамічної трансформації світового політичного та економічного простору розширюється спектр загроз і викликів національній безпеці України, зокрема у прикордонній сфері.

Активізація міжнародного тероризму, прояви гібридних загроз, розвиток торгівлі людьми, незаконного переміщення через кордон осіб, наркотрафіку, незаконного обігу зброї, боєприпасів, вибухових речовин, поширення зброї масового ураження, екологічно небезпечних речовин тощо зумовлюють необхідність посилення співпраці правоохоронних органів, зокрема у сфері прикордонної безпеки.

Одним із напрямів вирішення зазначеного питання є створення ефективної системи інформаційної взаємодії між правоохоронними органами як на національному, так і на міжнародному рівнях.

Це потребує дієвої обробки інформації, створення та розвитку системи інформаційно-аналітичного забезпечення інтегрованого управління кордонами.

Стратегією інтегрованого управління кордонами на період до 2025 р. визначено суб'єкти, які взаємодіють на міжвідомчому, державному та міжнародному рівнях для досягнення цілей державної політики у сфері інтегрованого управління кордонами. Для дієвої координації їх діяльності потрібні ефективні механізми, які б результативно забезпечували обмін інформацією, необхідною для протидії наявним і потенційним загрозам національній безпеці України на державному кордоні. Створення таких механізмів стає актуальним науковим завданням у контексті виконання задекларованих у Стратегії інтегрованого управління кордонами стратегічних цілей щодо розв'язання проблем у сфері інформаційної міжвідомчої взаємодії.

Вирішення цього питання потребує запровадження інноваційних технологій, методів аналізу інформації, інформаційної взаємодії, прогнозування розвитку ситуацій у сфері прикордонної безпеки, використання додаткових людських і фінансових ресурсів для здійснення інформаційно-аналітичної діяльності.

У статті розглянуто науково-практичні підходи до автоматизації процесів інформаційного співробітництва в інтегрованому управлінні кордонами на основі використання сучасних інформаційно-комунікаційних технологій.

Ключові слова: *інтегроване управління кордонами, інформаційне співробітництво, інформаційно-комунікаційні технології, автоматизація процесів, національна безпека, безпека державного кордону.*

Постановка проблеми. Із 2010 р. в Україні впроваджуються європейські механізми у сферу прикордонної безпеки – інтегроване управління кордонами (далі – ІУК).

Із часом, у процесі розвитку ІУК, збільшилося коло його суб'єктів. Зокрема, у 2010–2015 рр. безпосередньо до реалізації державної політики у сфері ІУК залучалися чотири державні органи. У 2015–2021 рр. їх кількість збільшилася до дванадцяти.

Координація діяльності цих суб'єктів здійснюється за допомогою інформаційного співробітництва, яке забезпечує своєчасний обмін актуальною інформацією, що необхідна для протидії наявним і потенційним загрозам національній безпеці України на державному кордоні.

Наразі залучення нових суб'єктів ІУК призвело до значного збільшення масивів інформації, що циркулює між ними й обробка якої вимагає застосування сучасних засобів автоматизації.

Аналіз останніх досліджень і публікацій. Окремим питанням інформаційного співробітництва у сфері ІУК приділяли увагу у своїх дослідженнях С. Дейнеко, Ю. Дем'янюк, О. Деркач, О. Діденко, Д. Дягель, М. Литвин, Г. Магась, А. Махнюк, О. Мейко, О. Морохов, І. Катеринчук, В. Кириленко, Д. Купрієнко, В. Нікіфоренко, А. Сіцінський, О. Ставицький та інші. Але науково-практичні підходи до автоматизації процесів інформаційного співробітництва в ІУК ще не отримали свого вивчення і потребують комплексного дослідження, особливо в контексті задекларованих у Стратегії інтегрованого управління кордонами на період до 2025 р. стратегічних цілей щодо розв'язання проблем у сфері інформаційних відносин між суб'єктами ІУК [1].

Крім того, сучасне законодавство України [2–4] вимагає від прикордонної інституції вдосконалення інформаційного співробітництва на міжвідомчому та міжнародному рівнях.

Постановка завдання включає розробку науково-практичних підходів до автоматизації процесів інформаційного співробітництва в інтегрованому управлінні кордонами на основі використання сучасних інформаційно-комунікаційних технологій.

Виклад основного матеріалу дослідження. Сучасні інформаційно-комунікаційні технології дозволяють побудувати ефективні системи автоматизації процесів інформаційного співробітництва в ІУК на центральному та регіональному рівнях.

Основою таких систем стають програмно-технічні компоненти, завданням яких є забезпечення необхідного рівня якості управлінських рішень, які приймаються завдяки раціональному використанню наявних інформаційних ресурсів [5].

Із 2011 р. адміністрацією Державної прикордонної служби України проводиться планова робота для налагодження обміну відкритою статистичною та аналітичною інформацією з правоохоронними органами України та прикордонними відомствами іноземних держав.

Метою обміну інформацією є забезпечення надійної взаємодії з питань охорони державного кордону, спільної протидії незаконній міграції та іншим проявам транснаціональної організованої злочинності.

Щодо іноземних держав, то такий обмін уже здійснюється на підставі двосторонніх домовленостей із прикордонними відомствами Білорусі, Польщі, Угорщини, Словаччини, Румунії, Молдови та Німеччини. Наразі тривають консультації щодо майбутнього запровадження такого обміну з прикордонними інституціями Грузії та Азербайджану.

Обмін інформацією здійснюється за допомогою надсилання повідомлень на офіційні електронні адреси визначених контактних осіб.

Аналіз практичного використання запровадженого обміну інформацією свідчить про певні труднощі, які з'являються внаслідок зміни контактних осіб, що унеможливлює своєчасне реагування на раптово виниклі загрози. Крім цього, відсутність автоматизованого централізованого зберігання отриманої інформації ускладнює її обробку та унеможливлює її пошук.

На думку автора, практична площина у контексті створення сучасних механізмів інформаційного співробітництва в ІУК починається саме з автоматизації процесів й охоплює центральний та регіональний рівні.

На центральному рівні передбачається обмін інформацією в межах міжвідомчого та міжнародного співробітництва.

На регіональному рівні передбачається запровадження в оперативно-службову діяльність органів охорони кордону результатів аналізу ризиків – профілювання ризиків.

Ефективним рішенням щодо автоматизації процесів інформаційного співробітництва в ІУК може бути створення на основі принципів хмарних технологій «Інформаційної мережі комплексного управління кордонами».

Хмарні технології – це спеціальні технології розподіленого зберігання та обробки цифрових даних, за допомогою яких електронні ресурси надаються користувачеві як онлайн-сервіс. Програми запускаються і видають результати роботи у веббраузері на клієнтському персональному комп'ютері. При цьому всі необхідні для роботи програми та їхні дані знаходяться на віддаленому інтернет-сервері й тимчасово кешуються на клієнтській стороні (віддаленому робочому місці) [6].

Дані зберігаються та обробляються у так званій «хмарі», яка становить, на погляд клієнта, один великий віртуальний сервер. Фізично такі сервери географічно віддалені один від одного.

«Хмара» (від англ. cloud computing – хмарні обчислення даних) – онлайн-модель забезпечення на вимогу зручного мережевого доступу до дея-

кого загального фонду сконфігурованих обчислювальних ресурсів (наприклад, мереж передачі даних, серверів, пристроїв зберігання даних, додатків та сервісів як разом, так і окремо), які можуть бути оперативно надані користувачеві за мінімальних експлуатаційних витрат або звернень до провайдера [6].

Щодо інформаційного співробітництва в ІУК, то тут «Інформаційна мережа комплексного управління кордонами» дасть змогу забезпечити:

– централізовану обробку інформаційних потоків із відстеження динаміки міграційних процесів у режимі реального часу;

– термінове реагування на загрози, що виникають, організацію та супровід спільних заходів (операцій, проєктів);

– координацію діяльності контактних аналітичних центрів і проведення всебічного аналізу та оцінки ризиків.

Інформаційна мережа має забезпечувати обмін, накопичення та доступ до:

– статистичної інформації за визначеними формами;

– статистичних бюлетенів основних результатів оперативно-службової діяльності (за квартал, півріччя, рік);

– профілів ризиків та уточнених індикаторів;

– інформаційних повідомлень про нові способи протиправної діяльності;

– інформаційних повідомлень про способи і характерні ознаки виявлених підроблених документів на право перетинання державного кордону;

– надсилання запитів (відповідей) для встановлення осіб, які причетні до протиправної діяльності; транспортних засобів, які використовуються, тощо;

– тематичних аналізів про стан і розвиток реальних та потенційних загроз національним інтересам держави, зокрема про можливість їх поширення через державний кордон;

– інформаційних повідомлень про нові та основні тенденції криміногенної ситуації щодо процесів незаконної міграції, торгівлі людьми, контрабанди (наркотичних засобів, отруйних, сильнодіючих і вибухових речовин, зброї та боєприпасів, матеріальних цінностей тощо); про фактори, які впливають на їх розвиток;

– узагальнених даних щодо активності поза межами прикордонних контрольованих районів організованих злочинних груп, діяльність яких проявляється на державному кордоні;

– інформаційних повідомлень про елементи оперативної ситуації на державному кордоні та в прикордонних районах, що можуть впливати на надійність їх охорони та на зростання злочинних проявів у них;

– результатів моніторингу чинників, які негативно впливають на загальний стан прикордонної безпеки;

– інформаційних повідомлень про пункти пропуску через державний кордон, які використовуються злочинними елементами в «сірих» схемах контрабандної діяльності, зокрема суб'єктами зовнішньоекономічної діяльності;

– інших інформаційно-аналітичних матеріалів в інтересах вирішення завдань з протидії злочинності на державному кордоні.

На регіональному рівні інформаційного співробітництва в ІУК важливим елементом є запровадження в оперативно-службову діяльність органів охорони кордону результатів аналізу ризиків – профілювання.

Профілювання ризиків – це сукупність способів і методик із оцінки ризиків. Під профілем ризику розуміють документ, що відображає сукупність інформації про загрозу, індикатори ризику та визначає порядок дій службових осіб Держприкордонслужби у разі їх виявлення [7].

Запровадження профілювання ризиків дає змогу забезпечити ухвалення обґрунтованих управлінських рішень за умов бюджетних та ресурсних обмежень і водночас підвищити ефективність оперативно-службової діяльності підрозділів охорони кордону та створити комфортні умови щодо перетинання державного кордону особами, які не становлять загрози у сфері прикордонної безпеки [8].

Профілювання ризиків спрямоване на інформаційно-аналітичну підтримку персоналу, який безпосередньо несе службу на державному кордоні і передбачає обробку значного масиву інформації в стислий період часу, що апріорі вимагає застосування засобів автоматизації.

Наразі в адміністрації Державної прикордонної служби України розроблено вимоги до програмного комплексу (далі – ПК) автоматизації профілювання ризиків у пунктах пропуску через державний кордон.

ПК автоматизації профілювання ризиків створюється як складник інформаційно-телекомунікаційної системи прикордонного контролю.

Об'єктом ПК автоматизації профілювання ризиків є інформація, що обробляється в інформаційно-телекомунікаційній системі прикордонного контролю. Зокрема, відомості про:

– іноземців та осіб без громадянства, яким заборонено в'їзд в Україну;

– іноземців держав із безвізовим порядком в'їзду, які перевищили дозволений термін перебування в Україні;

– осіб, стосовно яких є доручення уповноважених державних органів;

– осіб, які перебувають у міжнародному розшуку;

– викрадені, втрачені та оголошені недійсними документи і транспортні засоби, які перебувають у міжнародному розшуку (зокрема, «Інтерполом»);

– боржників, яких тимчасово обмежено у праві виїзду з України;

– громадян України, які впродовж доби перетинають державний кордон України більше одного разу;

– осіб, відбитки пальців яких належать громадянам із переліку країн міграційного ризику;

– інформацію МЗС України з центральної підсистеми «Віза-ЦП»;

– інформацію СБУ з «Реєстру дозволів для переміщення в районі ООС».

Система ПК автоматизації профілювання ризиків складається з:

– центральної підсистеми;

– вебсервера (Risk Broker) обробки запитів;

– системи адміністрування ПК автоматизації профілювання ризиків;

– автоматизованих робочих місць користувачів (далі – АРМ).

Основою ПК автоматизації профілювання ризиків є спеціальний програмний модуль (далі – СПМ) у складі центральної підсистеми прикордонного контролю.

СПМ забезпечує:

– створення Правил профілів ризику та керування ними (Profiler);

– генерацію автоматичного сповіщення про виявлені ризики і надсилання попередження через вебсервер (Risk Broker) на відповідний АРМ користувача для своєчасного вжиття необхідних заходів;

– формування звітів на основі будь-яких профілів та індикаторів ризиків.

Вебсервер (Risk Broker) обробки запитів, які надходять з АРМ користувачів, забезпечує: пошук збігів, відповідно до Правил профілів ризику; класифікацію ризиків, обробку та внесення їх до СПМ.

Система адміністрування ПК автоматизації профілювання ризиків має забезпечувати:

– адміністрування та технічну підтримку користувачів;

– ведення системного журналу функціонування ПК;

– аудит дій користувачів;

– формування повідомлень про потенційні та фактичні порушення політики безпеки ПК.

АРМ користувачів відповідальні за обробку інформації в СПМ та формують статистичні/аналітичні звіти за будь-якими критеріями профілів/індикаторів ризику (особою, індикатором, датою, часом спрацювання, пунктом пропуску, органом охорони державного кордону, ділянкою кордону, напрямом перетину тощо).

АРМ користувачів мають бути оснащені спеціальним програмним забезпеченням, інтегрованим із вебсервером (Risk Broker).

Алгоритм роботи користувачів АРМ у пунктах пропуску через державний кордон України під час здійснення прикордонного контролю осіб визначається розпорядчими документами адміністрації Державної прикордонної служби України.

СПМ має забезпечувати обробку даних в онлайн-режимі, що містять відомості про осіб, які перетинають державний кордон.

СПМ встановлюється на сервері додатків (сервісі доступу) центральної підсистеми і забезпечує зіставлення установчих даних осіб з електронними шаблонами профілів ризику, відповідно до визначеного алгоритму використання СПМ і спеціального програмного забезпечення на АРМ користувачів посадових осіб, що здійснюють прикордонний контроль у пунктах пропуску через державний кордон.

СПМ також має забезпечувати зіставлення даних в онлайн-режимі, що зберігаються в інформаційному ресурсі з профілювання ризиків, за одним із обов'язкових реквізитів у сукупності з іншими реквізитами або без такої: прізвищем та ім'ям особи (латинські літери, 90% збігу, обов'язковий); серією та номером паспортного документа (латинські літери, арабські цифри, 100% збіг, обов'язковий); громадянством особи (100% збіг); статтю особи (100% збіг); датою народження особи (день, місяць, рік, наприклад, «01.01.2001», 100% збіг); віком особи.

Користувачами ПК автоматизації профілювання ризиків є: адміністратор/оператор, користувач/інспектор.

Оператором ПК автоматизації профілювання ризиків є персонал відділу аналізу та профілювання ризиків управління аналітичного забезпечення, стратегічного і поточного планування Департаменту організації роботи, планування та контролю адміністрації Державної прикордонної служби України.

Умови доступу до ПК автоматизації профілювання ризиків – автоматизоване робоче місце «Користувач», яке підключене до захищеної мережі Державної прикордонної служби України або до відкритої мережі з використанням програмних засобів криптографічного захисту інформації.

Авторизація у ПК автоматизації профілювання ризиків здійснюється за допомогою кваліфікованого електронного підпису.

Шаблон для створення типового електронного профілю ПК автоматизації профілювання ризиків (адміністратором або оператором програмного комплексу) наведений у табл. 1.

Таблиця 1

Перелік даних і додаткових реквізитів, за якими формується шаблон електронного профілю ризиків

№	Назва полів шаблону «Є-Профіль»	Зміст заповнення поля «Є-Профіль»	Примітка
1	2	3	4
І. ЗАГАЛЬНІ ВІДОМОСТІ ПРО ПРОФІЛЬ ПК «Є-ПРОФІЛЬ»			
1.	Напрям застосування	– в'їзд; – виїзд; – в'їзд/виїзд.	Класифікатори з ІТС ПК «Гарт-1»
2.	Назва профілю	«Нелегальна міграція 032019»	
3.	Тип реагування за профілем	Збіг – Реагування	Порядок дій інспектора прикордонної служби
		Збіг – Інформування	Додаткова інформація для інспектора щодо прийняття рішення про пропуск
		Збіг – Приховане інформування	Спрацювання без інформування інспектора
3.1	Попередження	У разі виявлення провести заходи контролю 2-ї лінії, звернути увагу на…	Деталі про спрацювання, додаткова інформація, рекомендації інспектору щодо дій
3.2	Повідомлення		
3.3	Дія		
4.	Примітка	Поєднання профілів 01–04, притаманне для західної ділянки кордону	Примітка адміністратора/оператора, відповідального за створення профілю
5.	Тип/умови профілю	Складний – поєднаний. Простий	Спрацювання за результатами виконання умов профілю. Приклад: марка ТЗ «БМВ», 4 особи, віком 20–25 років
5.1	Кратність спрацювання	1…9999	Спрацювання на особу за умови вибору «Складного та поєднаного профілю»
6.	Період дії профілю	Із 01.01.2020 р. по 01.01.2021 р.	Період, дата та час активації профілю
7.	Термін дії профілю	До 10.02.2020 р.	Термін дії профілю
8.	Модифікація профілю	01.01.2020 р. 16:00 Петренко П.П.	Позначка про модифікацію профілю
ІІ. УМОВИ СКЛАДНОГО – ПОЄДНАНОГО ПРОФІЛЮ ВІДОМОСТЕЙ ПРО ТЗ			
9.	Тип ТЗ	Легковий, вантажний, автобус тощо.	Класифікатори з ІТС ПК «Гарт-1», довідник «Види (типи) транспорту»
10.	Маршрут, рейс	177 «Київ – Вільнюс»	Класифікатори з ІТС ПК «Гарт-1», поле «Рейс» Нечіткий пошук
11.	Марка	«БМВ», «Ауді» тощо.	Класифікатори з ІТС ПК «Гарт-1», довідник «Марки АТЗ»
12.	VIN-код ТЗ	SUPTF1234567890	
13.	Державний номер ТЗ	АА1234АА	
14.	Дата виготовлення або період	2015 р. або період з 2014–2016 рр.	
15.	Країна реєстрації	Україна	Класифікатори з ІТС ПК «Гарт-1», довідник «Держави»
16.	Колір	Білий	Класифікатори з ІТС ПК «Гарт-1», довідник «Кольори АТЗ»

Закінчення табл. 1

1	2	3	4
III. УМОВИ СКЛАДНОГО – ПОЄДНАНОГО ПРОФІЛЮ ВІДОМОСТЕЙ ПРО ОСОБУ (ДОКУМЕНТ)			
17.	Тип документа	Закордонний, внутрішній паспорти, посвідчення моряка тощо	Класифікатори з ІТС ПК «Гарт-1», довідник «Типи паспортів»
18.	Країна видачі документа	Україна	Класифікатори з ІТС ПК «Гарт-1», довідник «Держави»
19.	Дата видачі документа	25.03.2018 р.	Відомості про дату видачі документа зчитуємо в «SDK REGULA» СПЗ Є-Інспектор
20.	Регіон видачі документа		Відомості про місце видачі документа – у СПЗ Є-Інспектор («SDK REGULA»)
21.	Прізвище	Петренко; Петр***	Нечіткий пошук
22.	Ім’я	Петро; ***тро	Нечіткий пошук
23.	Серія, номер документа	АА123456; АА123***	Нечіткий пошук
24.	Громадянство	Україна; Україна або Ізраїль	Класифікатори з ІТС ПК «Гарт-1», довідник «Держави»
25.	Дата народження	01.01.1980 р.	
25.1	Вік Вік з – по	23 роки; 22–28 років	
26.	Стать	Чол.	Класифікатори з ІТС ПК «Гарт-1»
27.	Кратність перетину кордону	2 за добу	Онлайн-сервіс «Подвійний перетин» ІТС ПК «Гарт-1»
28.	ІПН, УНЗР	1234567890	
IV. УМОВИ СКЛАДНОГО – ПОЄДНАНОГО ПРОФІЛЮ ВІДОМОСТЕЙ ПРО ВІЗУ			
29.	Номер візи	Y12345678	
30.	Тип візи	Приватна, туризм, освіта тощо	Класифікатори з ІТС ПК «Гарт-1», довідник «Мета поїздки (типи віз)»
31.	Країна видачі	Україна	Класифікатори з ІТС ПК «Гарт-1», довідник «Держави»
V. СПРАЦЮВАННЯ У ВИЗНАЧЕНИХ ПУНКТАХ ПРОПУСКУ (КОНТРОЛЮ) ТА КПВВ			
32.	№ вузла ППр	400	Класифікатори з ІТС ПК «Гарт-1»
33.	Назва ППр	Бориспіль	Класифікатори з ІТС ПК «Гарт-1»
34.	Тип ППр	Повітряного сполучення	Класифікатори з ІТС ПК «Гарт-1»

Користувачем ПК автоматизації профілювання ризиків є персонал зміни прикордонних нарядів органів охорони державного кордону Державної прикордонної служби України, який в установленому порядку призначений та несе службу в прикордонному наряді «Перевірка документів» та «Старший прикордонного наряду».

Умови доступу до ПК автоматизації профілювання ризиків – АРМ «Інспектор» зі складу інформаційно-телекомунікаційної системи «Гарт-1/П», яке підключене до захищеної мережі Державної прикордонної служби України або до відкритої мережі з використанням програмних засобів криптографічного захисту інформації «Захист з’єднань-2».

Перелік даних і додаткових реквізитів інформаційного повідомлення за результатами спрацювання ПК автоматизації профілювання ризиків на першій лінії контролю у пункті пропуску (контролю), на контрольному посту в’їзду-виїзду наведений у табл. 2.

СПМ має реалізовувати такі функціональні завдання:

– авторизацію користувачів Державної прикордонної служби України для отримання доступу до бази даних ПК автоматизації профілювання ризиків;

– приймання даних про особу та передавання цих даних до серверів додатків (сервісу доступу), серверів баз даних центральної підсистеми з установленим СПЗ для отримання відповідей про результати проведених перевірок, надсилання та відображення відповідей користувачам на АРМ з установленим СПЗ;

– реєстрацію прийнятих даних і наданих повідомлень щодо результатів перевірки наявності/

Таблиця 2

Перелік даних і додаткових реквізитів інформаційного повідомлення за результатами спрацювання ПК автоматизації профілювання ризиків на першій лінії контролю у пункті пропуску (контролю), на контрольному посту в'їзду-виїзду

№	Назва полів шаблону «Є-Профіль»	Зміст заповнення поля «Є-Профіль»	Примітка
1.	Назва профілю	Нелегальна міграція 032019	
2.	Попередження	У разі виявлення провести заходи контролю 2-ї лінії, звернути увагу на…	Деталі про спрацювання, додаткова інформація. Рекомендації інспектору щодо дій
3.	Повідомлення		
4.	Дія		

відсутності збігів установчих даних про особу з електронними шаблонами профілів ризику;

– реєстрацію та надсилання користувачам АРМ у пунктах пропуску через державний кордон текстових повідомлень за типами реагування («Збіг – Реагування», «Збіг – Інформування», «Збіг – Приховане інформування»), відповідно до умов електронного профілю;

– зберігання записів системних журналів упродовж установленого терміну та автоматичне їх видалення після закінчення такого терміну;

– перегляд результатів обробки даних із можливістю складання звітів;

– перегляд системних журналів.

СПМ повинен включати вебсервіси та засоби забезпечення взаємодії користувачів ПК автоматизації профілювання ризиків.

Базовий алгоритм роботи сервісу складається з таких дій:

– приймання запиту на пошук від користувача;

– обробки запиту;

– реєстрації запиту в системному журналі;

– формування запиту до інформаційного ресурсу з електронного профілювання ризиків;

– отримання відповіді від інформаційного ресурсу електронного профілювання ризиків, реєстрації відповіді в системному журналі;

– формування, передавання та відображення відповіді користувачу ПК автоматизації профілювання ризиків.

СПМ має взаємодіяти з СПЗ та використовувати сервіси СПЗ для автоматичної обробки та порівняння установчих даних осіб з даними електронного профілю ризиків ПК автоматизації профілювання ризиків.

СПМ має завантажуватись автоматично та перебувати у стані штатного функціонування.

Вимоги до СПЗ автоматизації профілювання ризиків, що встановлюється і використовується на АРМ користувачів у пунктах пропуску через державний кордон:

1. СПЗ має здійснювати автоматизовану обробку даних про осіб і взаємодіяти з СПМ для забезпечення доступу до ПК автоматизації профілювання ризиків на контролі першої та другої ліній під час прикордонного оформлення і пропуску осіб через державний кордон.

2. У СПМ та СПЗ автоматизації профілювання ризиків реалізовується підтримка двостороннього інформаційного обміну з сервісами СПМ для обробки інформації в базі даних ПК автоматизації профілювання ризиків.

СПМ та СПЗ автоматизації профілювання ризиків повинні реалізовувати такі функціональні завдання:

– формування загальносистемного ідентифікатора факту реєстрації особи під час проходження прикордонного контролю (ID-номер запису);

– зчитування паспортного документа – отримання текстової та біометричної інформації, яка наведена у паспортному документі;

– автоматичну та інтерактивну візуальну ідентифікацію установчих текстових даних особи за такими оперативними базами даних, як:

1) «Відомості про осіб, яким заборонено в'їзд в Україну»;

2) «Відомості про осіб, стосовно яких є доручення уповноважених державних органів»;

3) «Загублені, викрадені та оголошені недійсними документи»;

4) «Оформлені перепустки»;

5) «Відомості про осіб, яким оформлені візи України»;

6) «Відомості про осіб, яким заборонено в'їзд в Україну органами охорони державного кордону»;

7) «Ризик_Особи»;

8) «Ризик_Перетин»;

9) банки даних «Інтерполу»;

– записування до відповідних розділів Бази даних осіб облікової інформації про особу, зокрема:

1) текстової інформації про особу;

2) результатів прикордонного контролю щодо особи («Пропуск», «Непропуск», «Контроль другої лінії»);

– передавання та записування актуальної інформації до Бази даних осіб центрального сховища даних центральної підсистеми прикордонного контролю Державної прикордонної служби України.

Для реалізації вищезазначених функціональних завдань необхідно розширити функціональні можливості інформаційно-телекомунікаційної системи прикордонного контролю «Гарт-1/П» та центральної підсистеми «Гарт-1/ЦП», зокрема щодо забезпечення автоматизованого зіставлення (порівняння даних) за електронними профілями ризиків.

Базовий алгоритм роботи СПМ і СПЗ на в'їзд в Україну та виїзд з України повинен включати такі дії на контролі першої та/або другої ліній:

– під час проведення процедури автоматичного зчитування даних із візуальної частини сторінок паспортного документа, машинозчитуваної зони та електронного чипа, вмонтованого в паспорт, відомостей про транспортний засіб із використанням СПЗ здійснюється автоматичний запит до ПК автоматизації профілювання ризиків;

– у центральній підсистемі проводиться процедура зіставлення установчих даних особи та відомостей про транспортний засіб із даними шаблону електронного профілю ризиків ПК автоматизації профілювання ризиків;

– результати перевірки (зіставлення) відображаються в СПЗ на АРМ користувача в пункті пропуску через державний кордон.

Загальна структура СПЗ визначається обраною технологією розробки.

СПЗ має виконувати функції у взаємодії з сервісами центральної підсистеми «Гарт-1/ЦП» інформаційно-телекомунікаційної системи прикордонного контролю «Гарт-1».

Висновки. Отже, впровадження «Інформаційної мережі комплексного управління кордонами» на центральному рівні дозволить забезпечити спільно з суміжними державами реалізацію концептуальних підходів до вирішення безпекових транскордонних питань з урахуванням «Принципів комплексного управління кордонами зовнішньої співпраці Європейської Комісії».

На регіональному рівні інформаційного співробітництва в ІУК автоматизація профілювання ризиків дозволить підвищити ефективність виконання покладених на підрозділи органів охорони державного кордону завдань з протидії тероризму, організованій злочинності та нелегальній міграції, підвищить рівень безпекового складника прикордонного контролю.

Упровадження ПК автоматизації профілювання ризиків дасть змогу скоротити час, що витрачається на процес їх профілювання.

Перспективи подальших досліджень у цьому напрямі полягають у вивченні спеціальних програмних засобів, які доцільно використовувати для забезпечення надійного захисту інформації в «Інформаційній мережі комплексного управління кордонами» та в ПК автоматизації профілювання ризиків, де оброблятиметься конфіденційна інформація.

Список літератури:

1. Про схвалення Стратегії інтегрованого управління кордонами на період до 2025 р. : розпорядження Кабінету Міністрів України від 24 серпня 2019 р. № 687-р. URL: https://zakon.rada.gov.ua/laws/show/687-2019-%D1%80#Text.

2. Про прикордонний контроль : Закон України. URL: https://zakon.rada.gov.ua/laws/show/1710-17#Text.

3. Про правовий статус іноземців та осіб без громадянства : Закон України. URL: https://zakon.rada.gov.ua/laws/show/3773-17#Text.

4. Про розвиток системи аналізу ризиків у Державній прикордонній службі України : Наказ адміністрації Державної прикордонної служби України від 26 грудня 2016 р. № 205.

5. Ліпінська А. Інформаційно-комунікаційні технології в організації інформаційно-аналітичного забезпечення державного управління. *Державне управління: удосконалення та розвиток.* 2015. № 10. URL: http://www.dy.nayka.com.ua/?op=1&z=908 (дата звернення: 20.08.2021).

6. Mell P., Grance T. The NIST Definition of Cloud Computing. Recommendations of the National Institute of Standards and Technology. NIST. URL: https://nvlpubs.nist.gov (дата звернення: 25.08.2021).

7. Про затвердження Інструкції з проведення аналізу ризиків у Державній прикордонній службі України : Наказ МВС України від 11 грудня 2017 р. № 1007, зареєстрований у Міністерстві юстиції України 22 січня 2018 р. за № 91/31543. URL: https://zakon.rada.gov.ua/laws/show/z0091-18#Text (дата звернення: 26.08.2021).

8. Махнюк А. Окремі підходи до запровадження аналізу та профілювання ризиків в інтегрованому управлінні кордонами. *Державне управління: удосконалення та розвиток.* 2012. № 2. URL: http://nbuv.gov.ua/UJRN/Duur_2012_2_4 (дата звернення: 26.08.2021).

Vikhtiuk A.V. SCIENTIFIC AND PRACTICAL APPROACHES TO AUTOMATION OF INFORMATION COOPERATION PROCESSES IN INTEGRATED BORDER MANAGEMENT

In the context of the dynamic transformation of the world political and economic space, the range of threats and challenges to Ukraine's national security is expanding, including in the border area.

Intensification of international terrorism, cases of hybrid threats, increase in human trafficking, illegal movement of persons across the border, drug trafficking, illicit trafficking in weapons, ammunition, explosives, proliferation of weapons of mass destruction, environmentally hazardous substances, etc., all these trends determine the need to strengthen law enforcement cooperation, including in the field of border security.

Creating an effective system of information cooperation between law enforcement agencies, both at the national and international levels is one of the solutions.

These measures require effective information management, creation and development of a system of information and analytical support for integrated border management.

The Strategy of Integrated Border Management for the period up to 2025 has identified entities that interact at the interagency, state and international levels to achieve the goals of state policy in the field of integrated border management. Effective coordination of their activities requires efficient mechanisms which would ensure the exchange of information necessary to counter existing and potential threats to Ukraine's national security at the state border. The creation of such mechanisms becomes an urgent scientific task in the context of the implementation of the strategic goals declared in the Strategy of Integrated Border Management concerning solving problems in the field of information interagency cooperation.

The introduction of innovative technologies, methods of information analysis, information interaction, forecasting the development of situations in the field of border security, the use of additional human and financial resources for information and analytical activities are necessary to solve the task.

Scientific and practical approaches to automation of information cooperation processes in integrated border management, based on the use of modern information and communication technologies, have been developed.

Key words: *integrated border management, information cooperation, information and communication technologies, process automation, national security, state border security.*