

Спеціальність: Менеджмент

Спеціалізація: Менеджмент

Освітньо-кваліфікаційний рівень: Магістр

Кваліфікаційна робота

на здобуття ступеня магістра

на тему:

**«Управління ризиками в системі Державної прикордонної служби
України»**

Студентка групи:

ТУяг-8-24-М1М (2.0 здс) _____ Кучеренко Неля Володимирівна
(підпис) (П.І.П. студента)

Наукових керівник _____ к.е.н. Гринчак Наталія Анатоліївна
(підпис) (посада, П.І.П.)

Допущено до захисту в ДЕК протокол № _____ від «__» _____ 2026 р.

Завідувач кафедри: _____ к.е.н. Грицай Віктор Григорович
(підпис) (звання, П.І.П.)

МІЖРЕГІОНАЛЬНА АКАДЕМІЯ УПРАВЛІННЯ ПЕРСОНАЛОМ

(повне найменування вищого навчального закладу)

Кафедра Економіки, фінансів та менеджменту

Освітньо-кваліфікаційний рівень - магістр

Галузь знань 07 «Управління та адміністрування»

Спеціальність 073 «Менеджмент»

ЗАТВЕРДЖУЮ

Завідувач кафедри _____

“ ____ ” _____ 20__ року

ЗАВДАННЯ НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТКИ

Кучеренко Нелі Володимирівни

(прізвище, ім'я, по батькові)

1. Тема проекту (роботи) «Управління ризиками в системі Державної прикордонної служби України»

керівник роботи _____

(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)

затверджені наказом вищого навчального закладу від “ ____ ” ____ 20__ року № ____

2. Строк подання студентом роботи _____

3. Вихідні дані до роботи _____

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити):

- дослідити сутність поняття «ризик» та класифікацію ризиків у системі управління;
- розглянути основні принципи та методи управління ризиками;
- визначити особливості управління ризиками в органах державної влади та сектору безпеки;
- надати загальну характеристику діяльності Державної прикордонної служби України;
- ідентифікувати основні види ризиків у діяльності ДПСУ;
- здійснити оцінку існуючої системи управління ризиками в ДПСУ;
- розробити напрями вдосконалення управління ризиками в діяльності служби;
- запропонувати практичні рекомендації щодо підвищення ефективності управління ризиками.

5. Перелік графічного матеріалу. Таблиці: Порівняльна характеристика ризику та невизначеності; Класифікація ризиків у системі управління; Основні принципи управління ризиками; Методи управління ризиками; Порівняльна характеристика управління ризиками в державному та приватному секторах; Ключові особливості управління ризиками в органах державної влади; Основні характеристики ДПСУ як

об'єкта управління; Класифікація пріоритетних корупційних ризиків у ДПСУ; Слабкі місця та обмеження діючої системи управління ризиками в ДПСУ; Основні технології ризик-менеджменту в діяльності ДПСУ; Основні напрями удосконалення організаційного управління ризиками в ДПСУ; Практичні рекомендації щодо мінімізації ризиків у ДПСУ. Рисунок: Місце ризику в системі управління організацією; Процес управління ризиками в організації; Особливості системи управління ризиками в органах державної влади; ДПСУ як об'єкт управління; Взаємозв'язок ризиків у діяльності ДПСУ; Модель технологічно орієнтованої системи управління ризиками в ДПСУ; Організаційна модель управління ризиками в ДПСУ; Основні напрями мінімізації ризиків у ДПСУ; Етапи впровадження системи управління ризиками в ДПСУ.

6. Консультанти розділів роботи

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Розділ 1			
Розділ 2			
Розділ 3			

7. Дата видачі завдання _____

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів магістерської роботи	Строк виконання	Примітка
1	Вибір теми і об'єкта дослідження, затвердження теми		
2	Опрацювання літературних джерел і складання попереднього плану роботи		
3	Розробка завдання на дипломну роботу, складання календарного плану виконання		
4	Збирання фактичного матеріалу під час переддипломної практики на об'єкті дослідження		
5	Обробка фактичного матеріалу		
6	Написання першого варіанту тексту, подання його на ознайомлення науковому керівникові		
7	Усунення зауважень, робота над кінцевим варіантом тексту, літературне та технічне оформлення дипломної роботи		
8	Подання роботи на перевірку керівнику та отримання його відзиву		
9	Подання роботи на кафедру		
10	Зовнішнє рецензування роботи		
11	Підготовка доповіді та ілюстративного матеріалу для захисту роботи		

Студент

(підпис)

(прізвище та ініціали)

Керівник роботи

(підпис)

(прізвище та ініціал)

РЕФЕРАТ
на тему «Управління ризиками в системі Державної прикордонної
служби України»

Магістерська робота складає 80 сторінок. Робота містить 12 таблиць та 9 рисунків. Перелік використаних джерел налічує 77 найменувань.

У сучасних умовах трансформації системи національної безпеки України, зумовлених повномасштабною збройною агресією та зростанням гібридних загроз, особливого значення набуває ефективне управління ризиками у діяльності державних органів сектору безпеки і оборони. Державна прикордонна служба України виконує ключову функцію щодо забезпечення недоторканності державного кордону, протидії незаконній міграції, контрабандній діяльності, терористичним загрозам та іншим видам правопорушень. За таких умов ризики, що виникають у процесі діяльності служби, мають комплексний, багаторівневий характер і потребують системного управління.

Зростання інтенсивності загроз на державному кордоні, ускладнення безпекового середовища, необхідність оперативного реагування на кризові ситуації обумовлюють потребу у вдосконаленні механізмів ідентифікації, оцінювання та мінімізації ризиків. Водночас існуюча система управління ризиками в державних органах потребує подальшого розвитку з урахуванням сучасних управлінських підходів, цифровізації та інтеграції аналітичних інструментів.

Об'єктом дослідження є процес управління ризиками в діяльності державних органів.

Предметом дослідження є сукупність теоретичних, методичних та практичних аспектів управління ризиками в системі Державної прикордонної служби України.

Метою дипломної роботи є обґрунтування теоретичних засад та розробка практичних рекомендацій щодо удосконалення системи управління ризиками в діяльності Державної прикордонної служби України.

У роботі використано загальнонаукові та спеціальні методи дослідження, зокрема: методи аналізу і синтезу — для узагальнення теоретичних положень; системний підхід — для дослідження управління ризиками як цілісної системи; порівняльний метод — для оцінки динаміки ризиків; метод узагальнення — для формулювання висновків та рекомендацій.

Практичне значення одержаних результатів полягає у можливості використання запропонованих рекомендацій для підвищення ефективності функціонування системи управління ризиками в діяльності ДПСУ, зокрема у процесах виявлення, оцінювання та мінімізації загроз у сфері охорони державного кордону.

Ключові слова: управління ризиками, ризик-менеджмент, Державна прикордонна служба України, прикордонна безпека, система управління ризиками, інтегроване управління кордонами, цифровізація управління, ризик-орієнтований підхід, антикорупційний контроль, інформаційно-аналітичні системи, предиктивна аналітика, міжнародні стандарти безпеки, організаційне управління, мінімізація ризиків, безпекове середовище.

ABSTRACT
on the topic “Risk Management in the System of the State Border
Guard Service of Ukraine”

This master’s thesis consists of 80 pages. It contains 12 tables and 9 figures. The list of references includes 77 sources.

In the current context of the transformation of Ukraine’s national security system, driven by full-scale armed aggression and the rise of hybrid threats, effective risk management in the activities of state agencies in the security and defense sector has become particularly important. The State Border Guard Service of Ukraine performs a key function in ensuring the integrity of the state border, countering illegal migration, smuggling, terrorist threats, and other types of offenses. Under such conditions, the risks arising in the course of the service’s activities are complex and multi-layered in nature and require systematic management.

The increasing intensity of threats at the state border, the growing complexity of the security environment, and the need for rapid response to crisis situations necessitate the improvement of mechanisms for identifying, assessing, and mitigating risks. At the same time, the existing risk management system in government agencies requires further development, taking into account modern management approaches, digitalization, and the integration of analytical tools.

The object of the study is the risk management process in the activities of state agencies.

The subject of the study is the set of theoretical, methodological, and practical aspects of risk management within the system of the State Border Guard Service of Ukraine.

The aim of this thesis is to substantiate the theoretical foundations and develop practical recommendations for improving the risk management system in the activities of the State Border Guard Service of Ukraine.

The study employs general scientific and specialized research methods, including: methods of analysis and synthesis—to generalize theoretical provisions; a systems approach—to study risk management as an integrated system; the comparative method—to assess risk dynamics; and the generalization method—to formulate conclusions and recommendations.

The practical significance of the findings lies in the possibility of using the proposed recommendations to improve the effectiveness of the risk management system within the State Border Guard Service of Ukraine, particularly in the processes of identifying, assessing, and mitigating threats to state border security.

Keywords: risk management, State Border Guard Service of Ukraine, border security, risk management system, integrated border management, digitalization of management, risk-based approach, anti-corruption control, information and analytical systems, predictive analytics, international security standards, organizational management, risk minimization, security environment.

ЗМІСТ

ВСТУП.....	9
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ В ОРГАНІЗАЦІЯХ.....	12
1.1. Сутність ризику та його класифікація в системі управління	12
1.2. Принципи та методи управління ризиками	18
1.3. Особливості управління ризиками в органах державної влади та безпеки	26
Висновок до розділу 1	35
РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ В ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ УКРАЇНИ	37
2.1. Загальна характеристика діяльності ДПСУ як об'єкта управління.....	37
2.2. Основні види ризиків у діяльності ДПСУ	43
2.3. Оцінка діючої системи управління ризиками в ДПСУ	50
Висновок до розділу 2.....	57
РОЗДІЛ 3. НАПРЯМИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ В ДПСУ	59
3.1. Впровадження сучасних технологій ризик-менеджменту в Державній прикордонній службі України	59
3.2. Підвищення ефективності організаційного управління ризиками в ДПСУ	65
3.3. Розробка практичних рекомендацій щодо мінімізації ризиків у ДПСУ ..	71
Висновок до розділу 3.....	78
ВИСНОВКИ	80
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	82

ВСТУП

Актуальність теми дослідження. У сучасних умовах трансформації системи національної безпеки України, зумовлених повномасштабною збройною агресією та зростанням гібридних загроз, особливого значення набуває ефективне управління ризиками у діяльності державних органів сектору безпеки і оборони. Державна прикордонна служба України виконує ключову функцію щодо забезпечення недоторканності державного кордону, протидії незаконній міграції, контрабандній діяльності, терористичним загрозам та іншим видам правопорушень. За таких умов ризики, що виникають у процесі діяльності служби, мають комплексний, багаторівневий характер і потребують системного управління.

Зростання інтенсивності загроз на державному кордоні, ускладнення безпекового середовища, необхідність оперативного реагування на кризові ситуації обумовлюють потребу у вдосконаленні механізмів ідентифікації, оцінювання та мінімізації ризиків. Водночас існуюча система управління ризиками в державних органах потребує подальшого розвитку з урахуванням сучасних управлінських підходів, цифровізації та інтеграції аналітичних інструментів.

Теоретичні та прикладні аспекти управління ризиками широко висвітлені у працях вітчизняних і зарубіжних науковців. Проте питання адаптації інструментарію ризик-менеджменту до специфіки діяльності Державної прикордонної служби України залишаються недостатньо розробленими, що й обумовлює актуальність обраної теми.

Метою дипломної роботи є обґрунтування теоретичних засад та розробка практичних рекомендацій щодо удосконалення системи управління ризиками в діяльності Державної прикордонної служби України.

Для досягнення поставленої мети необхідно вирішити такі завдання:

- дослідити сутність поняття «ризик» та класифікацію ризиків у системі управління;

- розглянути основні принципи та методи управління ризиками;
- визначити особливості управління ризиками в органах державної влади та сектору безпеки;
- надати загальну характеристику діяльності Державної прикордонної служби України;
- ідентифікувати основні види ризиків у діяльності ДПСУ;
- здійснити оцінку існуючої системи управління ризиками в ДПСУ;
- розробити напрями вдосконалення управління ризиками в діяльності служби;
- запропонувати практичні рекомендації щодо підвищення ефективності управління ризиками.

Об'єктом дослідження є процес управління ризиками в діяльності державних органів.

Предметом дослідження є сукупність теоретичних, методичних та практичних аспектів управління ризиками в системі Державної прикордонної служби України.

Методи дослідження. У роботі використано загальнонаукові та спеціальні методи дослідження, зокрема: методи аналізу і синтезу — для узагальнення теоретичних положень; системний підхід — для дослідження управління ризиками як цілісної системи; статистичні методи — для аналізу показників діяльності ДПСУ; порівняльний метод — для оцінки динаміки ризиків; метод узагальнення — для формулювання висновків та рекомендацій.

Наукова новизна одержаних результатів полягає у подальшому розвитку теоретико-методичних підходів до управління ризиками в державних органах шляхом адаптації сучасних інструментів ризик-менеджменту до специфіки діяльності Державної прикордонної служби України.

Практичне значення одержаних результатів полягає у можливості використання запропонованих рекомендацій для підвищення ефективності

функціонування системи управління ризиками в діяльності ДПСУ, зокрема у процесах виявлення, оцінювання та мінімізації загроз у сфері охорони державного кордону.

Інформаційну базу дослідження становлять нормативно-правові акти України, офіційні матеріали та статистичні дані Державної прикордонної служби України, аналітичні звіти, наукові праці вітчизняних і зарубіжних авторів.

Структура роботи. Дипломна робота складається зі вступу, трьох розділів, висновків, списку використаних джерел та додатків.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ УПРАВЛІННЯ РИЗИКАМИ В ОРГАНІЗАЦІЯХ

1.1. Сутність ризику та його класифікація в системі управління

У сучасних умовах функціонування організацій ризик виступає невід'ємною складовою управлінської діяльності. Динамічність зовнішнього середовища, посилення економічної та політичної нестабільності, а також зростання безпекових загроз зумовлюють необхідність врахування ризиків у процесі прийняття управлінських рішень. Особливої актуальності це набуває для державних органів, діяльність яких пов'язана із забезпеченням національної безпеки.

Поняття «ризик» є складною та багатогранною категорією, що досліджується в межах різних наукових підходів. У загальному вигляді ризик визначається як імовірність настання події, яка може призвести до відхилення фактичних результатів від запланованих. Водночас сучасні підходи до трактування ризику розглядають його не лише як загрозу, але й як можливість отримання додаткових переваг. Такий підхід суттєво розширює зміст ризику та підвищує його значення у системі управління.

Сутність ризику тісно пов'язана з категорією невизначеності. Невизначеність виникає внаслідок неповноти інформації, складності прогнозування майбутніх подій та впливу великої кількості факторів зовнішнього середовища. Саме невизначеність формує передумови для виникнення ризиків. Водночас ризик, на відміну від невизначеності, піддається оцінюванню, що дозволяє здійснювати його управління [15].

З метою більш чіткого розмежування зазначених категорій доцільно порівняти ризик і невизначеність (табл. 1.1).

Таблиця 1.1

Порівняльна характеристика ризику та невизначеності

Критерій	Ризик	Невизначеність
Можливість оцінювання	Піддається кількісній або якісній оцінці	Не піддається точній оцінці
Ймовірність	Може бути визначена	Невідома або невизначена
Управління	Можливе через відповідні методи	Обмежене
Інформаційна база	Часткова або достатня	Недостатня

Важливо зазначити, що в сучасній практиці управління ризик розглядається не ізольовано, а в тісному взаємозв'язку з цілями організації. Це означає, що рівень ризику визначається не лише ймовірністю настання певної події, але й значущістю її наслідків для досягнення стратегічних і тактичних цілей. У зв'язку з цим управління ризиками набуває стратегічного характеру та інтегрується в загальну систему менеджменту організації.

Крім того, ризик має об'єктивно-суб'єктивну природу. З одного боку, він формується під впливом зовнішніх факторів, які не залежать від діяльності організації, з іншого — значною мірою залежить від якості управлінських рішень, рівня професійної підготовки персоналу та ефективності організаційної структури. Це підкреслює необхідність комплексного підходу до управління ризиками.

Таким чином, ризик є конкретизованою формою прояву невизначеності, що робить його об'єктом управлінського впливу.

Важливим аспектом дослідження ризику є визначення факторів, що зумовлюють його виникнення. У загальному вигляді всі фактори ризику можна поділити на зовнішні та внутрішні. До зовнішніх факторів належать політична нестабільність, економічні коливання, зміни законодавства, розвиток міжнародних відносин, а також безпекова ситуація. Внутрішні фактори пов'язані з особливостями функціонування організації, зокрема

рівнем кваліфікації персоналу, ефективністю управління, станом матеріально-технічної бази та організаційною структурою.

Взаємодія зазначених факторів формує складне середовище ризику, в якому функціонує організація. При цьому важливо враховувати, що зовнішні фактори, як правило, є менш контрольованими, тоді як внутрішні можуть бути скориговані шляхом удосконалення управлінських процесів. Це визначає необхідність системного аналізу середовища ризику при прийнятті управлінських рішень [23].

У системі управління ризик виконує важливу функціональну роль. Він впливає на всі етапи управлінського процесу — від планування до контролю, що зумовлює необхідність його врахування при формуванні управлінських рішень. Інтеграцію ризику в систему управління організацією доцільно представити у вигляді схеми (рис. 1.1).



Рис. 1.1. Місце ризику в системі управління організацією

Як видно зі схеми, ризик супроводжує всі управлінські процеси, що підтверджує його системний характер.

Слід підкреслити, що ризик не є окремим елементом управління, а пронизує всі його функції. На етапі планування ризику пов'язані з неточністю прогнозів та обмеженістю інформації; на етапі організації — з неефективним розподілом ресурсів; у процесі мотивації — з людським фактором; під час контролю — з можливістю відхилення фактичних результатів від запланованих показників. Такий комплексний вплив ризиків зумовлює необхідність їх системного врахування в управлінській діяльності.

З метою глибшого розуміння сутності ризику доцільно розглянути його основні властивості. По-перше, ризик має ймовірнісний характер, що означає неможливість точно передбачити момент і наслідки його реалізації. По-друге, він є об'єктивно-суб'єктивною категорією, оскільки формується під впливом як зовнішніх умов, так і управлінських рішень. По-третє, ризик характеризується альтернативністю, тобто можливістю різних варіантів розвитку подій.

Крім того, важливою властивістю ризику є його динамічність, що проявляється у зміні рівня ризику залежно від умов функціонування організації. У зв'язку з цим управління ризиками має здійснюватися на постійній основі з урахуванням змін зовнішнього та внутрішнього середовища [18].

Важливим аспектом дослідження ризику є його класифікація. Класифікація дозволяє впорядкувати різноманітні види ризиків, визначити їх джерела та обрати відповідні методи управління. У науковій літературі існує значна кількість підходів до класифікації ризиків, однак для цілей даного дослідження доцільно узагальнити їх за основними ознаками (табл. 1.2).

Таблиця 1.2

Класифікація ризиків у системі управління

Ознака класифікації	Види ризиків	Характеристика
За сферою виникнення	економічні, політичні, соціальні, безпекові	Визначають сферу формування ризиків
За джерелом виникнення	внутрішні, зовнішні	Зумовлені внутрішніми або зовнішніми факторами
За характером наслідків	негативні, позитивні, змішані	Вплив на результати діяльності
За ступенем впливу	допустимі, критичні, катастрофічні	Рівень можливих втрат
За можливістю управління	керовані, частково керовані, некеровані	Ступінь впливу суб'єкта управління

Необхідно також враховувати, що окремі види ризиків можуть взаємодіяти між собою, утворюючи комплексні ризикові ситуації. Наприклад, економічні ризики можуть спричиняти соціальні наслідки, а політичні — впливати на безпекову ситуацію. Така взаємозалежність ускладнює процес управління ризиками та потребує використання інтегрованих підходів до їх оцінювання.

У контексті діяльності державних органів особливу роль відіграє системний підхід до класифікації ризиків, який дозволяє враховувати як внутрішні організаційні аспекти, так і вплив зовнішнього середовища. Це забезпечує більш повне розуміння природи ризиків та створює передумови для підвищення ефективності управлінських рішень [32].

Представлена класифікація ризиків має важливе практичне значення, оскільки дозволяє не лише ідентифікувати їх види, але й визначити пріоритетні напрями управлінського впливу. Зокрема, поділ ризиків на внутрішні та зовнішні дає змогу розмежувати ті фактори, на які організація може безпосередньо впливати, і ті, що перебувають поза межами її контролю. Відповідно, для внутрішніх ризиків застосовуються методи

управління, спрямовані на їх усунення або мінімізацію, тоді як для зовнішніх — переважно адаптаційні механізми.

Крім того, класифікація за ступенем впливу дозволяє визначити критичні ризики, які потребують першочергової уваги з боку управлінського персоналу. Це особливо важливо для державних органів, де реалізація окремих ризиків може мати значні соціально-економічні та безпекові наслідки. Таким чином, класифікація ризиків виступає не лише теоретичним інструментом, але й основою для побудови ефективної системи ризик-менеджменту.

Особливу увагу в сучасних умовах слід приділяти безпековим ризикам, які є характерними для діяльності державних органів. Такі ризики пов'язані з високим рівнем невизначеності та значними наслідками, що можуть впливати не лише на результати діяльності окремої організації, але й на національну безпеку в цілому.

Для Державної прикордонної служби України найбільш характерними є ризики, пов'язані з незаконним перетинанням державного кордону, контрабандною діяльністю, терористичними загрозами, нелегальною міграцією, а також ризики, зумовлені воєнними діями. Окрім зовнішніх загроз, важливе значення мають і внутрішні ризики, зокрема кадрові, організаційні та корупційні, які можуть негативно впливати на ефективність функціонування служби [15].

Отже, ризик є складною багатовимірною категорією, що відображає вплив невизначеності на результати діяльності організації. Його сутність полягає у ймовірності виникнення подій, які можуть як перешкоджати досягненню цілей, так і створювати додаткові можливості. Класифікація ризиків забезпечує системний підхід до їх аналізу та є необхідною передумовою формування ефективної системи управління ризиками, що має особливе значення для діяльності державних органів у сфері забезпечення безпеки.

Важливо підкреслити, що в сучасних умовах ризик перестає розглядатися виключно як загроза та набуває стратегічного значення. Ефективне управління ризиками дозволяє не лише мінімізувати можливі втрати, але й створює передумови для підвищення результативності діяльності організації. Саме тому ризик-менеджмент розглядається як невід'ємний елемент системи управління, інтегрований у всі її функції.

Для державних органів, зокрема Державної прикордонної служби України, значення управління ризиками є особливо високим, оскільки від ефективності його реалізації залежить рівень забезпечення національної безпеки, стабільність функціонування держави та захист її кордонів. Це обумовлює необхідність подальшого дослідження механізмів управління ризиками та їх практичного застосування, що буде розглянуто у наступних підрозділах роботи.

1.2. Принципи та методи управління ризиками

Ефективне функціонування організацій в умовах невизначеності зумовлює необхідність формування дієвої системи управління ризиками. Управління ризиками є складовою загальної системи менеджменту та передбачає сукупність взаємопов'язаних заходів, спрямованих на ідентифікацію, оцінювання, мінімізацію та контроль ризиків з метою забезпечення досягнення поставлених цілей.

Сучасні міжнародні стандарти, зокрема ISO 31000:2018, визначають управління ризиками як ітеративний процес, який допомагає організаціям розробляти стратегію, досягати цілей та приймати обґрунтовані рішення. Згідно з цим стандартом, ключовим є не просто усунення ризику, а управління "впливом невизначеності на цілі", що вимагає постійної адаптації інструментарію до змін безпекового ландшафту.

Важливим теоретичним аспектом є розмежування понять «ризик» та «невизначеність». Якщо невизначеність характеризує відсутність повної інформації щодо майбутніх подій, то ризик передбачає можливість кількісного або якісного оцінювання наслідків такої невизначеності. Саме тому управління ризиками ґрунтується не лише на аналізі наявних даних, але й на використанні прогнозних моделей, що дозволяють зменшити рівень невизначеності при прийнятті управлінських рішень.

Крім того, у сучасній науковій літературі управління ризиками розглядається як складова стратегічного менеджменту, що забезпечує узгодження цілей організації з наявними загрозами та можливостями середовища. Це означає, що процес ризик-менеджменту має інтегруватися у всі функціональні підсистеми організації — фінансову, кадрову, операційну та інформаційну [20].

Сучасне розуміння управління ризиками ґрунтується на інтегрованому підході, відповідно до якого ризики розглядаються не ізольовано, а у взаємозв'язку з усіма аспектами діяльності організації. Такий підхід передбачає включення процесів управління ризиками до стратегічного та оперативного управління, що дозволяє підвищити обґрунтованість управлінських рішень.

В основі ефективного управління ризиками лежать певні принципи, які визначають загальні правила та підходи до організації цього процесу. Узагальнення наукових підходів дозволяє виділити ключові принципи управління ризиками (табл. 1.3).

Таблиця 1.3

Основні принципи управління ризиками

Принцип	Характеристика
Системності	Розгляд ризиків як елементу єдиної системи управління
Комплексності	Охоплення всіх видів ризиків та сфер діяльності
Безперервності	Постійний характер процесу управління ризиками
Обґрунтованості	Прийняття рішень на основі аналізу та оцінки
Превентивності	Орієнтація на попередження ризиків
Адаптивності	Здатність системи змінюватися відповідно до умов середовища

Взаємозв'язок наведених принципів проявляється у тому, що вони не функціонують ізольовано, а формують єдину методологічну основу управління ризиками. Зокрема, принцип системності забезпечує інтеграцію ризик-менеджменту в загальну систему управління, тоді як принцип безперервності гарантує постійне оновлення інформації про ризики. У свою чергу, принцип адаптивності дозволяє оперативно реагувати на зміни зовнішнього середовища, що особливо актуально в умовах нестабільності.

У практичній площині це означає, що ефективна система управління ризиками повинна не лише відповідати зазначеним принципам, але й забезпечувати їх узгоджену реалізацію через відповідні організаційні механізми, процедури та інструменти аналізу.

Варто зауважити, що в контексті державних інституцій принципи управління ризиками доповнюються принципом прозорості та підзвітності. Це зумовлено необхідністю раціонального використання бюджетних коштів та забезпечення публічного інтересу. Окрім того, інтегрований підхід передбачає, що управління ризиками не є окремим лінійним процесом, а створює додану вартість через підтримку прийняття стратегічних рішень на всіх рівнях ієрархії [25].

Зазначені принципи визначають логіку побудови системи управління ризиками та забезпечують її ефективне функціонування. Особливо важливим

є принцип превентивності, який передбачає не лише реагування на вже реалізовані ризики, але й їх попередження шляхом своєчасного виявлення загроз.

Управління ризиками реалізується через послідовність взаємопов'язаних етапів, які формують єдиний процес ризик-менеджменту. Узагальнену модель процесу управління ризиками представлено на рис. 1.2.



Рис. 1.2. Процес управління ризиками в організації

На першому етапі здійснюється ідентифікація ризиків, яка передбачає виявлення потенційних загроз, що можуть вплинути на діяльність організації. Важливим є врахування як внутрішніх, так і зовнішніх факторів ризику. Процес ідентифікації не повинен бути одноразовим актом, він потребує створення постійно діючих каналів зворотного зв'язку. У науковій літературі виокремлюють такі методи ідентифікації, як SWOT-аналіз (для визначення стратегічних ризиків), метод Дельфі (опитування незалежних експертів) та створення «реєстру ризиків». Для структур сектору безпеки критично

важливим на цьому етапі є метод «мозкового штурму» серед оперативних співробітників, що дозволяє виявити латентні загрози, які не фіксуються офіційною статистикою.

Другий етап включає аналіз та оцінку ризиків, що передбачає визначення ймовірності їх виникнення та можливих наслідків. Оцінка може здійснюватися як якісними, так і кількісними методами, що дозволяє ранжувати ризики за рівнем їх значущості.

На етапі вибору методів реагування визначаються оптимальні способи впливу на ризики з урахуванням їх характеристик та можливостей організації. Реалізація заходів передбачає впровадження відповідних управлінських рішень, спрямованих на мінімізацію негативних наслідків або використання потенційних можливостей.

Заключним етапом є моніторинг і контроль, який забезпечує оцінку ефективності прийнятих заходів та дозволяє своєчасно коригувати систему управління ризиками [22].

Слід зазначити, що ефективність реалізації кожного етапу значною мірою залежить від якості інформаційного забезпечення. Наявність достовірних, своєчасних та повних даних дозволяє підвищити точність оцінювання ризиків та зменшити ймовірність помилок при прийнятті управлінських рішень. У сучасних умовах це досягається шляхом використання автоматизованих інформаційних систем та аналітичних платформ.

Водночас процес управління ризиками має циклічний характер. Результати моніторингу та контролю використовуються для коригування попередніх етапів, що забезпечує постійне вдосконалення системи. Таким чином, ризик-менеджмент виступає як динамічний процес, що постійно адаптується до змін середовища функціонування організації.

Залежно від характеру впливу на ризик у практиці управління використовуються різні методи, які можна згрупувати за основними напрямками (табл. 1.4)

Таблиця 1.4

Методи управління ризиками

Група методів	Методи	Характеристика
Уникнення ризику	відмова від ризикових дій	Повне усунення ризику
Зниження ризику	диверсифікація, лімітування, резервування	Зменшення ймовірності або наслідків
Передача ризику	страхування, аутсорсинг	Переклад відповідальності на інші суб'єкти
Прийняття ризику	самострахування, покриття збитків	Усвідомлене прийняття ризику

Варто підкреслити, що застосування зазначених методів у чистому вигляді зустрічається рідко. У більшості випадків організації формують комбіновані стратегії управління ризиками, які дозволяють одночасно впливати як на ймовірність виникнення ризику, так і на масштаби його наслідків. Наприклад, поєднання методів зниження та передачі ризику дозволяє мінімізувати втрати навіть у разі реалізації негативного сценарію.

Особливого значення набуває вибір методів у державному секторі, де можливості уникнення або передачі ризиків є обмеженими. У таких умовах пріоритет надається методам зниження ризиків та їх контролю, що реалізуються через вдосконалення процедур, підвищення кваліфікації персоналу та впровадження сучасних технологій.

Окрім базових стратегій, наведених у табл. 1.4, доцільно виділити стратегію «активного прийняття». На відміну від пасивного покриття збитків, вона передбачає розробку планів безперервної діяльності, що дозволяє організації функціонувати навіть у момент реалізації катастрофічного ризику. У державному секторі метод «передачі ризику» через страхування часто є обмеженим, тому основний акцент зміщується на «дисипацію»

(розподіл) ризику між різними структурними підрозділами або через міжвідомчу взаємодію [28].

Важливу роль у процесі управління ризиками відіграють методи їх оцінювання. До якісних методів належать експертні оцінки, метод аналогій, сценарний аналіз, які дозволяють визначити характер ризиків та їх можливі наслідки. Кількісні методи передбачають використання статистичних даних, математичних моделей та розрахункових показників, що забезпечує більш точну оцінку рівня ризику.

Серед сучасних методів кількісного аналізу особливу увагу привертають метод Монте-Карло, що дозволяє моделювати тисячі варіантів розвитку подій, та аналіз чутливості. Для специфічних безпекових структур, таких як ДПСУ, актуальним є використання інтелектуального аналізу даних (Data Mining) для прогнозування протиправної діяльності.

Матриця «ймовірність–вплив» (Heat Map) при цьому слугує візуальним інструментом для виокремлення критичних ризиків («червона зона»), які потребують негайного реагування керівництва, від прийнятних ризиків, що підлягають лише моніторингу.

Особливе значення має використання матриці ризиків, яка дозволяє поєднати оцінку ймовірності виникнення ризику та масштабу його наслідків. Це забезпечує можливість ранжування ризиків та визначення пріоритетів управління ними [47].

Окремим напрямом розвитку методів управління ризиками є використання цифрових технологій, що дозволяють перейти від традиційного аналізу до інтелектуального управління ризиками. Застосування технологій Big Data, штучного інтелекту та машинного навчання відкриває можливості для обробки значних обсягів інформації та виявлення прихованих закономірностей у поведінці ризиків.

Такі інструменти дозволяють формувати прогностичні моделі, які забезпечують раннє виявлення загроз та підвищують ефективність

управлінських рішень. У цьому контексті ризик-менеджмент трансформується з реактивного інструменту у проактивну систему, здатну діяти на випередження.

У сучасних умовах розвитку інформаційних технологій управління ризиками набуває нових форм, пов'язаних із використанням цифрових інструментів, аналітики даних та автоматизованих систем моніторингу. Це дозволяє підвищити оперативність прийняття рішень та ефективність реагування на ризики.

Важливим аспектом є також розмежування внутрішнього та зовнішнього середовища ризиків (контексту). Для організацій сектору безпеки зовнішні фактори (геополітична нестабільність, зміни у законодавстві, транскордонна злочинність) часто є домінуючими, що вимагає впровадження методів сценарного планування. Це дозволяє розробити готові алгоритми дій для різних рівнів загрози ще до їх фактичного виникнення.

Системність управління ризиками проявляється у формуванні відповідної організаційної культури. Це передбачає, що кожен працівник, від рядового виконавця до керівника вищої ланки, розуміє свою роль у виявленні загроз. В межах системного підходу важливо впроваджувати концепцію «трьох ліній захисту»:

1. Перша лінія: безпосередні керівники підрозділів, які володіють ризиками та керують ними щоденно.
2. Друга лінія: підрозділи внутрішнього контролю та моніторингу ризиків.
3. Третя лінія: внутрішній аудит, що надає незалежну оцінку ефективності всієї системи. Така архітектура дозволяє мінімізувати вплив людського фактору та забезпечує об'єктивність контролю [23].

Отже, управління ризиками є складним багаторівневим процесом, що базується на системі взаємопов'язаних принципів і реалізується через сукупність методів, інструментів та організаційних механізмів. Його

ефективність визначається не лише здатністю організації своєчасно ідентифікувати та оцінювати ризики, але й рівнем інтеграції ризик-менеджменту в систему стратегічного та оперативного управління.

У сучасних умовах зростання невизначеності особливого значення набуває проактивний підхід до управління ризиками, що передбачає використання аналітичних та цифрових інструментів для прогнозування загроз. Для державних органів, зокрема Державної прикордонної служби України, ефективна система управління ризиками виступає ключовим елементом забезпечення стабільності функціонування, раціонального використання ресурсів та зміцнення національної безпеки.

1.3. Особливості управління ризиками в органах державної влади та безпеки

Управління ризиками в органах державної влади має суттєві відмінності порівняно з аналогічними процесами у приватному секторі, що зумовлено специфікою їх функціонування, цілями діяльності та рівнем відповідальності перед суспільством. Особливого значення ці відмінності набувають у сфері безпеки, де ризики пов'язані не лише з економічними втратами, але й із загрозами національній безпеці, територіальній цілісності та життю громадян.

На відміну від підприємств, діяльність яких спрямована на отримання прибутку, органи державної влади орієнтовані на забезпечення суспільних інтересів. Це визначає інший підхід до оцінювання ризиків, де ключовим критерієм виступає не фінансовий результат, а рівень безпеки та стабільності функціонування держави.

Суттєвою особливістю управління ризиками в державному секторі є високий рівень регламентованості діяльності. Функціонування органів

державної влади здійснюється на основі нормативно-правових актів, що обмежує гнучкість прийняття рішень, але водночас забезпечує їх правову визначеність. Це впливає на процес управління ризиками, який повинен відповідати встановленим процедурам та стандартам.

Крім того, діяльність державних органів характеризується підвищеним рівнем відповідальності, що зумовлює необхідність врахування широкого спектра ризиків, включаючи політичні, соціальні, економічні та безпекові. Особливо це стосується органів сектору безпеки, де реалізація ризиків може мати критичні наслідки [15].

З метою систематизації відмінностей між управлінням ризиками в державному та приватному секторах доцільно представити їх у вигляді узагальнюючої таблиці (табл. 1.5).

Таблиця 1.5

Порівняльна характеристика управління ризиками в державному та приватному секторах

Критерій	Державний сектор	Приватний сектор
Основна мета	Забезпечення суспільних інтересів	Отримання прибутку
Рівень регламентації	Високий	Відносно гнучкий
Характер ризиків	Комплексні (у т.ч. безпекові)	Переважно економічні
Наслідки реалізації ризиків	Соціальні, політичні, безпекові	Фінансові
Гнучкість управління	Обмежена	Висока

Як видно з таблиці, управління ризиками в державному секторі має більш складний і багатовимірний характер, що потребує застосування комплексних підходів.

Важливою особливістю управління ризиками в органах безпеки є їх висока динамічність. Зміни у зовнішньому середовищі, зокрема політична ситуація, військові загрози, міграційні процеси та економічні фактори,

призводять до постійної трансформації ризиків. Це вимагає від державних органів здатності до швидкої адаптації та оперативного реагування.

Крім того, специфіка діяльності органів безпеки передбачає наявність значної частки невизначеності та обмеженості інформації. У багатьох випадках рішення приймаються в умовах дефіциту часу та неповних даних, що підвищує значення аналітичних та прогностичних методів управління ризиками [32].

Особливе місце в системі управління ризиками займає людський фактор. Рівень професійної підготовки персоналу, дисципліна, доброчесність та відповідальність працівників безпосередньо впливають на ефективність реалізації управлінських рішень. У зв'язку з цим важливого значення набувають заходи з підбору, навчання та контролю персоналу.

Загальна модель управління ризиками в органах державної влади та безпеки представлена на рис. 1.3.



Рис. 1.3. Особливості системи управління ризиками в органах державної влади

Слід зазначити, що в умовах воєнного стану та посилення загроз національній безпеці роль управління ризиками значно зростає. Це пов'язано

з необхідністю забезпечення безперервності функціонування державних органів, ефективного використання ресурсів та своєчасного реагування на кризові ситуації.

Для органів прикордонної служби особливе значення мають ризики, пов'язані з порушенням державного кордону, незаконною міграцією, контрабандою, диверсійною діяльністю та іншими загрозами. Управління такими ризиками потребує застосування комплексних підходів, що поєднують організаційні, технічні та аналітичні заходи.

Важливою особливістю управління ризиками в органах державної влади є багаторівневий характер прийняття управлінських рішень. На відміну від приватного сектору, де рішення часто приймаються на рівні керівництва підприємства, у державних органах існує чітка ієрархія управління. Це зумовлює необхідність координації дій між різними рівнями управління, що ускладнює процес оперативного реагування на ризики [33].

Крім того, суттєвий вплив на систему управління ризиками має політичний фактор. Зміни у державній політиці, пріоритетах розвитку, міжнародних відносинах можуть істотно змінювати характер ризиків та вимагати адаптації управлінських підходів. Це особливо актуально для органів сектору безпеки, діяльність яких безпосередньо пов'язана із зовнішньополітичними та внутрішньополітичними процесами.

Ще однією важливою особливістю є обмеженість ресурсів. Державні органи функціонують в умовах бюджетного фінансування, що обмежує можливості щодо реалізації заходів управління ризиками. У зв'язку з цим виникає необхідність пріоритизації ризиків та оптимального розподілу ресурсів.

Специфіка ресурсного забезпечення в державному секторі безпеки породжує феномен «бюджетного детермінізму» в управлінні ризиками. На відміну від бізнесу, де інвестиції в безпеку можуть бути збільшені за рахунок очікуваного прибутку, державні органи безпеки обмежені жорсткими

лімітами асигнувань. Це зумовлює перехід від стратегії «мінімізації загрози будь-якою ціною» до стратегії «прийнятного ризику в межах наявного бюджету». Відтак, головним завданням стає не повна ліквідація ризиків, а їх оптимізація через вартісно-орієнтований аналіз, де ціною помилки є не банкрутство, а зниження рівня національної безпеки.

У секторі безпеки, зокрема при охороні кордону, управління ризиками набуває характеру «стратегічної гри» в умовах інформаційної асиметрії. Державні органи мають справу з активним суб'єктом (контрабандисти, диверсійні групи), який свідомо маскує свої наміри та адаптується до методів контролю. Це докорінно відрізняє державний ризик-менеджмент від приватного, де ризики часто є стихійними (ринкові коливання, природні явища). У безпековому секторі ризик є інтелектуально зумовленим, що вимагає впровадження не просто статичних процедур, а ігрових моделей прогнозування поведінки порушників [48].

Окремої уваги потребує питання інформаційного забезпечення управління ризиками. У державному секторі інформація часто має обмежений доступ, що ускладнює її використання для аналізу та прогнозування ризиків. Водночас значна кількість інформації має конфіденційний характер, що обмежує можливості її відкритого використання (табл. 1.6).

Таблиця 1.6

Ключові особливості управління ризиками в органах державної влади

Особливість	Характеристика
Багаторівневе управління	Наявність ієрархічної системи прийняття рішень
Високий рівень відповідальності	Значні наслідки реалізації ризиків
Регламентованість діяльності	Чітке нормативно-правове регулювання
Обмеженість ресурсів	Залежність від бюджетного фінансування
Інформаційні обмеження	Часткова закритість інформації
Динамічність середовища	Постійна зміна зовнішніх умов

Важливим аспектом є також необхідність міжвідомчої взаємодії у процесі управління ризиками. Багато ризиків, особливо у сфері безпеки, мають міжгалузевий характер і потребують координації між різними державними органами. Це вимагає створення ефективних механізмів інформаційного обміну та спільного реагування.

У сучасних умовах значного поширення набуває ризик-орієнтований підхід до управління, який передбачає концентрацію уваги на найбільш значущих ризиках. Такий підхід дозволяє підвищити ефективність використання ресурсів та забезпечити більш цілеспрямоване управління [38].

Крім того, у діяльності органів безпеки важливе значення має фактор часу. Багато ризиків потребують негайного реагування, що зумовлює необхідність високого рівня оперативності управлінських рішень. У таких умовах значну роль відіграють автоматизовані системи моніторингу та аналізу інформації.

Слід також враховувати, що ризики у сфері безпеки часто мають латентний характер, тобто можуть тривалий час не проявлятися явно, але при цьому становити значну загрозу. Це ускладнює процес їх виявлення та оцінювання.

Для органів державної влади характерним є «каскадний ефект» реалізації ризиків. Через високу взаємопов'язаність державних інститутів, збій у системі прикордонної безпеки миттєво трансформується в економічні ризики (втрата митних надходжень), соціальні (зростання злочинності) та міжнародні (зниження довіри партнерів). Такий мультиплікативний характер наслідків вимагає від системи управління ризиками наявності високого рівня організаційної резильєнтності — здатності системи зберігати функціональність навіть за умови часткового руйнування її окремих елементів.

У контексті діяльності органів прикордонної служби зазначені особливості набувають ще більшої актуальності. Це пов'язано з тим, що

державний кордон є зоною підвищеного ризику, де перетинаються економічні, політичні та безпекові інтереси держави.

В сучасних умовах управління ризиками в ДПСУ стикається з явищем «конвергенції загроз», коли класичні військові загрози переплітаються з гібридними, кібернетичними та епідеміологічними. Це створює ситуацію «ідеального шторму», де стандартні алгоритми реагування можуть бути неефективними. Тому важливою особливістю стає перехід від лінійного управління до мережевої координації, що передбачає миттєвий обмін даними між різними суб'єктами сектору безпеки без бюрократичних затримок [15].

У сучасних умовах глобалізації та зростання транснаціональних загроз ефективність системи управління ризиками значною мірою визначається рівнем її відповідності міжнародним стандартам та практикам. Для сектору прикордонної безпеки це особливо актуально, оскільки ризики мають транскордонний характер і потребують узгоджених дій між державами.

Однією з ключових концепцій, що визначає сучасний підхід до організації прикордонної безпеки, є модель інтегрованого управління кордонами (Integrated Border Management, IBM). Вона передбачає комплексний підхід до управління ризиками, який охоплює всі етапи контролю — від аналізу загроз до безпосереднього реагування.

Модель IBM базується на таких ключових принципах:

- міжвідомча взаємодія;
- міжнародне співробітництво;
- багаторівневий контроль;
- застосування ризик-орієнтованого підходу.

Застосування цієї моделі дозволяє забезпечити баланс між безпекою та свободою пересування, що є особливо важливим для країн, які прагнуть інтеграції до європейського простору.

Важливу роль у формуванні сучасної системи управління ризиками відіграє діяльність Frontex — Агентства Європейського Союзу з охорони

зовнішніх кордонів. Дана інституція забезпечує координацію зусиль держав-членів ЄС у сфері прикордонної безпеки та розробляє уніфіковані підходи до оцінки ризиків [28].

Ключовим інструментом, який використовується у діяльності Frontex, є модель CIRAM (Common Integrated Risk Analysis Model). Сучасна версія цієї моделі — CIRAM 2.0 — являє собою комплексну систему аналізу ризиків, що включає:

- збір та інтеграцію даних з різних джерел;
- оцінку загроз, вразливостей та наслідків;
- формування аналітичних продуктів для прийняття рішень;
- прогнозування розвитку ризиків.

Особливістю CIRAM є те, що вона орієнтована не лише на фіксацію вже наявних загроз, а й на їх прогнозування, що відповідає сучасним вимогам проактивного управління.

У межах цієї моделі ризик розглядається як функція трьох складових: загрози (threat), вразливості (vulnerability), потенційного впливу (impact).

Такий підхід дозволяє комплексно оцінювати ситуацію та визначати пріоритети управління ризиками.

Зарубіжний досвід свідчить, що ефективні системи управління ризиками у сфері прикордонної безпеки базуються на широкому використанні цифрових технологій. Зокрема, у країнах ЄС активно застосовуються:

- системи біометричної ідентифікації;
- автоматизовані бази даних;
- інтелектуальні системи відеоспостереження;
- аналітика великих даних (Big Data).

Наприклад, у Німеччині та Франції впроваджено системи автоматичного аналізу пасажиропотоків, що дозволяють виявляти підозрілі маршрути ще до прибуття особи до пункту пропуску. У Польщі значну увагу

приділяють розвитку мобільних комплексів спостереження та інтеграції інформаційних систем із європейськими базами даних.

У США система прикордонного контролю реалізується через діяльність Служби митного та прикордонного контролю (CBP), яка активно використовує ризик-орієнтований підхід. Основна увага приділяється попередньому аналізу інформації про осіб та вантажі, що дозволяє мінімізувати навантаження на пункти пропуску та підвищити ефективність контролю [26].

Важливою складовою зарубіжного досвіду є також впровадження принципу «інформаційної інтеграції», який передбачає об'єднання даних з різних джерел у єдину систему. Це дозволяє уникнути дублювання інформації та забезпечити оперативний доступ до актуальних даних.

Окрім технологічного аспекту, значна увага приділяється організаційним механізмам управління ризиками. Зокрема, у країнах ЄС функціонують спеціалізовані аналітичні центри, які здійснюють централізований аналіз інформації та формують рекомендації для оперативних підрозділів. Такий підхід дозволяє забезпечити узгодженість дій та підвищити якість управлінських рішень.

Отже, управління ризиками в органах державної влади та безпеки характеризується високим рівнем складності, багатофакторністю та значущістю наслідків. Його ефективність визначається здатністю органів влади адаптуватися до змін зовнішнього середовища, забезпечувати належний рівень координації та впроваджувати сучасні методи управління ризиками. Врахування зазначених особливостей є необхідною передумовою для подальшого дослідження системи управління ризиками в діяльності Державної прикордонної служби України. Зарубіжний досвід управління ризиками свідчить про необхідність переходу від традиційних форм контролю до інтегрованих, технологічно орієнтованих систем, що забезпечують проактивне реагування на загрози. Використання найкращих

міжнародних практик створює основу для вдосконалення національної системи управління ризиками в Державній прикордонній службі України та підвищення рівня її ефективності.

Висновок до розділу 1.

У першому розділі досліджено теоретико-методологічні засади управління ризиками, що дозволило сформулювати цілісне розуміння цього процесу як критично важливого елементу сучасного менеджменту в державних структурах. За результатами проведеного теоретичного аналізу було зроблено такі висновки:

Ризик визначено не лише як імовірність настання негативної події, а як вплив невизначеності на досягнення стратегічних цілей організації. Встановлено, що для державних органів сектору безпеки ризик має мультиплікативний характер, де економічні втрати є вторинними порівняно із загрозами національній безпеці, територіальній цілісності та життю громадян.

Доведено, що ефективний ризик-менеджмент базується на принципах системності, безперервності та превентивності. Встановлено, що інтегрований підхід (ERM) вимагає поєднання якісних методів оцінювання (експертне оцінювання, сценарний аналіз) із кількісними математико-статистичними моделями. Це дозволяє трансформувати суб'єктивні прогнози у об'єктивні дані, необхідні для прийняття управлінських рішень.

Визначено, що на відміну від приватного сектору, де головним критерієм є прибутковість, управління ризиками в органах безпеки (зокрема ДПСУ) регламентується суворими нормативно-правовими рамками та міжнародними стандартами (ISO 31000). Встановлено, що в умовах воєнного стану класичні ризики трансформуються, набуваючи ознак кризового

управління, що вимагає високої оперативності та адаптивності системи управління.

Теоретичний аналіз підтвердив, що для Державної прикордонної служби України впровадження комплексної системи управління ризиками є не просто інструментом підвищення ефективності, а необхідною умовою забезпечення стійкості державного кордону в умовах гібридних загроз та зовнішньої агресії.

Отримані теоретичні результати створюють методичну базу для проведення подальшого аналізу діючої системи управління ризиками в Державній прикордонній службі України, що і буде здійснено у другому розділі дипломної роботи.

РОЗДІЛ 2. АНАЛІЗ СИСТЕМИ УПРАВЛІННЯ РИЗИКАМИ В ДЕРЖАВНІЙ ПРИКОРДОННІЙ СЛУЖБІ УКРАЇНИ

2.1. Загальна характеристика діяльності ДПСУ як об'єкта управління

Державна прикордонна служба України є ключовим елементом сектору безпеки і оборони держави, діяльність якого спрямована на забезпечення недоторканності державного кордону, реалізацію державної політики у сфері прикордонної безпеки та захист національних інтересів. У сучасних умовах функціонування держави роль прикордонної служби суттєво зростає, що обумовлено як внутрішніми трансформаційними процесами, так і зовнішніми загрозами, пов'язаними з воєнною агресією, нестабільністю міжнародного середовища та активізацією транскордонної злочинності.

Правовою основою діяльності Державної прикордонної служби України є Конституція України, профільні закони, а також підзаконні нормативно-правові акти, що визначають її функції, повноваження та організаційні засади функціонування. Як правоохоронний орган спеціального призначення, ДПСУ виконує широкий спектр завдань, що виходять за межі класичної охорони кордону та охоплюють безпекові, контрольні та правоохоронні функції [72].

Фундаментальне значення для сучасного етапу розвитку ДПСУ має Закон України «Про Державну прикордонну службу України», який закріплює її статус як правоохоронного органу спеціального призначення. Крім того, діяльність служби в контексті управління ризиками безпосередньо корелює із Стратегією інтегрованого управління кордонами на період до 2025 року. Цей документ визначає перехід до європейських стандартів моніторингу ситуації, де управління ризиками виступає не просто функцією, а основою для прийняття рішень на стратегічному, тактичному та оперативному рівнях.

Нормативно-правове забезпечення діяльності органів охорони державного кордону відіграє ключову роль у формуванні системи управління та визначає межі прийняття управлінських рішень. Діяльність Державної прикордонної служби України регламентується спеціалізованими нормативними актами, які встановлюють її функції, повноваження та організаційні засади. До них належать закони України, що визначають статус прикордонної служби, порядок охорони державного кордону, а також нормативні документи, що регулюють питання національної безпеки та оборони [3].

Важливе значення має також внутрішня нормативна база, яка включає накази, інструкції та положення, що деталізують порядок виконання службових завдань. Саме ці документи забезпечують уніфікацію управлінських процесів, встановлюють стандарти діяльності та визначають алгоритми реагування на різні види загроз.

Тож, нормативно-правове регулювання створює основу для функціонування системи управління ДПСУ, але водночас накладає певні обмеження щодо гнучкості прийняття рішень, що є важливим фактором у процесі управління ризиками.

З позиції теорії управління Державна прикордонна служба України розглядається як складна організаційно-управлінська система, що функціонує в умовах підвищеної невизначеності. Вона характеризується багаторівневою ієрархічною структурою, чітким розподілом повноважень, централізацією управлінських рішень та високим рівнем відповідальності за результати діяльності.

Як об'єкт управління ДПСУ має такі ключові особливості:

функціонування в умовах постійної дії ризиків та загроз;

значна залежність від зовнішнього середовища;

необхідність оперативного прийняття рішень;

поєднання адміністративних і силових методів управління;

подвійний характер функціонування: виконання правоохоронних завдань у мирний час та участь у відсічі збройній агресії в межах Сил оборони України під час дії воєнного стану, що потребує поєднання методів цивільного менеджменту та військового управління; високі вимоги до координації та взаємодії між підрозділами [2].

Організаційна структура ДПСУ побудована за принципом ієрархічності та включає центральний орган управління, регіональні управління, органи охорони державного кордону, морську охорону, спеціальні та забезпечувальні підрозділи. Така структура забезпечує реалізацію функцій служби на всіх рівнях та дозволяє ефективно реагувати на виклики зовнішнього середовища.

Основні функції ДПСУ можна систематизувати за такими напрямками:

1. контрольна (здійснення прикордонного контролю);
2. правоохоронна (протидія правопорушенням);
3. безпекова (захист державного кордону);
4. аналітична (збір і обробка інформації);
5. координаційна (взаємодія з іншими органами державної влади).

Слід підкреслити, що діяльність ДПСУ має міжвідомчий характер. Вона тісно взаємодіє з іншими органами сектору безпеки, митними органами, правоохоронними структурами та міжнародними партнерами. Така взаємодія є необхідною умовою ефективного реагування на комплексні загрози.

Значною особливістю діяльності служби є її функціонування в умовах підвищеного рівня ризику. Ризики виникають як у зовнішньому середовищі (збройна агресія, нелегальна міграція, контрабанда, транснаціональна злочинність), так і у внутрішньому (кадрові проблеми, обмеженість ресурсів, організаційні недоліки) [51].

Узагальнення характеристик ДПСУ як об'єкта управління представлено в табл. 2.1.

Таблиця 2.1

Основні характеристики ДПСУ як об'єкта управління

Характеристика	Зміст
Тип організації	Державний правоохоронний орган
Основна мета	Забезпечення безпеки державного кордону
Характер діяльності	Безпековий, правоохоронний
Структура управління	Ієрархічна, централізована
Рівень відповідальності	Високий (державний рівень)
Умови функціонування	Динамічне та ризиковане середовище

Аналіз наведених характеристик свідчить про те, що ДПСУ функціонує в умовах високого рівня невизначеності, що зумовлює необхідність впровадження сучасних підходів до управління, зокрема ризик-орієнтованого підходу.

Оцінка діяльності Державної прикордонної служби України як об'єкта управління свідчить про її функціонування в умовах постійного зростання складності завдань. Це пов'язано з розширенням спектра загроз, які мають як традиційний, так і новітній характер. Зокрема, поряд із класичними викликами, такими як незаконне перетинання державного кордону та контрабандна діяльність, актуальності набувають гібридні загрози, пов'язані з інформаційним впливом, диверсійною діяльністю та використанням новітніх технологій.

Аналіз умов функціонування ДПСУ дозволяє виділити ключові тенденції, що впливають на її діяльність:

- зростання рівня безпекових загроз у прикордонному просторі;
- підвищення вимог до оперативності реагування;
- необхідність інтеграції сучасних технологій у процес управління;
- посилення ролі аналітичної складової діяльності.

Зазначені тенденції свідчать про трансформацію ДПСУ з класичного правоохоронного органу у багатофункціональну безпекову структуру, що

функціонує в умовах високої невизначеності. Це, у свою чергу, обумовлює зростання ролі ризик-орієнтованого підходу до управління [3].

Крім того, важливо враховувати, що ефективність діяльності ДПСУ значною мірою залежить від рівня ресурсного забезпечення. Обмеженість фінансових ресурсів, необхідність модернізації матеріально-технічної бази та підвищення кваліфікації персоналу створюють додаткові виклики, які мають бути враховані у процесі управління.

Важливим елементом ресурсної бази в сучасній системі управління є цифровізація. Впровадження автоматизованих систем прикордонного контролю (наприклад, АСПК «Гарт») та інтеграція з базами даних Інтерполу та Європолу трансформують ДПСУ в цифровізовану систему, де об'єктом управління стають не лише людські ресурси, а й величезні масиви даних, що потребують автоматизованої обробки для виявлення ризиків.

У контексті управління ризиками особливе значення має інформаційне забезпечення діяльності ДПСУ. Своєчасне отримання, обробка та аналіз інформації дозволяють підвищити ефективність прийняття управлінських рішень та забезпечити оперативне реагування на загрози.

Загальна модель функціонування ДПСУ як об'єкта управління представлена на рис. 2.1.

Підсумовуючи характеристику Державної прикордонної служби України як об'єкта управління, слід підкреслити, що її ефективність на сучасному етапі визначається не лише жорсткістю організаційної структури, а насамперед динамічною здатністю системи до адаптації та резильєнтності (життєстійкості). В умовах воєнного стану та перманентних гібридних загроз ДПСУ трансформується з класичного правоохоронного органу у високотехнологічну безпекову систему, що вимагає переходу від реактивного управління (реагування на факти порушень) до превентивного, базованого на випереджальному аналізі ризиків [5].



Рис. 2.1. ДПСУ як об'єкт управління

Таким чином, ДПСУ постає як складна, багатоцільова ієрархічна система, функціонування якої нерозривно пов'язане з високим рівнем невизначеності та критичністю наслідків управлінських рішень. Це обґрунтовує об'єктивну необхідність впровадження інтегрованої моделі ризик-менеджменту, яка дозволить оптимізувати використання обмежених ресурсів та забезпечити надійність охорони державного кордону в умовах безпекової турбулентності. Саме детальний аналіз специфічних видів ризиків, що виникають у процесі такої діяльності, стане предметом дослідження у наступному підрозділі.

2.2. Основні види ризиків у діяльності ДПСУ

Діяльність Державної прикордонної служби України здійснюється в умовах підвищеної невизначеності, що обумовлено складністю безпекового середовища, динамічністю зовнішніх загроз та внутрішніми організаційними викликами. У сучасних умовах, особливо в період воєнного стану, ризики набувають комплексного характеру, що проявляється у їх взаємозв'язку та взаємному посиленні.

З метою більш глибокого аналізу ризиків діяльності ДПСУ доцільно використовувати ризик-орієнтований підхід, який передбачає ідентифікацію, оцінювання та ранжування ризиків залежно від ймовірності їх виникнення та потенційного впливу на результати діяльності. Такий підхід дозволяє не лише систематизувати загрози, але й визначити пріоритетні напрями управлінського впливу.

У контексті діяльності прикордонної служби доцільним є також використання елементів європейської моделі аналізу ризиків, зокрема CIRAM, яка передбачає врахування індикаторів загроз, вразливостей та потенційних наслідків. Це дозволяє розглядати ризики не ізольовано, а як частину єдиної аналітичної системи.

Аналіз нормативно-правових документів, зокрема антикорупційних програм, а також статистичних даних щодо діяльності ДПСУ дозволяє систематизувати основні ризики за функціональними напрямками [3].

Першу та найбільш критичну групу становлять ризики транскордонної злочинності та протиправної діяльності. Вони безпосередньо пов'язані з виконанням основних функцій прикордонної служби та мають тенденцію до зростання.

Зокрема, спостерігається суттєве підвищення ризику незаконного обігу засобів ураження. За оперативними даними, кількість вилученої зброї зросла з 373 одиниць у 2025 році до 503 одиниць у 2026 році, тоді як обсяг

вилучених боєприпасів збільшився з 23,9 тис. до понад 88,2 тис. штук. Це свідчить про активізацію незаконних каналів переміщення зброї та підвищення рівня загроз безпеці.

Не менш значущим є ризик наркотизації транскордонних каналів. Обсяг вилучених наркотичних речовин у I кварталі 2026 року зріс майже в чотири рази — до 90,9 кг порівняно з 24,7 кг за аналогічний період попереднього року. Така динаміка свідчить про зміну масштабів і організації наркоторгівлі через державний кордон.

Суттєве зростання демонструють і економічні ризики, пов'язані з товарною контрабандою. Вартість вилучених контрабандних товарів збільшилася з 59,5 млн грн до 254,3 млн грн, що свідчить про концентрацію контрабандних потоків у великих партіях та ускладнення схем їх переміщення.

Слід зауважити, що зростання вартості вилучених товарів у 4,2 рази на тлі незначного зниження пасажиропотоку (з 7,3 млн до 7,1 млн осіб) свідчить про зміну стратегії контрабандних угруповань. Ризики зміщуються у бік професіоналізації та використання технологічних засобів прихованого переміщення, що вимагає від ДПСУ перегляду профілів ризику для вантажних перевезень та посилення технічної складової контролю [7-8].

Ускладнення схем контрабандної діяльності супроводжується активним використанням цифрових технологій, зокрема засобів шифрування комунікацій, GPS-навігації та дистанційного управління переміщенням товарів. Це суттєво знижує ефективність традиційних методів контролю та потребує впровадження інтелектуальних систем аналізу ризиків.

Окремим аспектом трансформації ризиків транскордонної злочинності є їх гібридизація. У 2026 році спостерігається злиття класичної кримінальної діяльності з методами інформаційно-психологічного впливу. Зокрема, ідентифіковано ризик використання соціальних мереж та закритих месенджерів для координації незаконного перетину кордону в реальному

часі, що створює ефект «розпорошеної загрози». Це означає, що ризик переміщується з фізичної площини (накопичення груп на кордоні) у віртуальну (дистанційний інструктаж), що робить традиційні методи візуального спостереження недостатніми та вимагає впровадження інструментів OSINT-розвідки в систему ризик-менеджменту ДПСУ.

Тож, ризики у сфері транскордонної злочинності трансформуються від кількісних до якісних змін, що вимагає від ДПСУ переходу від реактивної до проактивної моделі управління.

Другу важливу групу становлять корупційні ризики, які мають системний характер і можуть нівелювати ефективність діяльності служби. Відповідно до антикорупційних програм ДПСУ, ключові загрози пов'язані з порушенням процедур контролю, розподілом ресурсів та кадровими рішеннями [5].

Зокрема, значним є ризик зловживань під час здійснення прикордонного контролю, що може проявлятися у сприянні незаконному перетину державного кордону або розголошенні службової інформації. Не менш важливими є ризики у сфері матеріально-технічного забезпечення, особливо у процесах закупівель сучасних технічних засобів, таких як безпілотні літальні апарати та засоби радіоелектронної боротьби.

Особливу категорію становлять фінансово-кадрові ризики, пов'язані з можливими порушеннями під час призначення на посади або нарахування додаткових виплат. Також актуальними є інформаційні ризики, що полягають у несанкціонованому доступі до баз даних або витоку службової інформації.

З метою систематизації зазначених загроз доцільно узагальнити їх у таблиці (табл. 2.3).

Таблиця 2.3

Класифікація пріоритетних корупційних ризиків у ДПСУ

Категорія ризику	Сутність загрози	Об'єкт впливу
Процедурні	Зловживання під час пропускних операцій	Прикордонний контроль
Ресурсні	Порушення у сфері закупівель	Матеріально-технічне забезпечення
Фінансово-кадрові	Непрозорі кадрові рішення та виплати	Персонал
Інформаційні	Витік або несанкціоноване використання даних	Інформаційні системи
Логістичні	Порушення ланцюгів постачання пального та запчастин	Оперативна готовність підрозділів
Технологічні	Вразливість систем «Гарт» та «Аркан» до кібератак	Цілісність державних реєстрів
Репутаційні	Дискредитація служби через висвітлення поодиноких фактів корупції	Рівень довіри суспільства та партнерів

Аналіз наведених у таблиці 2.3 даних свідчить про те, що найбільш небезпечними є процедурні та ресурсні корупційні ризики, оскільки саме вони безпосередньо впливають на результати основної діяльності ДПСУ. Їх реалізація може створювати умови для виникнення інших видів ризиків, зокрема безпекових та економічних.

Водночас інформаційні ризики набувають особливої актуальності в умовах цифровізації управління. Несанкціонований доступ до баз даних може призводити до витоку критично важливої інформації, що створює загрозу не лише окремим підрозділам, але й національній безпеці в цілому.

Природа корупційних ризиків у ДПСУ тісно пов'язана з наявністю значних дискреційних повноважень у посадових осіб на місцях. В умовах воєнного стану, коли нормативне регулювання може змінюватися оперативно (наприклад, правила виїзду окремих категорій громадян), виникає ризик суб'єктивного трактування норм. Це створює «корупційну ренту», де

об'єктом впливу стає не лише фінансовий ресурс, а й саме право на перетин кордону. Організаційний ризик тут полягає у можливому створенні стійких ієрархічних корупційних ланцюгів, які здатні блокувати впровадження автоматизованих систем контролю, оскільки останні мінімізують людський фактор [72].

Окремої уваги заслуговують ризики, ідентифіковані в Антикорупційній програмі ДПСУ на 2026–2028 рр., що стосуються специфічних викликів воєнного стану (Додаток А). До них віднесено ризик зловживань під час видачі дозволів на перебування у прикордонній смузі та ризики, пов'язані з непрозорим розподілом гуманітарної допомоги для потреб підрозділів. Характерною рисою цих ризиків є їх високий рівень латентності, що потребує впровадження автоматизованих систем моніторингу службової діяльності та посилення ролі підрозділів внутрішньої безпеки.

Третьою групою є ризики, зумовлені умовами воєнного стану та безпекової турбулентності. Вони мають специфічний характер та пов'язані з військовими діями, нестабільністю середовища та підвищеним рівнем загроз.

До таких ризиків належить ризик втрати або нецільового використання майна, включаючи військову техніку та матеріальні ресурси. Також значно зріс ризик незаконного обігу вибухових речовин: обсяг вилучених вибухових матеріалів збільшився з 76,6 кг до понад 1 тонни (1089 кг) лише за перший квартал 2026 року.

Таке безпрецедентне зростання обсягів вилучених вибухових речовин (у 14 разів порівняно з аналогічним періодом минулого року) вказує на формування нового вектора загроз — ризику внутрішньої дестабілізації через насичення цивільного обігу небезпечними засобами ураження. Це трансформує роль ДПСУ: з класичного органу охорони кордону вона стає критичним бар'єром для запобігання терористичним актам у тилкових регіонах України [5].

Поряд із зовнішніми безпековими загрозами, критичного значення набуває внутрішній кадровий ризик. Зростання обсягів вилучень зброї та вибухівки свідчить про колосальне психофізичне навантаження на особовий склад. Ризик полягає у «втомі металу» — зниженні пильності через перманентний стрес та високу інтенсивність служби. Це створює умови для ненавмисних помилок при ідентифікації загроз. Крім того, існує ризик відтоку кваліфікованих кадрів (офіцерів-аналітиків, ІТ-спеціалістів) у приватний сектор, що може призвести до «інтелектуального знекровлення» підрозділів аналізу ризиків саме в момент їх найбільшої затребуваності.

Зазначені тенденції свідчать про зміну характеру ризиків від локальних до системних. У таких умовах управління ризиками повинно базуватися на принципах гнучкості, адаптивності та міжвідомчої координації. [34].

Особливістю ризиків у діяльності ДПСУ є їх взаємозв'язок та здатність до взаємного посилення. Реалізація одного ризику може створювати передумови для виникнення інших, що формує складні ризикові ситуації.



Рис. 2.2. Взаємозв'язок ризиків у діяльності ДПСУ

Як показано на рис. 2.2, корупційні ризики виконують роль «каталізатора» для інших груп загроз. Наприклад, зловживання під час

прикордонного контролю (корупційний ризик) створює «вікно» для незаконного переміщення зброї чи вибухівки (безпековий ризик), що в умовах воєнного стану безпосередньо загрожує життю особового складу та обороноздатності країни.

Слід виділити специфічний ефект кумуляції ризиків. У діяльності ДПСУ ризики рідко реалізуються поодиночі. Зазвичай ми спостерігаємо «ланцюгову реакцію»: фінансова нестабільність (низька зарплата) посилює корупційний ризик, який, у свою чергу, відкриває шлях для безпекових загроз (пропуск контрабанди зброї). Такий взаємозв'язок потребує впровадження в ДПСУ методології «динамічних профілів ризику», які б змінювалися автоматично при зміні хоча б одного з індикаторів у суміжній сфері

Таким чином, система ризиків у діяльності Державної прикордонної служби України характеризується високим рівнем складності, динамічністю та взаємозалежністю окремих елементів. Проведений аналіз свідчить не лише про зростання кількісних показників ризиків, але й про їх якісну трансформацію, що проявляється у появі нових форм загроз та ускладненні механізмів їх реалізації.

У таких умовах особливої актуальності набуває впровадження інтегрованої системи управління ризиками, що поєднує аналітичні, організаційні та технологічні інструменти. Отримані результати є основою для оцінки ефективності існуючої системи управління ризиками в ДПСУ, що буде здійснено у наступному підрозділі роботи.

2.3. Оцінка діючої системи управління ризиками в ДПСУ

Сучасна система управління ризиками в Державній прикордонній службі України (ДПСУ) перебуває на етапі активної трансформації від жорсткої централізованої моделі до гнучкої ризик-орієнтованої системи, що відповідає стандартам ЄС та критеріям інтегрованого управління кордонами (IBM).

Важливим аспектом оцінки є відповідність внутрішніх процедур ДПСУ вимогам Постанови КМУ №1062 «Про затвердження Основних засад здійснення внутрішнього контролю розпорядниками бюджетних коштів». У ході аналізу встановлено, що в Службі сформовано вертикаль відповідальності, де кожен рівень управління (від Адміністрації до прикордонного загону) має власні паспорти ризиків. Проте, як показує практика, існує проблема «формального звітування», коли ідентифіковані ризики кочують із одного звітного періоду в інший без суттєвої зміни заходів реагування. Це вказує на необхідність перегляду методології переоцінки ризиків, щоб вона базувалася не на календарних датах, а на тригерних подіях (зміна інтенсивності обстрілів, поява нових видів контрабанди тощо).

Оцінку ефективності системи управління ризиками в ДПСУ доцільно здійснювати за такими ключовими критеріями, як рівень виявлення та попередження ризиків, швидкість реагування на загрози, ефективність використання ресурсів, рівень цифровізації процесів управління, а також ступінь інтеграції антикорупційних механізмів у загальну систему управління. Застосування зазначених критеріїв дозволяє здійснити комплексну оцінку функціонування системи ризик-менеджменту [10].

Основою діючої системи є багаторівневий моніторинг, який охоплює стратегічний (Адміністрація ДПСУ), регіональний (Регіональні управління) та оперативний (органи охорони кордону) рівні. Ключовим інструментом на оперативному рівні є використання автоматизованих систем, таких як АСПК

«Гарт», що дозволяє в реальному часі здійснювати перевірку осіб та транспортних засобів за базами даних. Проте аналіз результатів діяльності за I квартал 2026 року вказує на те, що технічна складова потребує подальшого посилення, особливо в частині протидії новітнім загрозам (БПЛА, засоби РЕБ).

Оцінюючи аналітичний інструментарій, слід відзначити спроби інтеграції Спільної інтегрованої моделі аналізу ризиків (CIRAM 2.0), що використовується країнами-членами ЕС та агентством Frontex. Діюча система в ДПСУ демонструє високу ефективність у зборі первинних даних, проте етап «інтерпретації та оцінки впливу» часто залишається слабкою ланкою. У I кварталі 2026 року було зафіксовано, що незважаючи на наявність розвідувальної інформації про накопичення товарних груп у прикордонні, превентивне посилення ділянок відбувалося з певною затримкою. Це підтверджує тезу про те, що діюча система управління ризиками все ще залишається «людино центричною» — її швидкість залежить від суб'єктивного рішення аналітика, а не від автоматизованих алгоритмів раннього попередження [8].

Водночас слід зазначити, що ефективність використання автоматизованих систем значною мірою залежить від рівня їх інтеграції з іншими інформаційними ресурсами та якості аналітичної обробки даних. За відсутності єдиної аналітичної платформи навіть сучасні технічні засоби можуть використовуватися лише як інструменти фіксації інформації, а не її прогнозування. Це обмежує можливості переходу до проактивної моделі управління ризиками.

Оцінка фінансового стану інституції, що забезпечує реалізацію безпекових функцій, дозволяє ідентифікувати рівень ресурсного ризику. Згідно зі звітом про фінансові результати за 2025 рік (Форма №2-дс), витрати на оплату праці персоналу склали понад 280 млрд грн, що свідчить про значну концентрацію ресурсів на підтримці кадрового потенціалу в умовах

воєнного стану. Водночас, аналіз балансу (Форма №1-дс) на 01.01.2026 демонструє суттєве зростання вартості основних засобів — з 262,7 млрд грн до 381 млрд грн. (Додатки Б-Г).

Зростання вартості основних засобів з 262,7 млрд грн до 381 млрд грн свідчить про інтенсивне насичення служби дороговартісним обладнанням. Проте оцінка системи управління виявляє ризик «інвестиційної пастки»: швидкість закупівлі нових технічних засобів (БПЛА, РЕБ) випереджає швидкість підготовки персоналу для їх обслуговування та захисту. У поєднанні з наявністю дебіторської заборгованості це створює ризик неефективного простою дорогої техніки через відсутність витратних матеріалів або кваліфікованого сервісу. Відтак, система управління ризиками повинна включати блок LCC-аналізу (Life Cycle Costing) — оцінку ризику не лише закупівлі, а й повного життєвого циклу активів в умовах інтенсивних бойових дій [7].

Детальний розгляд фінансової звітності (Форма №1-дс) дозволяє виявити прихований ризик, пов'язаний із дебіторською заборгованістю за розрахунками з бюджетом. Станом на 01.01.2026 вона залишається стабільно високою, що в поєднанні із зростанням поточних зобов'язань (за платежами до бюджету — з 1,1 млрд до 4,9 млрд грн) створює касові розриви. Для системи управління ризиками це означає, що плани з модернізації інженерних споруд «інтелектуального кордону» можуть бути недофінансовані в критичні моменти. Такий стан справ вимагає від керівництва ДПСУ впровадження методів стрес-тестування бюджету, щоб забезпечити критичні закупівлі (РЕБ, БПЛА) навіть за умови затримок бюджетних асигнувань [9].

Таке динамічне оновлення матеріально-технічної бази свідчить про активну модернізацію об'єкта управління, проте водночас породжує додаткові ризики щодо ефективності адміністрування та збереження такого обсягу активів у зонах активних бойових дій.

Проведений аналіз фінансових показників свідчить про ресурсну орієнтованість діяльності ДПСУ, де основний акцент зроблено на забезпеченні кадрового потенціалу та матеріально-технічної модернізації. Водночас така структура витрат формує додаткові ризики неефективного використання ресурсів, особливо в умовах обмеженого бюджетного фінансування. Це підсилює необхідність впровадження ризик-орієнтованого бюджетування та посилення контролю за ефективністю витрат.

Важливим елементом системи є антикорупційний контроль. Відповідно до Антикорупційної програми ДПСУ на 2026–2028 роки, у Службі запроваджено механізм ідентифікації корупційних ризиків на основі методології НАЗК. Оцінка цієї підсистеми свідчить про високий ступінь формалізації процедур:

- створено Комісію з оцінки корупційних ризиків;
- впроваджено систему вибірових перевірок (не менше 30%) нарахувань грошових виплат згідно з ПКМУ №168;
- встановлено жорсткий контроль за процесом публічних закупівель [5].

Важливим індикатором ефективності системи управління ризиками є здатність забезпечувати безперебійне фінансування за рахунок бюджетних асигнувань. Дані звітності вказують на збільшення обсягів цільового фінансування (з 42,4 млрд грн до 44,9 млрд грн), що підтверджує пріоритетність безпекового сектору для держави. Однак наявність довгострокових зобов'язань у розмірі 33,1 млрд грн вказує на ризик бюджетного дефіциту та необхідність оптимізації витрат на закупівлю засобів захисту кордону, що корелює з виявленими корупційними ризиками у сфері публічних закупівель.

Окремої оцінки потребує підсистема управління кадровими ризиками. Витрати на оплату праці (280 млрд грн) включають значні виплати за ПКМУ №168, що є потужним стимулом, але водночас формує ризик "соціальної напруги" у разі зміни законодавства. Аналіз Антикорупційної програми

свідчить, що 30% перевірок виплат — це лише механічний контроль. Насправді система потребує глибшого психологічного моніторингу особового складу, який працює в умовах надвисоких ризиків, оскільки саме «людський фактор» стає вирішальним у ланцюгу реалізації як безпекових, так і корупційних загроз.

Однак, незважаючи на значні зусилля, аналіз діючої системи дозволяє виділити низку проблемних аспектів та «слабких місць» (табл. 2.4).

Таблиця 2.4

Слабкі місця та обмеження діючої системи управління ризиками в
ДПСУ

Напрямок оцінки	Виявлені проблеми та обмеження	Наслідки для системи управління
Технологічний	Моральне застаріння окремих елементів системи «Гарт», недостатня кількість мобільних комплексів спостереження	Зниження швидкості ідентифікації ризиків на віддалених ділянках кордону
Організаційний	Недостатня координація між підрозділами внутрішньої безпеки та оперативними загонами у реальному часі	Виникнення «часових вікон» для реалізації корупційних або безпекових загроз
Аналітичний	Переважаючий реактивний підхід (фіксація факту) над предиктивним (прогнозування на основі Big Data)	Несвоєчасне розгортання сил на ділянках з потенційним зростанням загрози
Кадровий	Високе психологічне навантаження та ризик «професійного вигорання» особового складу в умовах війни	Зниження пильності та зростання вразливості до корупційних пропозицій
Фінансово-економічний	Значна дебіторська заборгованість та зростання довгострокових зобов'язань (понад 33 млрд грн)	Ризик затримок у модернізації інженерних споруд через нестабільність розрахунків з підрядниками

Продовження таблиці 2.4

Міжнародно-правовий	Складність синхронізації баз даних із суміжними країнами в реальному часі через різницю у протоколах безпеки	Затримка в ідентифікації осіб, що знаходяться в міжнародному розшуку, на каналах легального перетину
---------------------	--	--

Аналіз наведених у таблиці 2.4 даних свідчить про наявність системних дисбалансів у функціонуванні системи управління ризиками. Зокрема, технологічні та аналітичні обмеження взаємно підсилюють один одного, формуючи ситуацію, коли навіть за наявності значних ресурсів система не здатна повною мірою забезпечити своєчасне виявлення загроз.

Особливо критичним є переважання реактивного підходу до управління, що проявляється у фокусі на ліквідації наслідків, а не на попередженні ризиків. Це суттєво знижує ефективність діяльності ДПСУ в умовах швидкозмінного безпекового середовища.

Оцінка інформаційного обміну в системі управління ризиками вказує на існуючий розрив між збором даних та їх оперативною інтерпретацією. Хоча ДПСУ активно співпрацює з Інтерполом та Європолем, внутрішні алгоритми обробки інформації часто залишаються надмірно бюрократизованими. Це підтверджується статистикою вилучень: різке зростання обсягів контрабанди зброї та вибухівки (з 76,6 кг до 1089 кг) свідчить про те, що система контролю працює в режимі «пікового навантаження», де існуючі методи стримування не завжди встигають за темпами адаптації транскордонної злочинності. Це свідчить про необхідність переходу до централізованих аналітичних платформ, що забезпечують обробку великих масивів даних у режимі реального часу. Впровадження таких рішень дозволить суттєво підвищити точність прогнозування ризиків та ефективність управлінських рішень [55].

Оцінка діючої моделі за критерієм CIRAM 2.0 виявила проблему когнітивного фільтра аналітиків. Через надмірне інформаційне навантаження

(Big Data з камер, супутників, БПЛА) людський мозок схильний ігнорувати слабкі сигнали загрози, фокусуючись лише на явних порушеннях. Це підтверджує, що існуюча «людино центрична» модель вичерпала свій ресурс ефективності. Оцінка вказує на критичну потребу впровадження ML-алгоритмів (Machine Learning) для первинної фільтрації даних, що дозволить звільнити аналітиків від рутинної роботи та сфокусувати їхню увагу на прийнятті стратегічних рішень.

Особливої уваги потребує оцінка управління ризиками в умовах воєнного стану. Діюча система була змушена швидко адаптуватися до ризиків бойових втрат та втрати контролю над окремими ділянками кордону. Впровадження підрозділів аеророзвідки частково вирішило проблему моніторингу, проте системна інтеграція даних з БПЛА в загальну систему ризик-менеджменту наразі знаходиться на стадії становлення.

Оцінка антикорупційної складової через призму фінансової звітності (зобов'язання у 33,1 млрд грн) вказує на ризик «бюджетного волюнтаризму». В умовах дефіциту коштів рішення про пріоритетність фінансування тих чи інших закупівель приймаються в ручному режимі, що автоматично створює корупційне поле. Попри наявність Комісії з оцінки ризиків, система залишається вразливою на етапі формування технічних завдань для тендерів. Це вимагає впровадження організаційного запобіжника — автоматизованого порівняння цін закупівель із ринковими індикаторами в режимі реального часу [5].

Таким чином, оцінка діючої системи управління ризиками в ДПСУ дозволяє зробити висновок про її функціональну спроможність у кризових умовах, проте виявляє критичну потребу в цифровій модернізації та переході до проактивних методів управління. Існуюча система ефективно виявляє вже реалізовані ризики, але потребує вдосконалення механізмів раннього попередження та автоматизації антикорупційного моніторингу, що стане основою для розробки рекомендацій у третьому розділі роботи.

Висновок до розділу 2.

У другому розділі проведено комплексне дослідження Державної прикордонної служби України як об'єкта управління ризиками, проаналізовано динаміку основних загроз та оцінено ефективність діючих механізмів реагування. За результатами аналізу сформульовано такі висновки:

Встановлено, що в умовах воєнного стану ризики транскордонної злочинності набули нових якісних характеристик. Статистичні дані за I квартал 2026 року свідчать про безпрецедентне зростання обсягів вилучених вибухових речовин (у 14 разів порівняно з попереднім роком), наркотичних засобів (у 4 рази) та зброї. Це підтверджує зміщення акцентів протиправної діяльності з дрібної контрабанди у площину організованої злочинності та терористичних загроз, що вимагає перегляду існуючих профілів ризиків.

Аналіз фінансової звітності (Форма №1-дс та №2-дс) засвідчив значне зростання вартості основних засобів (з 262,7 млрд грн до 381 млрд грн), що вказує на інтенсивну технічну модернізацію. Проте встановлено наявність високої дебіторської заборгованості та зростання довгострокових зобов'язань (понад 33,1 млрд грн), що створює ризики фінансової нестабільності та може призводити до затримок у реалізації довгострокових безпекових проектів («інтелектуальний кордон», системи РЕБ).

Встановлено, що реалізація Антикорупційної програми на 2026–2028 роки дозволила формалізувати процеси контролю, зокрема через запровадження вибірових перевірок (не менше 30%) виплат додаткових винагород та аудиту закупівель БПЛА. Водночас виявлено, що корупційні ризики залишаються високими в зонах інтенсивного ресурсного розподілу, що потребує переходу від періодичних перевірок до автоматизованого моніторингу в режимі реального часу.

Основними «слабкими місцями» системи визначено переважання реактивного підходу (реагування на факти порушень) над предиктивним

аналізом. Незважаючи на використання АСПК «Гарт», спостерігається розрив між збором даних та їх оперативною аналітичною інтерпретацією. Встановлено, що існуюча модель управління потребує інтеграції з сучасними аналітичними платформами та впровадження алгоритмів Big Data для прогнозування кризових ситуацій.

Досвід використання підрозділів аеророзвідки та засобів РЕБ показав високу ефективність у виявленні загроз, проте їх дані наразі не повною мірою інтегровані в єдину систему прийняття управлінських рішень. Це підтверджує актуальність розробки рекомендацій щодо вдосконалення системи управління ризиками на засадах цифровізації та проактивності.

Результати проведеного аналізу стають підґрунтям для розробки у третьому розділі конкретних заходів та рекомендацій щодо вдосконалення системи управління ризиками в Державній прикордонній службі України.

РОЗДІЛ 3. НАПРЯМИ УДОСКОНАЛЕННЯ УПРАВЛІННЯ РИЗИКАМИ В ДПСУ

3.1. Впровадження сучасних технологій ризик-менеджменту в Державній прикордонній службі України

В умовах зростання складності безпекового середовища та трансформації характеру загроз, впровадження сучасних технологій ризик-менеджменту в Державній прикордонній службі України набуває стратегічного значення. Проведений у попередньому розділі аналіз дозволив встановити, що ключовою проблемою є наявність «інформаційного розриву» між моментом виявлення загрози та прийняттям управлінського рішення.

У сучасних умовах ефективність управління ризиками визначається здатністю системи працювати з великими обсягами даних у режимі реального часу. Саме тому впровадження новітніх цифрових технологій виступає основою переходу від реактивної до проактивної моделі ризик-менеджменту.

У цьому контексті особливої актуальності набуває питання системної інтеграції технологічних рішень у єдиний інформаційно-аналітичний контур. Розрізнене використання окремих цифрових інструментів не забезпечує належного рівня ефективності управління ризиками, оскільки не дозволяє сформувати цілісне бачення безпекової ситуації. Натомість комплексний підхід, що передбачає поєднання джерел даних, аналітичних платформ та механізмів прийняття рішень, створює основу для безперервного моніторингу та своєчасного реагування на загрози [28].

Для наочного відображення ролі сучасних технологій у системі управління ризиками доцільно представити відповідну структурну схему (рис. 3.1).



Рис. 3.1. Модель технологічно орієнтованої системи управління ризиками в ДПСУ

Як видно з рис. 3.1, сучасна система управління ризиками базується на безперервному інформаційно-аналітичному циклі, в якому кожен етап тісно пов'язаний із попереднім. Використання технологій Big Data та штучного інтелекту забезпечує не лише обробку значних обсягів інформації, але й формування аналітичних висновків, що лежать в основі прийняття управлінських рішень.

Важливою особливістю такої моделі є наявність зворотного зв'язку, який дозволяє постійно оновлювати базу даних та адаптувати систему до змін у безпековому середовищі. Це забезпечує її гнучкість та здатність до самонавчання, що є ключовою умовою ефективного функціонування в сучасних умовах.

Першим ключовим напрямом є впровадження технологій Big Data та предиктивної аналітики. Зростання обсягів вилученої зброї, вибухових

речовин та наркотичних засобів свідчить про ускладнення структури транскордонної злочинності, що робить традиційні методи контролю недостатньо ефективними.

Важливим елементом технологічного вдосконалення є автоматизація процесів прийняття управлінських рішень. Використання сучасних інформаційних систем дозволяє формувати рекомендації щодо реагування на ризики на основі заздалегідь визначених алгоритмів та сценаріїв. Це значно скорочує час реагування та мінімізує вплив суб'єктивних факторів.

Автоматизовані системи підтримки прийняття рішень можуть інтегрувати дані з різних джерел, оцінювати рівень загрози та пропонувати оптимальні варіанти дій. Такий підхід особливо ефективний у ситуаціях, що потребують оперативного реагування, зокрема при виявленні спроб незаконного перетину кордону або переміщення заборонених предметів [42].

Практична реалізація цього напрямку передбачає створення єдиного інтегрованого аналітичного середовища, яке об'єднує дані автоматизованих систем прикордонного контролю, відеоспостереження, міжнародних баз даних та відкритих джерел інформації (OSINT). Використання таких платформ дозволяє формувати поведінкові профілі ризику та виявляти аномальні дії ще до моменту реалізації правопорушення.

Другим напрямом є впровадження технологій штучного інтелекту та машинного навчання. Застосування алгоритмів AI дозволяє автоматизувати процеси аналізу даних, знижуючи вплив людського фактору та підвищуючи точність прогнозування ризиків.

Особливо ефективним є використання таких технологій у сфері антикорупційного контролю. Автоматизований аналіз фінансових операцій, службових дій та управлінських рішень дозволяє виявляти потенційні зловживання на ранніх стадіях, що суттєво знижує рівень внутрішніх ризиків.

Окремим напрямом технологічного розвитку системи управління ризиками є забезпечення кібербезпеки та захисту інформаційних ресурсів. В

умовах цифровізації діяльності ДПСУ інформаційні системи стають не лише інструментом управління, але й об'єктом потенційних загроз. Несанкціонований доступ до баз даних, кібератаки або втручання в роботу автоматизованих систем можуть призвести до витоку службової інформації або спотворення даних, що безпосередньо впливає на якість прийняття управлінських рішень [39].

У зв'язку з цим доцільним є впровадження комплексних систем кіберзахисту, що включають багаторівневу автентифікацію, криптографічний захист даних, системи виявлення вторгнень та безперервний моніторинг інформаційних потоків. Реалізація таких заходів дозволяє підвищити стійкість системи управління ризиками до зовнішніх і внутрішніх кіберзагроз.

Третім напрямом є розвиток систем відеоаналітики та інтелектуального спостереження. Використання сучасних камер із функціями розпізнавання об'єктів, номерних знаків та поведінкових характеристик дозволяє значно підвищити ефективність контролю на пунктах пропуску та прикордонних ділянках.

Інтеграція таких систем із аналітичними платформами створює можливість автоматичного формування сигналів ризику, що забезпечує оперативне реагування на потенційні загрози.

Четвертим напрямом є використання безпілотних авіаційних комплексів та сенсорних систем моніторингу. В умовах воєнного стану такі технології відіграють ключову роль у забезпеченні контролю за важкодоступними ділянками кордону.

Інтеграція даних із безпілотних систем у єдину інформаційну систему дозволяє формувати динамічні карти ризиків у режимі реального часу, що значно підвищує ефективність управління прикордонною безпекою.

П'ятим напрямом є впровадження хмарних технологій та міжвідомчого обміну даними. Синхронізація інформаційних систем із міжнародними

партнерами забезпечує доступ до актуальної інформації та сприяє підвищенню ефективності виявлення транскордонних загроз [44].

Для узагальнення запропонованих технологічних рішень доцільно представити їх у вигляді таблиці.

Таблиця 3.1

Основні технології ризик-менеджменту в діяльності ДПСУ

Технологія	Сутність	Ефект
Big Data	Аналіз великих масивів даних	Прогнозування ризиків
AI	Автоматизація аналізу	Зниження людського фактору
Відеоаналітика	Інтелектуальне спостереження	Швидке виявлення загроз
БПЛА	Дистанційний моніторинг	Контроль складних ділянок
Хмарні технології	Обмін даними	Підвищення ефективності

Аналіз представлених у таблиці 3.1 технологічних рішень свідчить про їх комплексний характер та взаємодоповнюваність. Кожна із запропонованих технологій виконує окрему функцію в системі управління ризиками, проте максимальний ефект досягається лише за умови їх інтегрованого використання. Зокрема, технології Big Data забезпечують накопичення та структурування інформації, алгоритми штучного інтелекту — її аналітичну обробку, тоді як системи відеоаналітики та безпілотного моніторингу виступають джерелами первинних даних.

Важливим аспектом є те, що впровадження зазначених технологій дозволяє суттєво скоротити часовий інтервал між виявленням загрози та прийняттям управлінського рішення. Це безпосередньо сприяє усуненню «інформаційного розриву», який був визначений як ключова проблема у функціонуванні системи управління ризиками ДПСУ.

Слід також підкреслити, що впровадження сучасних технологій ризик-менеджменту має не лише безпековий, але й економічний ефект. Оптимізація процесів контролю дозволяє більш раціонально використовувати кадрові та

матеріально-технічні ресурси, зменшуючи витрати на проведення перевірок та підвищуючи їх результативність.

Автоматизація процесів аналізу ризиків сприяє зниженню кількості помилкових спрацьовувань систем контролю, що дозволяє зосередити увагу на найбільш критичних загрозах. У довгостроковій перспективі це забезпечує підвищення загальної ефективності функціонування ДПСУ та покращення показників її діяльності [60].

Крім того, інтеграція цифрових технологій створює передумови для формування єдиного інформаційного простору безпеки, в межах якого забезпечується безперервний обмін даними між різними рівнями управління та суміжними органами. Такий підхід відповідає сучасним міжнародним стандартам у сфері інтегрованого управління кордонами та підвищує загальну ефективність функціонування служби.

Впровадження сучасних технологій ризик-менеджменту також сприяє гармонізації діяльності ДПСУ із європейськими стандартами інтегрованого управління кордонами. Використання цифрових інструментів, аналітичних систем та автоматизованих процедур відповідає практикам країн ЄС та підвищує рівень взаємодії з міжнародними партнерами у сфері безпеки.

Узагальнюючи, слід зазначити, що технологічна модернізація системи управління ризиками має не фрагментарний, а системний характер, оскільки передбачає трансформацію всієї логіки управління — від реагування на загрози до їх прогнозування та попередження.

Таким чином, впровадження сучасних технологій ризик-менеджменту створює основу для формування проактивної моделі управління ризиками в Державній прикордонній службі України. Реалізація зазначених напрямів дозволить підвищити оперативність реагування на загрози, знизити вплив людського фактору та забезпечити більш ефективне використання ресурсів, що є особливо важливим в умовах воєнного стану.

3.2. Підвищення ефективності організаційного управління ризиками в ДПСУ

У сучасних умовах підвищення ефективності управління ризиками в Державній прикордонній службі України неможливе без удосконалення організаційних механізмів функціонування системи. Проведений у попередніх розділах аналіз засвідчив, що поряд із технологічними обмеженнями вагомим стримуючим фактором є недосконалість координації та переважання реактивного підходу.

Слід зазначити, що організаційний аспект управління ризиками відіграє визначальну роль у забезпеченні ефективності функціонування всієї системи, оскільки саме через організаційні механізми реалізуються аналітичні висновки та управлінські рішення. Недостатня узгодженість дій між структурними підрозділами, нечіткий розподіл функцій та повноважень, а також надмірна бюрократизація процесів можуть суттєво знижувати результативність навіть за наявності сучасного технічного забезпечення.

Особливої актуальності це набуває в умовах воєнного стану, коли швидкість прийняття рішень та їх адекватність безпосередньо впливають на рівень національної безпеки. За таких умов будь-які затримки в передачі інформації або неузгодженість дій можуть призводити до реалізації критичних ризиків, пов'язаних із незаконним переміщенням зброї, діяльністю диверсійних груп або іншими загрозами.

Дослідження існуючої вертикалі управління вказує на наявність явища «інформаційного шуму» при передачі даних від тактичного рівня (прикордонний наряд, блокпост) до стратегічного (Адміністрація ДПСУ). Організаційна структура наразі переобтяжена проміжними ланками звітності, що призводить до втрати актуальності ризик-індикаторів [15].

Крім того, значна кількість рівнів погодження управлінських рішень спричиняє уповільнення процесу реагування на зміну безпекової ситуації. У

результаті система функціонує переважно в режимі реагування на вже реалізовані загрози, а не їх попередження, що суперечить сучасним підходам до управління ризиками.

Відтак, організаційне вдосконалення має базуватися на принципах «плоскої структури» (Flat Organization) у частині обміну безпековими даними, що дозволить скоротити час реакції на критичні загрози, такі як прорив диверсійно-розвідувальних груп чи зміна тактики контрабандних угруповань.

Важливо підкреслити, що впровадження елементів «плоскої» організаційної структури не означає повної відмови від ієрархічної моделі управління, а передбачає оптимізацію інформаційних потоків і скорочення надлишкових ланок комунікації. Це дозволяє зберегти керованість системи, одночасно підвищуючи її гнучкість та адаптивність [18].

З метою підвищення ефективності системи доцільним є впровадження ризик-орієнтованої організаційної моделі, яка базується на принципах централізованого аналізу та децентралізованого реагування. Такий підхід забезпечує поєднання високої якості аналітичної обробки інформації з оперативністю прийняття рішень на місцях (рис. 3.2).



Рис. 3.2. Організаційна модель управління ризиками в ДПСУ

Як видно з рис. 3.2, ключову роль у системі відіграє аналітичний центр ризиків, який акумулює інформацію з різних джерел, здійснює її обробку та формує управлінські рішення. Такий центр може функціонувати як окремий структурний підрозділ або як інтегрована платформа в межах існуючих організаційних структур.

Ключовою функцією запропонованого Аналітичного центру ризиків має стати не лише моніторинг безпекової ситуації, але й проведення фінансового стрес-тестування управлінських рішень. Враховуючи значний обсяг довгострокових зобов'язань, будь-які зміни в організації охорони кордону повинні супроводжуватися оцінкою їх ресурсного забезпечення. Такий підхід дозволить уникнути дисбалансу між оперативними потребами та фінансовими можливостями, а також забезпечити стабільність функціонування системи в умовах обмежених ресурсів.

Зазначена організаційна модель дозволяє суттєво зменшити втрати інформації при її передачі між рівнями управління. Завдяки концентрації аналітичної функції в єдиному центрі забезпечується узгодженість управлінських рішень та уніфікація підходів до оцінки ризиків. Водночас делегування повноважень на рівень оперативних підрозділів сприяє підвищенню швидкості реагування на загрози, що є критично важливим в умовах воєнного стану [20].

Така модель створює передумови для підвищення відповідальності на кожному рівні управління, оскільки чітко визначає функціональні ролі та зони відповідальності, що мінімізує ризик дублювання управлінських функцій.

Важливим напрямом удосконалення організаційного управління є підвищення рівня координації між підрозділами. Це передбачає впровадження єдиних стандартів обміну інформацією, скорочення часу передачі даних та усунення дублювання функцій.

Доцільним є запровадження комплексної системи внутрішнього контролю за управлінням ризиками, яка повинна охоплювати не лише регулярний моніторинг діяльності підрозділів, але й системну оцінку ефективності прийнятих управлінських рішень, а також своєчасне виявлення відхилень від встановлених стандартів і процедур. Така система має функціонувати на постійній основі та бути інтегрованою в загальну модель управління ризиками, забезпечуючи безперервний зворотний зв'язок між рівнями управління.

Ефективний внутрішній контроль виконує не лише функцію виявлення порушень, але й превентивну роль, формуючи середовище, у якому ризики мінімізуються ще на етапі їх виникнення. Це особливо актуально для діяльності ДПСУ, де ціна управлінських помилок може мати критичні наслідки для національної безпеки.

Організаційне посилення внутрішнього контролю повинно базуватися на положеннях Антикорупційної програми ДПСУ на 2026–2028 роки. У цьому контексті доцільним є перехід від традиційної моделі періодичних інспекцій до створення постійно діючих груп моніторингу доброчесності. Основним завданням таких груп на рівні регіональних управлінь має стати проведення превентивного аудиту найбільш ризикованих процесів, зокрема у сфері державних закупівель спеціальних технічних засобів та обґрунтованості нарахування додаткових виплат відповідно до ПКМУ №168.

Запровадження такого підходу дозволить змінити концепцію внутрішнього контролю з орієнтації на «виявлення та покарання» до моделі «попередження та усунення умов виникнення порушень». Це сприятиме підвищенню рівня прозорості управлінських процесів, зміцненню довіри до системи та зниженню корупційних ризиків [5].

Водночас важливим напрямом організаційного вдосконалення є оновлення внутрішніх регламентів та процедур управління ризиками. Чітке документування управлінських процесів, визначення алгоритмів дій у

типових і кризових ситуаціях, а також стандартизація процедур прийняття рішень дозволяють суттєво знизити рівень невизначеності та підвищити узгодженість дій структурних підрозділів.

Крім того, регламентація процесів сприяє підвищенню відповідальності посадових осіб, оскільки забезпечує прозорість розподілу функцій та повноважень. У результаті це дозволяє мінімізувати ризики дублювання функцій, уникнути управлінських конфліктів та підвищити загальну ефективність функціонування системи управління ризиками в ДПСУ.

Для систематизації основних організаційних заходів доцільно представити їх у вигляді таблиці.

Таблиця 3.2

Основні напрями удосконалення організаційного управління ризиками
в ДПСУ

Напрямок	Зміст заходу	Очікуваний ефект
Координація	Впровадження єдиних стандартів взаємодії	Скорочення часу реагування
Централізація аналізу	Створення аналітичного центру	Підвищення якості рішень
Децентралізація реагування	Надання повноважень підрозділам	Оперативність дій
Контроль	Внутрішній аудит ризиків	Зниження управлінських помилок
Регламентація	Чіткий розподіл повноважень	Усунення дублювання функцій

Аналіз представлених у таблиці 3.2 заходів свідчить про їх взаємозалежність та комплексний характер. Реалізація кожного із зазначених напрямів окремо не забезпечить суттєвого підвищення ефективності системи, тоді як їх поєднання створює синергетичний ефект.

Зокрема, підвищення рівня координації без належного контролю може призвести до зростання управлінських ризиків, тоді як централізація

аналітичних функцій без децентралізації реагування уповільнює процес прийняття рішень. Таким чином, ефективність організаційного управління визначається збалансованістю впроваджених змін.

Водночас підвищення ефективності організаційного управління неможливе без розвитку кадрового потенціалу. Необхідним є впровадження системи підготовки та підвищення кваліфікації персоналу у сфері управління ризиками, що сприятиме формуванню відповідних компетенцій та підвищенню якості управлінських рішень [53].

Особливу увагу слід приділити формуванню ризик-орієнтованого мислення у персоналу. Це передбачає не лише формальне навчання, але й інтеграцію принципів ризик-менеджменту у повсякденну діяльність підрозділів. Працівники повинні бути здатними самостійно ідентифікувати потенційні загрози та приймати обґрунтовані рішення в умовах невизначеності.

У цьому контексті доцільним є впровадження системи безперервного професійного розвитку, що включає тренінги, моделювання кризових ситуацій та обмін досвідом між підрозділами. Це дозволить підвищити адаптивність персоналу та його готовність до реагування на нові виклики.

Організаційна модель буде дієвою лише за умови перегляду системи мотивації. Витрати на оплату праці у розмірі 280 млрд грн свідчать про те, що персонал є головним активом. Організаційне удосконалення має включати впровадження КРІ (ключових показників ефективності) для офіцерів-аналітиків, де основним критерієм буде не кількість складених звітів, а відсоток попереджених правопорушень. Також, з огляду на «пікове навантаження», про яке свідчить статистика вилучень зброї та вибухівки, необхідно організаційно закріпити ротаційні цикли для запобігання професійному вигоранню особового складу [15].

Таким чином, удосконалення організаційного управління ризиками в Державній прикордонній службі України передбачає комплексний підхід, що

включає оптимізацію структури управління, підвищення рівня координації, розвиток кадрового потенціалу та впровадження ефективних механізмів контролю. Реалізація зазначених заходів дозволить підвищити ефективність функціонування системи управління ризиками та забезпечити належний рівень прикордонної безпеки в умовах сучасних викликів.

3.3. Розробка практичних рекомендацій щодо мінімізації ризиків у ДПСУ

В умовах сучасних безпекових викликів, зумовлених воєнним станом, транснаціональною злочинністю та високим рівнем невизначеності зовнішнього середовища, питання мінімізації ризиків у діяльності Державної прикордонної служби України набуває особливої актуальності. Динамічний характер загроз, їх взаємопов'язаність та здатність швидко трансформуватися вимагають від системи управління ризиками не лише оперативного реагування, але й здатності до прогнозування та попередження негативних явищ.

Проведений у попередніх підрозділах аналіз дозволив виявити ключові проблеми функціонування системи управління ризиками, що пов'язані з технологічними обмеженнями, організаційною неузгодженістю та недостатнім рівнем превентивного управління. Встановлено, що існуюча система значною мірою орієнтована на реагування на вже реалізовані загрози, що знижує її ефективність в умовах зростання складності безпекового середовища.

Недостатня інтегрованість інформаційних потоків, обмеженість аналітичних інструментів та недосконалість механізмів внутрішнього контролю створюють передумови для виникнення додаткових ризиків, у тому числі корупційного та організаційного характеру. Це обумовлює необхідність переходу до комплексного підходу в управлінні ризиками, який

передбачає одночасне вдосконалення технологічних, організаційних та кадрових складових.

З огляду на це, доцільним є формування комплексної системи практичних рекомендацій, спрямованих на підвищення ефективності управління ризиками, що охоплює технологічний, організаційний, кадровий та контрольний напрями [5].

Для наочного відображення основних напрямів мінімізації ризиків у діяльності Державної прикордонної служби України доцільно представити їх у вигляді структурної схеми (рис. 3.3).

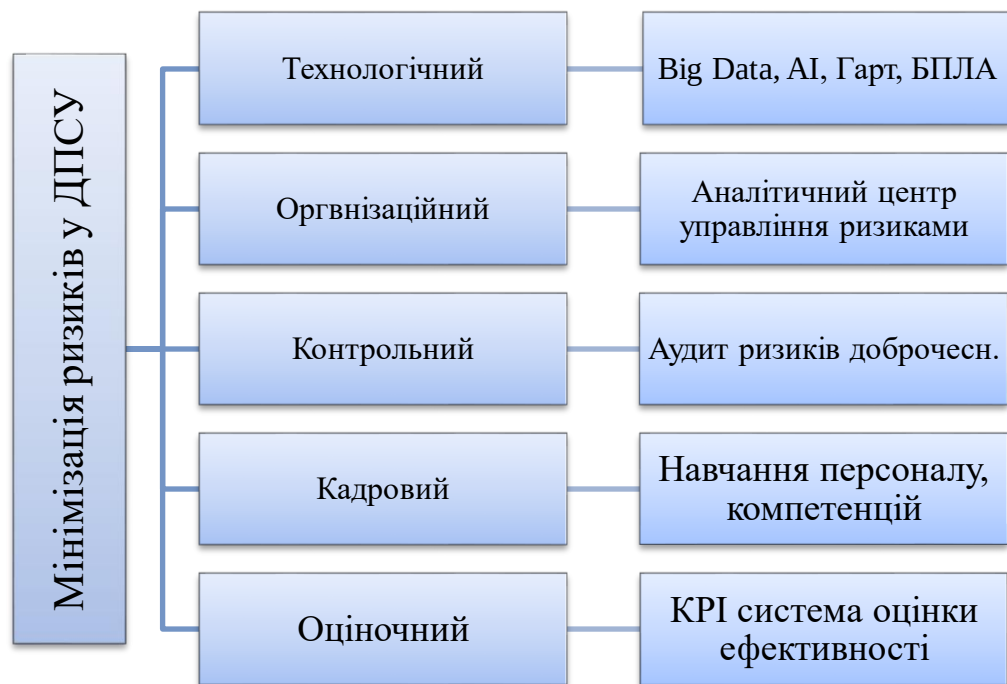


Рис. 3.3. Основні напрями мінімізації ризиків у ДПСУ

Як показано на рис. 3.3, система мінімізації ризиків має комплексний характер і охоплює взаємопов'язані напрями, кожен з яких виконує окрему функцію в загальній системі управління. Технологічний напрям забезпечує інформаційно-аналітичну основу, організаційний — формує структуру прийняття рішень, контрольний — спрямований на попередження порушень,

кадровий — забезпечує людський потенціал, тоді як оціночний напрям дозволяє здійснювати моніторинг ефективності функціонування системи.

Взаємодія зазначених елементів створює цілісну модель управління ризиками, орієнтовану на попередження загроз та підвищення ефективності діяльності ДПСУ в умовах сучасних викликів.

Першим напрямом є впровадження інтегрованої цифрової платформи управління ризиками. Така платформа повинна об'єднувати дані з усіх наявних інформаційних систем, включаючи АСПК «Гарт», результати відеоспостереження, дані безпілотних авіаційних комплексів та інформацію з відкритих джерел. Практична реалізація цього заходу передбачає створення єдиного аналітичного середовища, яке забезпечить автоматизовану обробку даних та формування ризик-профілів у режимі реального часу [61].

Другим напрямом є вдосконалення організаційної структури управління ризиками. Зокрема, пропонується створення Аналітичного центру ризиків як ключового координаційного елементу системи, що здійснюватиме централізований аналіз інформації та формування управлінських рішень. Одночасно необхідно забезпечити децентралізацію функцій реагування, надавши оперативним підрозділам більшу автономію у прийнятті рішень в межах визначених повноважень.

Третім напрямом є впровадження системи превентивного внутрішнього контролю. Рекомендується створення постійно діючих груп моніторингу доброчесності, основною функцією яких стане проведення превентивного аудиту найбільш ризикованих процесів, таких як державні закупівлі та нарахування грошових виплат. Це дозволить мінімізувати корупційні ризики та підвищити прозорість управлінських процедур.

Четвертим напрямом є розвиток кадрового потенціалу у сфері управління ризиками. Доцільним є впровадження системи безперервного навчання персоналу, що включає тренінги з аналізу ризиків, моделювання кризових ситуацій та використання сучасних цифрових інструментів.

Особливу увагу слід приділити формуванню аналітичного мислення та здатності приймати рішення в умовах невизначеності.

П'ятим напрямом є впровадження системи оцінки ефективності управління ризиками на основі ключових показників результативності (KPI). Зокрема, до таких показників можуть бути віднесені: рівень попереджених правопорушень, швидкість реагування на загрози, ефективність використання ресурсів та рівень виявлених корупційних порушень. Це дозволить здійснювати об'єктивну оцінку діяльності підрозділів та підвищити відповідальність персоналу [41].

Для систематизації запропонованих рекомендацій доцільно представити їх у вигляді таблиці (табл. 3.3).

Таблиця 3.3

Практичні рекомендації щодо мінімізації ризиків у ДПСУ

Напрямок	Зміст рекомендації	Очікуваний ефект
Технологічний	Створення інтегрованої цифрової платформи	Підвищення швидкості обробки даних
Організаційний	Формування аналітичного центру ризиків	Покращення якості управлінських рішень
Контрольний	Впровадження превентивного аудиту	Зниження корупційних ризиків
Кадровий	Розвиток компетенцій персоналу	Підвищення ефективності діяльності
Оціночний	Впровадження системи KPI	Об'єктивізація управління

Аналіз представлених у таблиці 3.3 рекомендацій свідчить про їх комплексний та взаємопов'язаний характер. Кожен із запропонованих напрямів спрямований на усунення конкретних недоліків, виявлених у процесі дослідження, однак їх ефективність значною мірою залежить від узгодженості впровадження.

Зокрема, технологічні рішення забезпечують підвищення швидкості та точності обробки інформації, тоді як організаційні заходи створюють умови для оперативного використання отриманих аналітичних результатів. У свою

чергу, кадрові та контрольні інструменти формують середовище, в якому мінімізується вплив людського фактора та підвищується відповідальність за прийняті рішення.

Тож, запропонована система рекомендацій має інтегрований характер і спрямована на формування цілісної моделі управління ризиками, що поєднує аналітичну, організаційну та контрольну складові.

Для забезпечення практичної реалізації запропонованих рекомендацій доцільно визначити поетапний механізм їх впровадження, який дозволить мінімізувати організаційні ризики та забезпечити керованість процесу змін (рис.3.4).



Рис. 3.4. Етапи впровадження системи управління ризиками в ДПСУ

Як показано на рис. 3.4, процес впровадження системи управління ризиками має поетапний та логічно узгоджений характер. Кожен із етапів виконує окрему функцію, формуючи цілісний механізм трансформації системи управління [44].

На першому етапі (підготовчому) необхідно здійснити аудит існуючої системи управління ризиками, включаючи оцінку технічного забезпечення,

організаційної структури та кадрового потенціалу. Результатом даного етапу має стати визначення пріоритетних напрямів модернізації та формування дорожньої карти змін.

Другий етап (організаційно-структурний) передбачає створення Аналітичного центру ризиків, перегляд функціональних обов'язків підрозділів та оптимізацію інформаційних потоків. На цьому етапі важливим є забезпечення чіткого розподілу повноважень та відповідальності між рівнями управління.

Третій етап (технологічний) включає впровадження інтегрованої цифрової платформи, налагодження обміну даними між інформаційними системами та інтеграцію результатів моніторингу у процес прийняття рішень. Особливу увагу слід приділити автоматизації аналітичних процесів.

Четвертий етап (кадрово-функціональний) передбачає підготовку персоналу до роботи в нових умовах, впровадження системи навчання та формування компетенцій у сфері ризик-менеджменту.

П'ятий етап (контрольно-оцінювальний) включає впровадження системи KPI та механізмів внутрішнього контролю, що дозволяють оцінити ефективність функціонування системи та своєчасно коригувати її роботу.

Послідовна реалізація зазначених етапів дозволить забезпечити поступовий перехід до сучасної моделі управління ризиками без суттєвих організаційних потрясінь. Запропонована поетапна модель впровадження дозволяє забезпечити системність, послідовність та контрольованість процесу вдосконалення управління ризиками в Державній прикордонній службі України [5].

Оцінка економічної ефективності запропонованих заходів є важливим елементом обґрунтування їх доцільності. Враховуючи значні обсяги фінансування діяльності ДПСУ, навіть незначне підвищення ефективності використання ресурсів може забезпечити відчутний економічний ефект.

Зокрема, якщо припустити, що впровадження інтегрованої системи управління ризиками дозволить знизити рівень неефективних витрат лише на 3–5%, то за умов річного фінансування на рівні понад 40 млрд грн економія може становити від 1,2 до 2 млрд грн. Додатковий ефект може бути досягнутий за рахунок зменшення втрат від контрабанди, підвищення ефективності використання матеріально-технічних ресурсів та оптимізації кадрового навантаження.

Крім прямого економічного ефекту, слід враховувати і непрямі вигоди, зокрема підвищення рівня безпеки, зниження корупційних ризиків, зміцнення міжнародного іміджу держави та підвищення довіри до прикордонної служби [56].

Як бачимо, впровадження запропонованих заходів є економічно доцільним та обґрунтованим як з точки зору оптимізації витрат, так і підвищення загальної ефективності функціонування системи.

Реалізація запропонованих практичних рекомендацій дозволить сформувати сучасну, ефективну та адаптивну систему управління ризиками в Державній прикордонній службі України, здатну забезпечити належний рівень прикордонної безпеки в умовах сучасних викликів.

Запропонований комплекс заходів охоплює ключові напрями вдосконалення системи — технологічний, організаційний, кадровий та контрольний, що забезпечує їх системний характер та взаємодоповнюваність. Впровадження інтегрованих цифрових рішень сприятиме підвищенню швидкості обробки інформації та точності оцінки ризиків, тоді як удосконалення організаційної структури дозволить забезпечити ефективну координацію між рівнями управління.

Особливе значення має розвиток кадрового потенціалу та формування ризик-орієнтованого мислення персоналу, що є необхідною умовою переходу від реактивної до проактивної моделі управління. Запровадження системи внутрішнього контролю та оцінки ефективності діяльності підрозділів

забезпечить прозорість управлінських процесів та своєчасне виявлення відхилень.

Важливою перевагою запропонованих рекомендацій є їх практична спрямованість та можливість поетапного впровадження, що дозволяє мінімізувати організаційні ризики та забезпечити керованість процесу змін. Це створює передумови для підвищення стійкості системи управління ризиками до зовнішніх загроз та внутрішніх викликів.

Отже, запропоновані заходи формують основу для переходу до інтегрованої, проактивної та технологічно орієнтованої моделі управління ризиками, що відповідає сучасним вимогам безпеки та сприяє зміцненню прикордонної безпеки держави.

Висновок до розділу 3.

У третьому розділі дипломної роботи було обґрунтовано напрями вдосконалення системи управління ризиками в Державній прикордонній службі України з урахуванням сучасних безпекових викликів та результатів проведеного аналізу.

Зокрема, визначено, що ключовою умовою підвищення ефективності управління ризиками є впровадження сучасних цифрових технологій, які забезпечують обробку великих обсягів інформації в режимі реального часу та дозволяють перейти від реактивної до проактивної моделі управління. Запропоновано інтеграцію технологій Big Data, штучного інтелекту та автоматизованих аналітичних систем у діяльність ДПСУ, що сприятиме підвищенню точності оцінки ризиків та своєчасності прийняття управлінських рішень.

Водночас доведено, що технологічне оновлення має супроводжуватися вдосконаленням організаційних механізмів управління. У цьому контексті обґрунтовано доцільність впровадження ризик-орієнтованої організаційної

моделі, яка передбачає поєднання централізованого аналізу інформації та децентралізованого реагування. Запропоновано створення Аналітичного центру ризиків, оптимізацію інформаційних потоків та підвищення рівня координації між підрозділами.

Окрему увагу приділено розвитку кадрового потенціалу та вдосконаленню системи внутрішнього контролю. Визначено, що підвищення ефективності управління ризиками неможливе без формування відповідних компетенцій персоналу, впровадження системи безперервного навчання та запровадження механізмів оцінки результативності діяльності на основі ключових показників ефективності.

На основі узагальнення отриманих результатів розроблено комплекс практичних рекомендацій щодо мінімізації ризиків у діяльності ДПСУ, які охоплюють технологічний, організаційний, кадровий та контрольний напрями. Запропоновано поетапний механізм їх впровадження, що забезпечує системність, послідовність та керованість процесу трансформації.

Отже, реалізація запропонованих заходів дозволить сформувати сучасну, ефективну та адаптивну систему управління ризиками, здатну забезпечити належний рівень прикордонної безпеки, підвищити стійкість до зовнішніх і внутрішніх загроз та сприяти інтеграції України до європейського безпекового простору.

ВИСНОВКИ

У процесі виконання дипломної роботи було здійснено комплексне дослідження теоретичних, методичних та практичних аспектів управління ризиками в діяльності Державної прикордонної служби України в умовах сучасних безпекових викликів.

У першому розділі досліджено сутність ризику як економічної та управлінської категорії, розкрито його основні характеристики та здійснено класифікацію ризиків у системі управління. Визначено, що ризик є невід'ємною складовою діяльності будь-якої організації, а ефективне управління ним передбачає системний підхід, який включає ідентифікацію, оцінку, аналіз та мінімізацію негативних наслідків. Узагальнено принципи та методи управління ризиками, серед яких ключове місце займають превентивність, системність, безперервність та адаптивність. Окрему увагу приділено особливостям управління ризиками в органах державної влади та секторі безпеки, де ризики мають підвищений рівень складності, динамічності та соціальної значущості.

У другому розділі проведено аналіз діяльності Державної прикордонної служби України як об'єкта управління та досліджено існуючу систему управління ризиками. Встановлено, що в умовах воєнного стану та трансформації характеру загроз діяльність ДПСУ супроводжується широким спектром ризиків, серед яких ключовими є ризики транскордонної злочинності, корупційні ризики, а також ризики, пов'язані з воєнною агресією та безпековою нестабільністю. Аналіз статистичних даних засвідчив зростання обсягів незаконного переміщення зброї, наркотичних засобів та вибухових речовин, що свідчить про ускладнення безпекового середовища.

Оцінка діючої системи управління ризиками дозволила встановити, що вона характеризується наявністю багаторівневої структури управління, використанням автоматизованих інформаційних систем та впровадженням антикорупційних механізмів. Водночас виявлено низку проблем, зокрема:

переважання реактивного підходу, недостатній рівень інтеграції інформаційних потоків, обмеженість аналітичних інструментів, а також наявність організаційних та кадрових обмежень. Це зумовлює необхідність удосконалення системи управління ризиками на основі сучасних підходів.

У третьому розділі обґрунтовано напрями вдосконалення системи управління ризиками в ДПСУ. Запропоновано впровадження сучасних технологій ризик-менеджменту, зокрема використання Big Data, штучного інтелекту та інтегрованих цифрових платформ, що забезпечують обробку інформації в режимі реального часу та підвищують точність прогнозування ризиків. Доведено доцільність удосконалення організаційної структури шляхом впровадження ризик-орієнтованої моделі управління, створення Аналітичного центру ризиків та оптимізації інформаційних потоків.

Розроблено комплекс практичних рекомендацій щодо мінімізації ризиків у діяльності ДПСУ, який охоплює технологічний, організаційний, кадровий та контрольний напрями. Запропоновано поетапний механізм їх впровадження, що дозволяє забезпечити системність, послідовність та ефективність процесу змін. Особливу увагу приділено розвитку кадрового потенціалу, впровадженню системи внутрішнього контролю та оцінці ефективності управління на основі ключових показників результативності.

Отже, результати проведеного дослідження підтверджують, що підвищення ефективності управління ризиками в Державній прикордонній службі України можливе за умови комплексного поєднання технологічних інновацій, організаційних змін та розвитку людського капіталу. Реалізація запропонованих заходів сприятиме формуванню сучасної, проактивної та адаптивної системи управління ризиками, що відповідає міжнародним стандартам та забезпечує належний рівень прикордонної безпеки держави.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Конституція України : Закон від 28.06.1996 № 254к/96-ВР.
2. Про Державну прикордонну службу України : Закон України від 03.04.2003 № 661-IV.
3. Про прикордонний контроль : Закон України від 05.11.2009 № 1710-VI.
4. Про запобігання корупції : Закон України від 14.10.2014 № 1700-VII.
5. Антикорупційна програма Державної прикордонної служби України на 2026–2028 роки. – К. : Адміністрація ДПСУ, 2026. – 45 с.
6. Питання грошового забезпечення військовослужбовців : Постанова Кабінету Міністрів України від 28.02.2022 № 168.
7. Баланс Державної прикордонної служби України на 01 січня 2026 року (Форма № 1-дс).
8. Звіт про фінансові результати ДПСУ за 2025 рік (Форма № 2-дс).
9. Звіт про рух грошових коштів ДПСУ за 2025 рік (Форма № 3-дс).
10. Примітки до річної фінансової звітності ДПСУ за 2025 рік (Форма № 5-дс).
11. Адізес І. Управління в часи кризи. – К. : Наш Формат, 2021. – 224 с.
12. Ансофф І. Стратегічне управління. – К. : Знання, 2022. – 344 с.
13. Друкер П. Практика менеджменту. – К. : Вільямс, 2020. – 398 с.
14. Єльнікова Г. В. Управління організацією. – Х. : Основа, 2021. – 288 с.
15. Журавський В. С. Державний менеджмент. – К. : Освіта, 2020. – 312 с.
16. Калініна Л. М. Управління закладом. – К. : Педагогічна думка, 2020. – 256 с.
17. Карамушка Л. М. Психологія управління: навч. посіб. – К., 2022. – 296 с.
18. Кузьмін О. Є. Основи менеджменту. – Львів : Світ, 2021. – 360 с.
19. Мескон М. Основи менеджменту. – К. : Дело, 2018. – 704 с.
20. Осовська Г. В. Менеджмент організацій. – К. : Кондор, 2020. – 366 с.
21. Савченко О. Я. Дидактика менеджменту. – К. : Освіта, 2022. – 512 с.

- 22.Вітлінський В. В. Ризикологія в економіці та підприємстві. – К. : КНЕУ, 2021. – 480 с.
- 23.Донець Л. І. Економічні ризики та методи їх вимірювання. – К. : Центр навчальної літератури, 2022. – 312 с.
- 24.Ілляшенко С. М. Менеджмент ризиків. – Суми : Університетська книга, 2020. – 256 с.
- 25.Клименко С. М. Обґрунтування господарських рішень і оцінка ризиків. – К. : КНЕУ, 2023. – 248 с.
- 26.Машина Н. І. Економічний ризик і методи його вимірювання. – К. : Центр навчальної літератури, 2022. – 188 с.
- 27.Шемаєва Л. Г. Економічна безпека підприємства. – К. : Центр навчальної літератури, 2020. – 232 с.
- 28.Биков В. Ю. Цифрова трансформація управління // Інформаційні технології. – 2020. – № 3. – С. 15–27.
- 29.Гриньова В. М. Управління якістю процесів // Педагогіка. – 2021. – № 4. – С. 45–52.
- 30.Даниленко Л. І. Менеджмент у системі безпеки // Освіта і управління. – 2020. – № 2. – С. 23–30.
- 31.Єльнікова Г. В. Внутрішня система якості // Педагогіка. – 2021. – № 1. – С. 12–19.
- 32.Коваль О. М. Ризик-менеджмент у державному секторі // Економіка та держава. – 2023. – № 5. – С. 10–16.
- 33.Мельник П. В. Проблеми фінансового забезпечення оборони // Фінанси України. – 2025. – № 2. – С. 40–54.
- 34.Павленко С. В. Антикорупційний моніторинг // Юридичний радник. – 2026. – № 1. – С. 22–30.
- 35.Рижиков В. С. Методи оцінки ризиків // Менеджмент в Україні. – 2022. – № 3. – С. 18–25.
- 36.Сидоров І. П. Інформаційні технології в ДПСУ // Вісник кордону. – 2026. – № 1. – С. 5–12.

- 37.Ткаченко А. А. Стратегічне планування в умовах війни // Публічне управління. – 2025. – № 4. – С. 112–120.
- 38.Шевченко О. В. Кадровий менеджмент у ДПСУ // Державна служба. – 2024. – № 2. – С. 45–51.
- 39.Яковенко В. Л. Предиктивна аналітика в безпеці // Кібербезпека. – 2026. – № 3. – С. 60–68.
- 40.Anderson J. Risk Management in the Public Sector. – London : Routledge, 2022. – 310 p.
- 41.Borowski J. Border Management Paradigms. – Warsaw : Frontex, 2024. – 156 p.
- 42.Davis M. Artificial Intelligence in Security. – New York : Springer, 2025. – 412 p.
- 43.Miller G. Financial Resilience of State Agencies. – Oxford : OUP, 2025. – 288 p.
- 44.Smith L. Predictive Policing and Border Control. – Berlin : De Gruyter, 2024. – 340 p.
- 45.Taylor R. Integrated Border Management Standards. – Geneva : ISO, 2023. – 210 p.
- 46.Common Integrated Risk Analysis Model (CIRAM 2.0). – Warsaw : Frontex, 2023. – 114 p.
- 47.Risk Management Standard ISO 31000:2018. – Geneva : ISO, 2018. – 45 p.
- 48.European Integrated Border Management (IBM). – Brussels : EU Commission, 2024. – 88 p.
- 49.Global Risk Report 2026. – Geneva : World Economic Forum, 2026. – 124 p.
- 50.Anti-Corruption Standards for Law Enforcement. – Vienna : UNODC, 2023. – 140 p.
- 51.Цифрова трансформація ДПСУ: звіт за 2025 рік. – К. : ДПСУ, 2026. – 56 с.

52. Аналіз загроз прикордонній безпеці : метод. рек. – К. : НАДПСУ, 2025. – 92 с.
53. Психологія професійного вигорання військових. – Х. : Основа, 2024. – 215 с.
54. Логістика в умовах воєнного стану. – К. : Знання, 2025. – 310 с.
55. Протидія контрабанді: новітні технології. – Одеса : Гельветика, 2026. – 240 с.
56. Управління публічними фінансами. – К. : КНЕУ, 2023. – 400 с.
57. Кібербезпека державних реєстрів. – К. : Наукова думка, 2024. – 190 с.
58. Етика державного службовця: антикорупційний аспект. – К. : НАДС, 2025. – 120 с.
59. Організаційна культура в силових структурах. – Львів : Світ, 2024. – 280 с.
60. Інтелектуальні системи відеоспостереження. – К. : Техніка, 2025. – 175 с.
61. Моніторинг ризиків у системі «Гарт». – К. : ДПСУ, 2026. – 64 с.
62. Економічна теорія захисту кордону. – К. : Освіта, 2023. – 350 с.
63. Досвід країн НАТО у сфері прикордонної безпеки. – К. : Варта, 2024. – 220 с.
64. Прогнозування міграційних процесів. – К. : КНЕУ, 2025. – 210 с.
65. Управління конфліктами в колективі. – К. : Каравела, 2024. – 195 с.
66. Світовий досвід боротьби з корупцією. – К. : Юрінком Інтер, 2025. – 300 с.
67. Прикордонний менеджмент: навч. посіб. – Хмельницький : НАДПСУ, 2023. – 420 с.
68. Аудит операційної діяльності підрозділів. – К. : Фінанси, 2024. – 210 с.
69. Авіаційний моніторинг кордону за допомогою БПЛА. – К. : Либідь, 2025. – 180 с.
70. Міжнародне співробітництво у сфері безпеки. – К. : Знання, 2024. – 260 с.

- 71.Грошове забезпечення військових: правовий аналіз. – К. : Юрист, 2025. – 145 с.
- 72.Офіційний сайт Державної прикордонної служби України. URL: <https://dpsu.gov.ua/>.
- 73.База даних «Законодавство України». URL: <https://zakon.rada.gov.ua/>.
- 74.Офіційний портал НАЗК. URL: <https://nazk.gov.ua/>.
- 75.Веб-сайт Агентства Frontex. URL: <https://frontex.europa.eu/>.
- 76.Портал відкритих даних України. URL: <https://data.gov.ua/>.
- 77.Офіційний сайт МВС України. URL: <https://mvs.gov.ua/>.