Ф А 2.2.1-32-367

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ
Фармацевтичний факультет
Кафедра менеджменту, маркетингу та забезпечення якості у фармації

КВАЛІФІКАЦІЙНА РОБОТА

на тему: **ЗАСТОСУВАННЯ РИЗИК-ОРІЄНТОВАНОГО МЕНЕДЖМЕНТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ УСТАНОВИ**

Виконала:
здобувачка вищої освіти
2 курсу, групи 1
спеціальності 073 Менеджмент
освітньої програми
Якість, стандартизація та сертифікація
Катерина ПРОНЯЄВА

Керівник:
доцент закладу вищої освіти
кафедри
менеджменту, маркетингу та
забезпечення якості у фармації,
к. фармац. наук, доцент
Тетяна ЗБОРОВСЬКА

Рецензент:
завідувачка кафедри організації,
економіки та управління фармацією
ІПКСФ НФаУ, д. фарм. наук,
професор
Юлія БРАТІШКО

Харків – 2026 рік

АНОТАЦІЯ

Застосування ризик-орієнтованого менеджменту для забезпечення безперервності діяльності Держлікслужби полягає в створені системи управління, яка включає: аналіз бізнес-процесів, ідентифікацію ризиків, розробку політики та плану безперервності діяльності, формування культури управління ризиками, постійне навчання персоналу та встановлення показників моніторингу ефективності системи управління ризиками та безперервності діяльності відповідно до міжнародних стандартів.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 44 найменувань, 7 додатків, і містить 4 рисунки, 4 таблиці. Повний обсяг кваліфікаційної роботи складає 102 сторінки, з яких перелік посилань займає 4 сторінки, додатки – 28 сторінок.

Ключові слова: Держлікслужба, система забезпечення безперервності бізнесу, ризик-орієнтований підхід.

ABSTRACT

The application of risk-based management to ensure the continuity of the State Medical Service's activities consists in creating a management system that includes: business process analysis, risk identification, development of a policy and business continuity plan, formation of a risk management culture, ongoing staff training and establishment of indicators for monitoring the effectiveness of the risk management system and business continuity in accordance with international standards.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references of 44 items, 7 appendices, and contains 4 figures, 4 tables. The full scope of the qualification work is 102 pages, of which the list of references takes up 4 pages, appendices – 28 pages.

Keywords: State Medical Service, business continuity system, risk-based approach.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BCM – Business Continuity Management – управління безперервністю бізнесу.

BCP – Business Continuity Planning – планування безперервності бізнесу.

BIA – Business impact analysis – аналіз впливу на бізнес

DRP – Disaster Recovery Planning) – план відновлення після збоїв.

ERM – Enterprise Risk Management – управління ризиками підприємства

ISO – International Organization for Standardization – міжнародна організація зі стандартизації

KRI – Key Risk Indicators – Ключові індикатори ризику

QRM – Quality Risk Management – Система управління ризиками

RPO – Recovery Point Objective – рівень допустимої втрати даних

RTO – Recovery Time Objective – цільовий час відновлення процесу

Держлікслужба – Державна служба з лікарських засобів та контролю за наркотиками

ЛЗ – лікарський засіб

МОЗ – Міністерством охорони здоров’я України

ВСТУП

Упродовж останніх років діяльність українських підприємств зазнає впливу значної кількості зовнішніх чинників, серед яких визначальними стали пандемія COVID-19 та воєнні дії. Важливим є не лише масштаб і сила дії цих факторів, а й надзвичайно висока динамічність середовища функціонування, що супроводжується зростанням рівня невизначеності. За таких умов накопичений раніше управлінський досвід часто не забезпечує достатньої інформаційної бази для ухвалення ефективних управлінських рішень. Це зумовлює необхідність активного впровадження ризик-орієнтованого підходу до управління з урахуванням реальних умов здійснення безпекової діяльності на конкретному підприємстві.

Підприємницька діяльність у період воєнного стану має низку принципових особливостей, за яких пріоритетною стає стратегія збереження та адаптації бізнесу. Водночас помилковим є підхід, що ототожнює таку стратегію виключно з уповільненням господарських процесів, зокрема скороченням виробництва, вивільненням персоналу, розпродажем активів чи припиненням взаємодії з партнерами в очікуванні стабілізації ситуації. Слід враховувати, що зниження ділової активності частини суб'єктів ринку не призводить до зменшення загального попиту на товари й послуги, натомість створює додаткові можливості для посилення конкурентних позицій тих підприємств, які, попри підвищений рівень ризику, продовжують активно провадити господарську діяльність. Крім того, відкритість внутрішнього ринку зумовлює ймовірне посилення присутності іноземних компаній у післявоєнний період, що може поглибити конкурентне відставання вітчизняних виробників у разі їхньої тривалої пасивності.

У контексті забезпечення економічної безпеки підприємства ризик постає як невід'ємний елемент безпекової парадигми та одна з форм прояву загроз. Водночас реальні можливості впливу суб'єктів безпеки на перебіг фінансово-господарських процесів є обмеженими, що в сучасних умовах потребує переосмислення підходів до управління. Це актуалізує необхідність

розвитку та поширення ризик-орієнтованого управління, а також формування ризик-орієнтованого мислення як основи прийняття управлінських рішень. Особливої ваги набуває усвідомлене та системне ініціювання розвитку бізнесу на основі розуміння природи виникнення ризиків і здатності комплексно оцінювати потенційні вигоди, які можуть бути досягнуті незалежно від результатів реалізації ризикових управлінських рішень [1].

Ризик-орієнтований менеджмент – це підхід, при якому управлінські рішення, процеси та ресурси організації формуються з урахуванням системного виявлення, оцінки та реагування на ризики, що можуть вплинути на досягнення цілей організації. Він інтегрує управління ризиками у всі ключові операційні та стратегічні процеси організації (ідентифікація, оцінка, вибір заходів реагування, моніторинг) [2]. Робота над всіма групами ризиків призводить до розробки заходів, що дають можливість працювати на випередження небезпеки, але вони не гарантують безперервності виконання всіх функцій, тому важливим є формування стратегії безперервності діяльності яка базується на ризик-орієнтованому управлінні.

Безперервність діяльності (business continuity) – сукупність заходів, процедур та систем, спрямованих на збереження виконання критичних функцій організації під час інцидентів (стихійні лиха, технічні збої, кіберінциденти, воєнні загрози тощо) і на швидке відновлення після них. Міжнародний підхід до системи управління безперервністю бізнесу (Business Continuity Management: BCM) описаний у відповідних стандартах, що визначають вимоги й кращі практики для систем менеджменту безперервності [3].

Державні установи надають суспільно важливі послуги (юридичні, соціальні, медіа-реєстраційні, адміністративні тощо); їхній простій має прямі наслідки для безпеки, економіки та довіри громадян. Відтак ризики, які порушують роботу таких установ, мають високий соціальний пріоритет – відновлення функціонування має відбуватися швидко й прогнозовано [4].

Державні установи працюють в умовах зростаючої складності загроз (кібернетичні атаки, гібридні та воєнні загрози, пандемії, кліматичні екстремуми). Тому традиційне реактивне адміністрування вже не достатнє – потрібен системний ризик-орієнтований підхід, що поєднує оцінку й превентивні заходи з планами відновлення [5].

Для державних органів існує вимога прозорості, підзвітності й збереження даних – отже заходи з управління ризиками й забезпечення безперервності мають бути документовані, стандартизовані та підлягати аудитам; впровадження стандартів (ISO, національних вимог) сприяє єдиному підходу та сумісності [4, 5].

Не виключенням є Державна служба з лікарських засобів та контролю за наркотиками (Держлікслужба). За інформацію Держлікслужби в умовах воєнного стану критично важливим є забезпечення належного та безперервного функціонування діяльності суб'єктів господарювання, які займаються забезпеченням населення лікарськими засобами. Держлікслужба у свою чергу продовжує працювати та виконувати свої обов'язки [6, 7].

Актуальність застосування ризик-орієнтованого менеджменту для забезпечення безперервності діяльності державних установ є очевидною: сучасні загрози вимагають системного, проактивного підходу, який поєднує управління ризиками та готовність до відновлення критичних функцій. Впровадження принципів стандартів ISO 31000 і ISO 22301 у поєднанні з дотриманням національних нормативних вимог забезпечує структуру, що підвищує стійкість державних послуг і мінімізує негативні наслідки інцидентів для суспільства.

Мета роботи. У ході дослідження нами було здійснено аналіз основних принципів ризик-орієнтованого підходу та окреслено механізми їх практичного впровадження з метою забезпечення безперервного функціонування державної установи в умовах дії внутрішніх і зовнішніх загроз. У зв'язку з цим метою роботи є обґрунтування шляхів реалізації ризик-орієнтованого підходу під час формування системи заходів,

спрямованих на забезпечення безперервності діяльності Державної служби України з лікарських засобів та контролю за наркотиками.

Об'єкт та предмет дослідження. Об'єктом дослідження є діяльність Держлікслужби, а предметом дослідження є заходи з реалізації ризик-орієнтованого управління для безперервної діяльності державної установи.

Основні завдання роботи:

– проаналізувати сутність, принципи та еволюцію ризик-орієнтованого менеджменту в системі державного управління;

– дослідити нормативно-правові та методологічні засади забезпечення безперервності діяльності державних установ в Україні;

– визначити основні внутрішні та зовнішні ризики, що впливають на безперервність діяльності Держлікслужби;

– проаналізувати сучасні підходи та вибрати інструменти ризик-орієнтованого менеджменту, які застосовуються для управління безперервністю діяльності;

– оцінити можливості інтеграції ризик-орієнтованого менеджменту в систему управління безперервністю діяльності Держлікслужби;

– розробити практичні рекомендації щодо підвищення ефективності забезпечення безперервності діяльності державної установи на основі ризик-орієнтованого підходу.

Методи дослідження. У процесі проведення дослідження було використано комплекс загальнонаукових і спеціальних методів, зокрема аналіз нормативно-правових актів, положень національних і міжнародних стандартів ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови» та ДСТУ EN ISO 22301:2021 «Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги», а також статистичних даних, що відображають вплив різних чинників на діяльність державних установ. Методологічну основу дослідження становили такі методи наукового пізнання:

– аналіз наукових джерел з метою узагальнення існуючих підходів і результатів досліджень за обраною тематикою;

– експериментальний метод – формування контрольованих умов для дослідження причинно-наслідкових зв’язків;

– статистичний аналіз – застосування статистичних інструментів для опрацювання масивів даних, виявлення залежностей, здійснення прогнозних оцінок;

– порівняльний аналіз – зіставлення теоретичних підходів, моделей і практик з метою визначення їхніх особливостей, переваг і обмежень;

– метод аналізу конкретних ситуацій (case study) – дослідження реальних прикладів діяльності державних установ для виявлення проблемних аспектів і можливих шляхів їх вирішення.

Практичне значення отриманих результатів. Запропоновані практичні рекомендації можуть бути використанні для вдосконалення роботи Держлікслужби та формуванню стратегії безперервності діяльності.

Дослідження і публікації. «Принципи застосування ризик-орієнтованого менеджменту для забезпечення безперервності діяльності державної установи» Збірник матеріалів Youth Pharmacy Science: матеріали VI Всеукраїнської науково-практичної конференції з міжнародною участю, 10-11 грудня 2025 р. (Додаток А, Б, В).

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 44 найменувань, 7 додатків, і містить 4 рисунки, 4 таблиці. Повний обсяг кваліфікаційної роботи складає 102 сторінки, з яких перелік посилань займає 4 сторінки, додатки – 28 сторінок.

РОЗДІЛ 1

МЕТОДОЛОГІЧНІ ПІДХОДИ ДО РИЗИК-ОРІЄНТОВАНОГО МЕНЕДЖМЕНТУ ТА ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ДІЯЛЬНОСТІ

1.1 Поняття та сутність ризик-орієнтованого менеджменту.

Ризик-орієнтований менеджмент (risk-based management) – це системний підхід до управління організацією, що передбачає виявлення, аналіз, оцінювання та контроль ризиків, які можуть вплинути на досягнення її цілей. Основна ідея цього підходу полягає у прийнятті управлінських рішень на основі оцінки ризиків, що дозволяє підвищити ефективність діяльності організації, забезпечити її стійкість до зовнішніх і внутрішніх загроз та запобігти небажаним наслідкам [1].

У сучасних умовах постійної невизначеності ризик-орієнтований менеджмент стає ключовим елементом стратегічного планування й операційної діяльності організацій. Він базується на філософії проактивного управління, коли організація не просто реагує на проблеми, а передбачає їх і розробляє превентивні заходи. Такий підхід дозволяє ефективно використовувати ресурси, підвищувати надійність процесів та забезпечувати безпеку працівників та споживачів [2].

Застосування методів наукової логіки та теоретичного узагальнення наявних наукових праць дало змогу дійти висновку, що небезпеки в діяльності підприємства формуються з урахуванням часових лагів їх прояву та є комплексом:

– потенційних загроз майбутнього, які потребують своєчасної ідентифікації та моніторингу їх розвитку;

– поточних наслідків реалізації загроз минулих періодів, щодо яких не було впроваджено належних управлінських рішень із їх нейтралізації;

– актуальних загроз сьогодення, вплив яких на рівень стійкості підприємства може проявитися у перспективі;

– наявних втрат, що виникли внаслідок реалізації ризиків.

Результати аналітичних досліджень підтверджують, що зміна параметрів розвитку підприємства зумовлена впливом небезпек різного походження, дослідження яких потребує застосування спеціалізованого інструментарію та відповідних методів оцінювання. У межах наявної системи небезпек, що включає загрози як події, небезпеки як оцінений вплив загроз та ризики як оцінену зміну стану підприємства під дією небезпек, дослідження має зосереджуватися не лише на оцінюванні ризиків, що є сферою ризик-менеджменту, а й на ідентифікації загроз, визначенні спрямованості їх впливу на рівень стійкості підприємства та формуванні напрямів нейтралізації негативних наслідків такого впливу. На сучасному етапі в системі небезпек діяльності підприємства саме ризики характеризуються найвищою ймовірністю спричинення втрати його стійкості [8].

Згідно зі стандартом ISO 31000:2018, ризик визначається як «вплив невизначеності на цілі», що підкреслює багатовимірний характер ризиків і необхідність їх урахування на всіх рівнях діяльності організації – від стратегічного до операційного [2]. Ризик-орієнтований менеджмент забезпечує формування цілісної системи, яка включає:

– ідентифікацію ризиків – виявлення можливих подій або чинників, що можуть негативно вплинути на діяльність організації;

– аналіз ризиків – визначення причин, імовірності та потенційних наслідків ризиків;

– оцінювання ризиків – визначення рівня ризику та необхідних заходів реагування;

– розроблення та впровадження заходів щодо мінімізації ризиків;

– моніторинг та перегляд управлінських рішень з метою постійного вдосконалення (Рис. 1.1) [1, 2, 3, 10].

У межах сучасних систем управління, таких як ISO 9001:2015, ризик-орієнтоване мислення розглядається як основоположний принцип, що сприяє стабільності процесів, підвищенню якості та задоволеності споживачів [3, 9].

У свою чергу, стандарти ISO 22301:2019 та ISO/IEC 17025:2017 інтегрують ризик-орієнтований підхід у контекст забезпечення неперервності діяльності та надійності процесів [4].

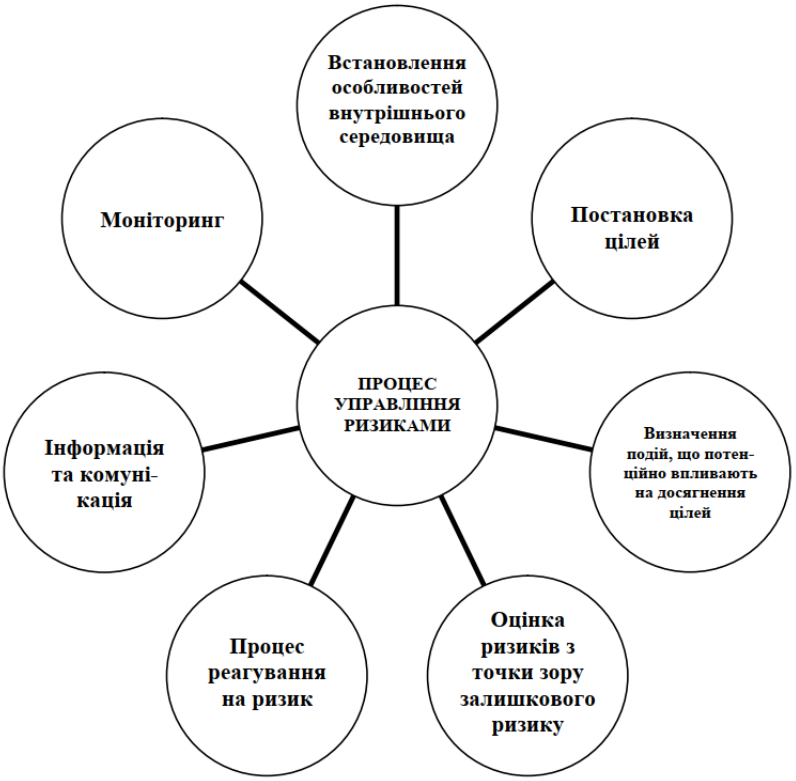

Рис. 1.1 Основні компоненти процесу управління ризиками

Сутність ризик-орієнтованого менеджменту полягає у тому, що організація переходить від реактивної до проактивної моделі управління, де ризики стають не загрозою, а об’єктом планування. Це підвищує стійкість, адаптивність і конкурентоспроможність організації, забезпечує раціональне використання ресурсів та сприяє прийняттю обґрунтованих рішень [10].

Нормативне та методологічне забезпечення процесу формування системи ризик-орієнтованого управління підприємством передбачає запровадження комплексу ключових елементів, зокрема:

– управлінської політики, заснованої на систематичному оцінюванні та прогнозуванні ризиків;

– внутрішнього організаційно-розпорядчого документа або методичного положення, яке визначає порядок упровадження та реалізації ризик-орієнтованого управління;

– методичних матеріалів, призначених для ідентифікації та оцінювання ризиків;

– нормативного документа, що регламентує взаємодію внутрішніх структурних підрозділів у сфері управління ризиками та забезпечення економічної безпеки підприємства;

– документа, який передбачає формування переліку потенційних ризиків діяльності підприємства та містить обґрунтовану й достовірну інформацію щодо їх характеристик;

– системи звітної документації з питань виявлення, оцінювання та мінімізації ризиків [11, 12, 13].

На рисунку 1.2 представлено орієнтовну структуру ризик-орієнтованого управління, спрямовану на підвищення результативності управлінських процесів і забезпечення належного рівня економічної безпеки підприємства. Застосування зазначених підходів створює передумови для впровадження та практичного використання ризик-орієнтованого підходу в системі управління підприємством.

Реалізація такого підходу забезпечує отримання низки переваг, зокрема [11, 14]:

– можливість здійснювати оцінювання ефективності впроваджених підходів до організації системи управління ризиками із залученням як внутрішніх ресурсів підприємства (експертів і штатних працівників), так і зовнішніх зацікавлених сторін;

– виявлення слабких місць і недоліків у діяльності підприємства через ідентифікацію внутрішніх ризиків;

– зменшення управлінських витрат і оптимізацію документообігу;

– делегування окремих функцій, зокрема щодо розроблення та впровадження безпекоорієнтованих заходів, на аутсорсинг з метою підвищення їх професійного рівня та скорочення операційних витрат;

– формування ефективної системи ідентифікації й протидії потенційним і реальним ризикам, що сприяє зниженню можливих втрат у

перспективі та підвищенню загальної ефективності управління й рівня економічної безпеки підприємства;

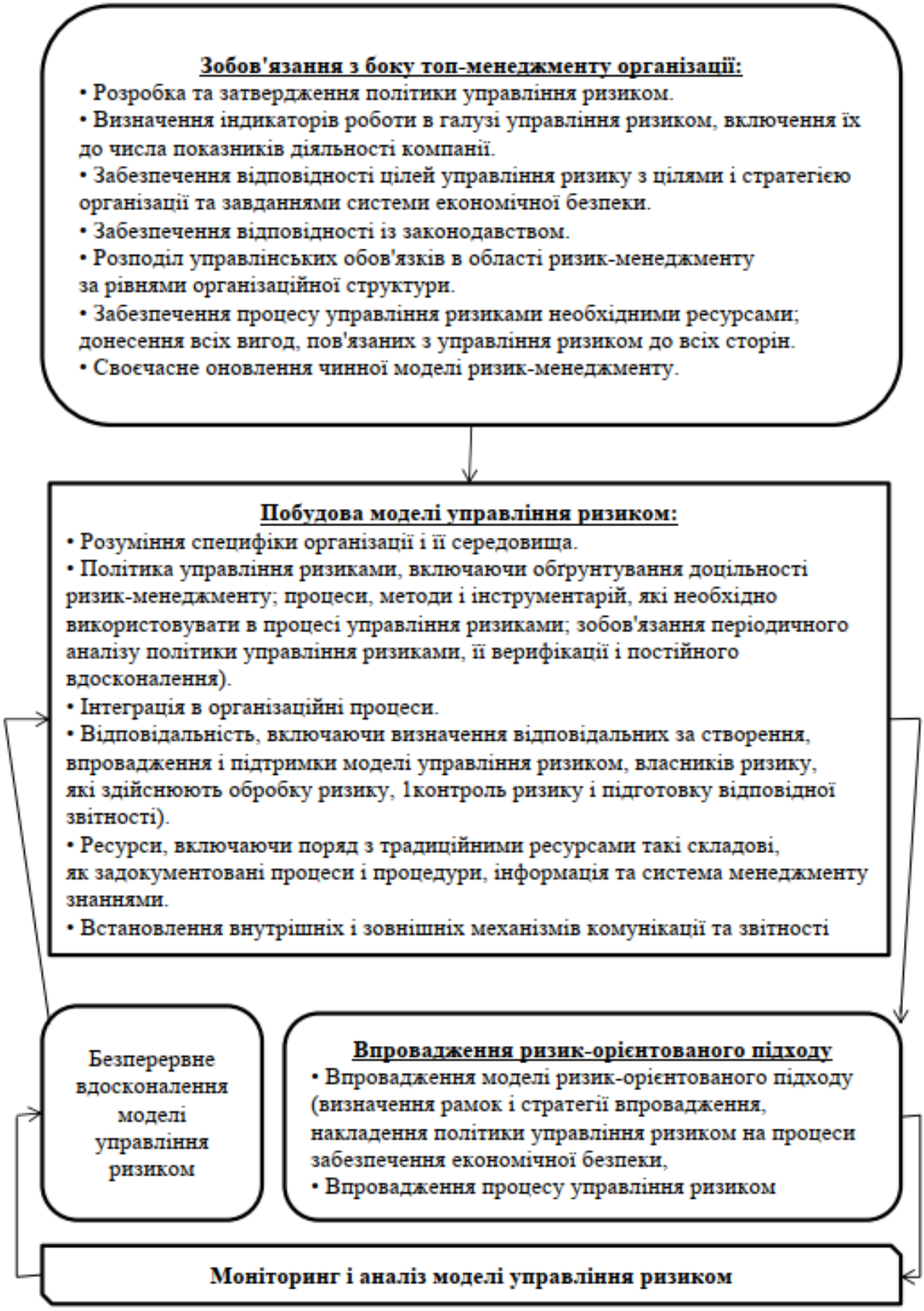

Рис. 1.2 Структур ризик-орієнтованого управління

– створення умов для обміну досвідом і кращими практиками у сфері ризик-орієнтованого управління з метою вдосконалення власних підходів та розвитку загальнонаціональної системи управління ризиками на підприємствах і в організаціях.

Для попередження та мінімізації ризиків підприємству доцільно використовувати результати теоретичних досліджень у практичній діяльності, що сприятиме підвищенню ефективності бізнес-процесів і зміцненню економічної безпеки (рис. 1.3) [11, 15, 16]. Ризик-орієнтований підхід базується на послідовних процесах ідентифікації, аналізу та оцінювання ризиків, а його ключовим елементом є усвідомлення всіма працівниками організації важливості визначення вразливих до ризику сфер діяльності та бізнес-процесів. Його реалізація передбачає застосування визначеного алгоритму дій, який подано на рисунку 1.4 [11, 17, 18].

Таким чином, ризик-орієнтований менеджмент є універсальним інструментом сучасного управління, який дозволяє організаціям ефективно функціонувати в умовах невизначеності та мінливого середовища, зменшуючи вплив негативних подій та забезпечуючи стабільність діяльності.

Сучасна система публічного управління в Україні, функціонуючи в умовах постійних трансформацій і реформ, об’єктивно потребує подальшого вдосконалення, зокрема через упровадження інноваційних управлінських підходів і методів управління складними соціальними системами. Орієнтація публічного управління на концепцію New Public Management передбачає використання інструментарію, запозиченого з практики корпоративного управління. У результаті умови функціонування державних і муніципальних установ значною мірою наблизилися до середовища, в якому діють організації корпоративного сектору [10].

До таких умов належать розгалуженість внутрішніх і зовнішніх взаємозв’язків, динамічність зовнішнього середовища, вплив науково-технічного прогресу, обмеженість ресурсного забезпечення, дефіцит часу та

інші чинники. Сукупність зазначених обставин формує підвищений рівень невизначеності та ризику в діяльності організацій.

Рис. 1.3 Елементи ризик-орієнтованого підходу до управління підприємством

У межах діяльності суб’єктів публічного управління особливої актуальності набуває застосування корпоративної методології управління

ризиками, що вже тривалий час є усталеною практикою в економічно розвинених країнах.

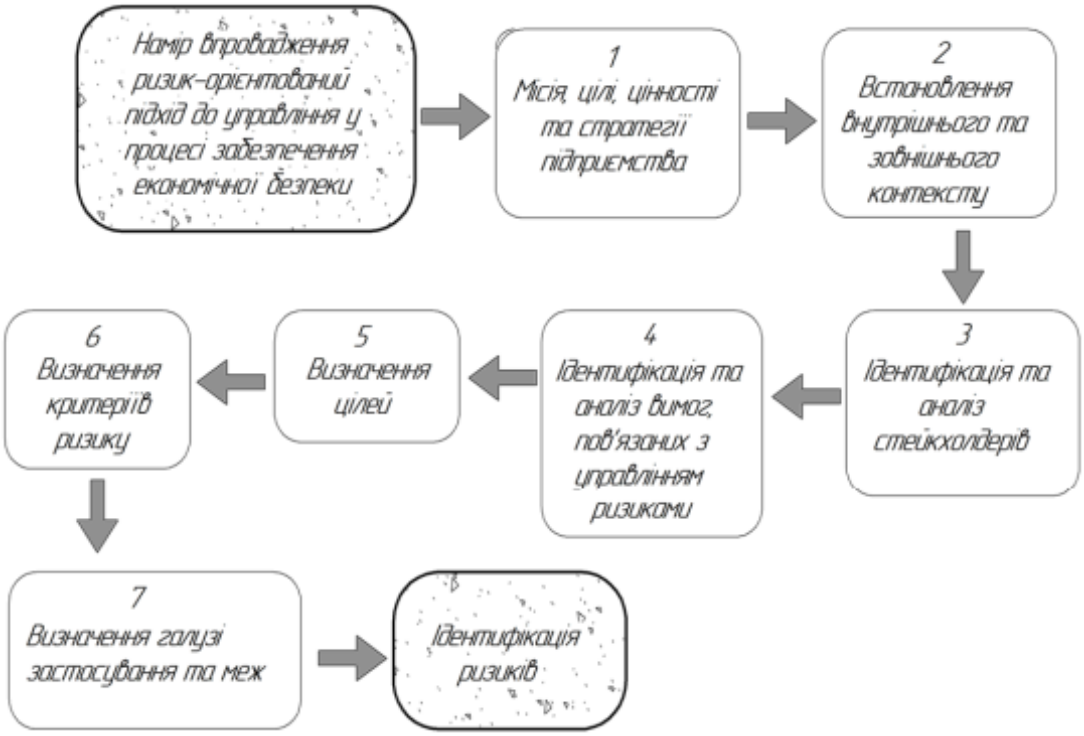

Рис. 1.4 Алгоритм впровадження системи управління ризиками

Належним чином вибудувана система ризик-менеджменту дає змогу скоротити час на ідентифікацію та аналіз ризиків, а також забезпечити відносну впевненість у надійності окремих елементів системи внутрішнього контролю. Управління ризиками сприяє досягненню низки переваг, зокрема мінімізації фінансових втрат і необґрунтованих витрат, запобіганню шахрайству, раціональному розподілу ресурсів, зниженню ймовірності виникнення непередбачуваних негативних подій, удосконаленню внутрішнього контролю, оперативному використанню нових можливостей та забезпеченню реалізації стратегічних цілей [10].

Управління ризиками охоплює як потенційно негативні, так і позитивні наслідки для діяльності організації. Його зміст полягає в ідентифікації можливих відхилень від запланованих результатів та цілеспрямованому впливі на такі відхилення з метою підвищення ефективності діяльності, мінімізації втрат і підвищення якості управлінських рішень.

Процес управління ризиками передбачає не лише запобігання або зменшення ймовірності реалізації небажаних подій, а й виявлення перспектив і можливостей для вдосконалення функціонування організації та досягнення її стратегічних цілей [19].

1.2 Класифікація ризиків у системі управління

У загальному розумінні ризик визначається як імовірність настання несприятливих наслідків. У теорії менеджменту ризик розглядають як можливість виникнення втрат або недосягнення запланованих результатів у процесі діяльності організації. Ризики можуть проявлятися в усіх сферах функціонування – виробничій, фінансовій, маркетинговій, кадровій, управлінській та інших.

У наукових дослідженнях сформувалися різні підходи до трактування поняття «ризик»: як потенційної події, здатної спричинити негативні наслідки; як імовірності виникнення збитків або недоотримання очікуваних вигод; як загрози втрат у конкретній господарській ситуації. Водночас сучасні концепції управління ризиками відображають еволюцію цього поняття від виключно негативного трактування до інтегрованого підходу, за яким ризик поєднує як потенційні загрози, так і можливості для розвитку організації [20].

З метою систематизації та ефективного управління ризиками в управлінській практиці застосовується їх класифікація за різними ознаками.

1. За джерелом виникнення. Внутрішні ризики зумовлені особливостями діяльності самої організації та виникають унаслідок недоліків управління ресурсами й процесами. До них належать:

– організаційні ризики (неефективна структура, недосконалі процедури);

– управлінські ризики (помилки у прийнятті рішень, слабкий контроль);

– кадрові ризики (низька мотивація, недостатня кваліфікація, плинність персоналу);

– технічні та інформаційні ризики (відмови обладнання, збої інформаційних систем);

– фінансові, операційні та репутаційні ризики.

Зовнішні ризики формуються під впливом факторів, що не залежать безпосередньо від діяльності організації. До них належать:

– політичні ризики (зміни законодавства, політична нестабільність);

– економічні ризики (інфляція, скорочення фінансування);

– соціальні ризики (демографічні зміни, протести);

– екологічні та природно-кліматичні ризики (катастрофи, стихійні лиха);

– техногенні ризики та кіберзагрози.

2. За сферою прояву (впливу). Ризики поділяють на:

– економічні та фінансові;

– виробничі та операційні;

– технологічні та інформаційні;

– екологічні;

– соціальні;

– політичні та правові;

– репутаційні.

Кожна група відображає специфіку потенційних загроз і характер можливих наслідків для діяльності організації.

3. За масштабом поширення. Залежно від рівня охоплення ризики поділяють на:

– глобальні (зміна клімату, світові пандемії);

– національні (економічні кризи в межах держави);

– регіональні (катастрофи або соціально-економічні проблеми окремих регіонів);

– локальні (ризики конкретних організацій);

– індивідуальні (ризики, пов’язані з особистими обставинами).

4. За ймовірністю реалізації та масштабом наслідків. За ймовірністю виникнення розрізняють ризики з високою, середньою та низькою ймовірністю реалізації.

За масштабом наслідків ризики поділяють на:

– незначні;

– значні;

– катастрофічні, що можуть призвести до припинення діяльності організації.

Поєднання цих параметрів використовується в матрицях ризиків відповідно до методології ISO 31000.

Ідентифікація ризиків є базовим етапом процесу управління ризиками та передбачає виявлення й опис потенційних загроз, які можуть вплинути на діяльність організації. Для цього застосовують аналітичне моделювання, експертні оцінки, опитування, аналіз історичних даних та комбінування методів. Вибір інструментарію залежить від цілей дослідження, специфіки діяльності, доступності інформації та ресурсних обмежень. Результати ідентифікації створюють основу для подальшого оцінювання ризиків і розроблення заходів реагування [21].

У державному управлінні ризики мають підвищене значення, оскільки їх реалізація впливає не лише на окремі органи влади, а й на функціонування суспільства, економіки та системи національної безпеки. Тому класифікація ризиків у державних установах здійснюється за такими ключовими ознаками:

– за джерелом виникнення (внутрішні та зовнішні);

– за сферою впливу (операційні, фінансові, правові, репутаційні);

– за характером прояву (стратегічні, тактичні, кризові);

– за ймовірністю та масштабом наслідків.

Застосування міжнародних стандартів, зокрема ISO 31000:2018, ISO 9001:2015 та ISO 22301:2019, сприяє формуванню ризик-орієнтованої культури управління, підвищенню прозорості, відповідальності та ефективності діяльності державних установ [20].

1.3 Концепція безперервності діяльності. Взаємозв'язок між ризик-менеджментом і безперервністю діяльності: моделі й підходи

Концепція безперервності діяльності є однією з ключових сучасних методологій забезпечення стійкості організацій до впливу зовнішніх і внутрішніх загроз. BCM спрямована на створення системи, яка дозволяє підготуватися до інцидентів, ефективно реагувати на них та швидко відновлювати критично важливі функції, мінімізуючи негативні наслідки для організації, споживачів та суспільства [2].

У XXI столітті роль BCM значно зросла через збільшення кількості кризових ситуацій: техногенних аварій, кібератак, стихійних лих, пандемій, військових конфліктів. Особливо це актуально для України, яка перебуває в умовах тривалої військової агресії та пов'язаних із нею ризиків для державного управління, інфраструктури та бізнесу. Запровадження систем безперервності діяльності стає необхідною умовою забезпечення національної та організаційної безпеки [10].

1. Міжнародні стандарти BCM

1.1. ISO 31000:2018 – загальні принципи управління ризиками

Стандарт ISO 31000:2018 визначає фундаментальні принципи управління ризиками та формує концептуальну основу для процесів BCM. Він наголошує, що безперервність діяльності неможлива без систематичного ризик-менеджменту, включаючи ідентифікацію загроз, їхній аналіз, оцінку та розроблення заходів реагування [2].

Основні положення ISO 31000:

- інтеграція ризик-менеджменту в усі процеси організації;
- стратегічний і проактивний характер управління ризиками;
- необхідність постійного моніторингу та вдосконалення;
- орієнтація на створення цінності та стійкості.

Цей стандарт забезпечує методичну базу для подальшого впровадження системи безперервності діяльності відповідно до ISO 22301.

1.2. ISO 22301:2019 – спеціалізований стандарт систем управління безперервністю діяльності

Він є ключовим документом у сфері BCM на міжнародному рівні [3].

Основні компоненти ISO 22301:

– аналіз впливу на бізнес (Business Impact Analysis, BIA);
– оцінка ризиків у контексті безперервності діяльності;
– визначення критично важливих процесів;
– розроблення планів реагування та відновлення;
– забезпечення ресурсів (людських, технічних, інформаційних);
– навчання персоналу та тестування планів;
– аудит, моніторинг і постійне вдосконалення системи.

ISO 22301 встановлює єдину міжнародну рамку, яка дозволяє організаціям будувати стійкі системи та гарантувати безперебійну роботу навіть у кризових ситуаціях.

Україна активно впроваджує концепцію BCM у державному секторі, критичній інфраструктурі, промисловості, фінансовій сфері та охороні здоров'я. Посилення ролі BCM пояснюється необхідністю:

– підвищення стійкості установ під час війни;
– захисту критичної інфраструктури (енергетики, транспорту, медицини);
– забезпечення безперервності роботи органів влади;
– виконання міжнародних зобов'язань та гармонізації зі стандартами ЄС;
– відповідності вимогам міжнародних донорів та партнерів, які фінансують відновлення України.

В Україні відбувається адаптація підходів BCM через:

– розроблення норм безпеки та стійкості об'єктів критичної інфраструктури;

– впровадження ризик-орієнтованого менеджменту в державних установах;

– використання вимог ISO 31000 та ISO 22301 при створенні систем управління якістю, інформаційною безпекою та операційною діяльністю.

Також українські підприємства дедалі частіше проходять сертифікацію за ISO 22301, що підвищує їхню конкурентоспроможність та надійність.

У сучасних умовах BCM є критично важливим для:

– забезпечення безперервності державного управління;

– збереження функціонування медичних та фармацевтичних установ;

– гарантування надання публічних послуг;

– стабільності ланцюгів постачання;

– відновлення економіки в умовах воєнних та кризових загроз.

Планування безперервності діяльності та ризик-менеджмент є взаємодоповнювальними елементами сучасних систем управління, спрямованих на підвищення стійкості організації до загроз та зменшення негативного впливу кризових подій. Незважаючи на те, що ці концепції мають різні цілі та інструменти, їх інтеграція є критично важливою для формування ефективної системи забезпечення стабільності функціонування організацій, зокрема державних, промислових та фармацевтичних установ [22].

Ризик-менеджмент відповідно до стандарту ISO 31000:2018 визначається як систематичний процес ідентифікації, аналізу, оцінки та оброблення ризиків у цілому спектрі діяльності організації [2]. У свою чергу, BCM, регламентований ISO 22301:2019, фокусується на забезпеченні здатності організації продовжувати виконання критично важливих функцій під час інцидентів і після них [3].

Хоча ризик-менеджмент зосереджується на запобіганні негативним подіям, а BCM – на реагуванні та відновленні, обидва підходи є частинами єдиної логіки забезпечення стійкості. Вони спираються на схожі принципи:

– системність;
– проактивність;
– циклічність (PDCA);
– необхідність моніторингу й удосконалення;
– орієнтація на мінімізацію впливу невизначеності [2; 3].

2. Моделі інтеграції ризик-менеджменту та BCM

2.1. Класична модель послідовної інтеграції. Згідно з цією моделлю, ризик-менеджмент передує BCM і є її основою. Послідовність виглядає так:

– Ідентифікація ризиків.
– Аналіз та оцінка ризиків.
– Визначення ризиків, які можуть спричинити переривання діяльності.
– Передача результатів аналізу в процес BCM.
– Розроблення планів реагування та відновлення.

Такий підхід використовується в системах управління якістю та безпеки за ISO 9001:2015 і ISO 22301:2019 [2; 3].

2.2. Інтегрована модель управління ризиками та безперервністю діяльності. У цій моделі ризик-менеджмент і BCM розглядаються як нерозривні процеси, які діють у тісній взаємодії. Основні характеристики:

– спільні методи оцінки ризиків та критичних процесів;
– єдиний реєстр ризиків і бізнес-процесів;
– узгоджені процедури реагування;
– інтегровані команди управління інцидентами.

Цей підхід прописаний у сучасних системах корпоративного управління та ризик-менеджменту, орієнтованих на resilience (організаційну стійкість) [22].

2.3. Модель “Enterprise Risk Management (ERM) + BCM”

В рамках моделі ERM ризик-менеджмент є стратегічною функцією, яка формує політику щодо ризиків на всіх рівнях організації. BCM у цьому випадку стає інструментом управління специфічною групою ризиків – тими, що можуть порушити безперервність діяльності.

ERM визначає:

– толерантність до ризиків;

– політику прийнятних і неприйнятних ризиків;

– інтеграцію аналізу ризиків у стратегічні рішення.

А BCM реалізує практичні рішення щодо реагування та відновлення [3].

3. Спільні методи та інструменти. Обидві системи використовують схожі інструменти, включаючи:

– Аналіз ризиків (Risk Assessment) – базовий етап обох підходів.

– Аналіз впливу на діяльність (BIA) – спеціалізований інструмент BCM, який ґрунтується на даних ризик-аналізу.

– Матриця ризиків, що використовується для визначення пріоритетів у плануванні.

– Сценарний аналіз, який дозволяє прогнозувати розвиток кризових ситуацій.

– Плани реагування (Incident Response Plans) та плани відновлення (Recovery Plans) – операційні інструменти BCM, що базуються на результатах ризик-менеджменту [2, 3, 22].

4. Значення інтеграції для сучасних організацій. Поєднання ризик-менеджменту та BCM дозволяє:

– підвищити стійкість і адаптивність організації;

– оптимізувати витрати, уникаючи дублювання функцій;

– забезпечити найкращу готовність до криз і надзвичайних ситуацій;

– зменшити час простою та обсяг збитків;

– зміцнити відповідність міжнародним стандартам та регуляторним вимогам [3; 22, 23].

Особливо важливим цей взаємозв’язок є для державних установ, медичних лабораторій, фінансових організацій, фармацевтичного сектору та критичної інфраструктури.

Ризик-менеджмент і планування безперервності діяльності є двома взаємопов’язаними компонентами сучасної системи забезпечення стійкості організації. Ризик-менеджмент забезпечує систематичне виявлення та оцінку загроз, тоді як BCM фокусується на реагуванні та відновленні після кризових подій. Їх інтеграція (на основі ISO 31000 та ISO 22301) дозволяє організації діяти проактивно, мінімізувати збитки та гарантувати безперервність операцій навіть у складних умовах.

Висновки до розділу 1

У результаті проведеного методологічного аналізу встановлено, що ризик-орієнтований менеджмент є ключовим інструментом сучасного управління організаціями в умовах зростаючої невизначеності, динамічності зовнішнього середовища та підвищеного рівня загроз. Його сутність полягає у системному та проактивному підході до ідентифікації, аналізу, оцінювання й управління ризиками з метою забезпечення стійкості, безперервності та ефективності діяльності організацій.

Доведено, що ризики мають комплексний і багатовимірний характер, формуються під впливом внутрішніх і зовнішніх чинників та проявляються з урахуванням часових лагів – від потенційних майбутніх загроз до фактичних втрат унаслідок реалізованих ризиків. Це обґрунтовує необхідність застосування розгалуженої класифікації ризиків за джерелом виникнення, сферою впливу, масштабом поширення, а також за ймовірністю реалізації та тяжкістю наслідків, що відповідає положенням міжнародного стандарту ISO 31000:2018.

Встановлено, що ефективне управління ризиками неможливе без належної ідентифікації загроз та використання спеціалізованого інструментарію їх оцінювання, що створює підґрунтя для прийняття обґрунтованих управлінських рішень і мінімізації негативного впливу ризикових подій. Особливого значення ризик-орієнтований підхід набуває у сфері публічного управління, де реалізація ризиків може мати суспільно значущі наслідки та впливати на національну безпеку.

Обґрунтовано, що концепція безперервності діяльності є логічним продовженням і практичним інструментом реалізації ризик-орієнтованого менеджменту, спрямованим на забезпечення здатності організацій підтримувати та відновлювати критично важливі функції в умовах кризових ситуацій. Аналіз міжнародних стандартів ISO 22301:2019 та ISO 31000:2018 підтвердив доцільність інтеграції ризик-менеджменту та систем безперервності діяльності як єдиної методологічної основи управління організаційною стійкістю.

Загалом встановлено, що поєднання ризик-орієнтованого менеджменту та систем безперервності діяльності формує сучасну парадигму управління, яка забезпечує підвищення адаптивності організацій, зниження втрат від кризових подій, раціональне використання ресурсів та досягнення стратегічних цілей в умовах нестабільного та ризиконасиченого середовища.

РОЗДІЛ 2

РИЗИКИ ЯК ОСНОВА СИСТЕМИ УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ УСТАНОВИ

2.1 Проблеми, обмеження та методики впровадження ризик-орієнтованого менеджменту.

Упровадження ризик-орієнтованого підходу до управління у вітчизняних держустановах та організаціях стикається з низкою глибинних проблем і бар'єрів:

1. Відсутність або фрагментарність нормативно-правової і методичної бази.

У ряді публічних секторів досі нема чіткої законодавчої або нормативної бази, яка б регламентувала загальні принципи і процедури управління ризиками. Наслідком є відсутність уніфікованих методик, відмінностей у підходах між установами, «дір» у процедурах, що ускладнює масштабне або міжвідомче впровадження ризик-менеджменту.

2. Недостатній рівень кадрів, компетенцій і культури ризик-менеджменту.

Ефективне управління ризиками передбачає наявність фахівців з належною експертизою – у аналізі ризиків, оцінці, плануванні заходів реагування. Але у багатьох установах такі кадри відсутні або мають недостатню підготовку.

Важлива також «ризик-культура» – усвідомлення серед менеджменту й персоналу необхідності системного підходу, готовності до змін, відповідальності за ризики. Без цього ризик-менеджмент залишається декларативним. Часто відсутні мотиваційні механізми (стимули, заохочення, відповідальність) для персоналу, щоб активно брати участь у процесах ідентифікації, оцінки та реагування на ризики.

3. Обмежені ресурси та фінансування, нестабільні бюджетні умови.

Для реалізації комплексного ризик-менеджменту потрібні ресурси: на розробку політик, процедури, інструменти оцінювання, навчання, тестування, моніторинг. Багато держустанов не мають відповідного бюджету. У періоди економічної нестабільності, криз чи воєнних викликів фінансування ризик-орієнтованих систем часто скорочується, адже пріоритети зміщуються на критичні поточні завдання.

4. Організаційні, управлінські та міжвідомчі бар'єри.

Відсутність чіткої відповідальності: коли немає призначених відповідальних за ризик-менеджмент, процеси часто «зависають» або реалізуються формально, без належної уваги. Недостатня координація між підрозділами, відомствами чи структурними одиницями: різні підрозділи можуть мати свої, неузгоджені підходи до ризиків, що ускладнює інтеграцію системи на рівні всього органу. Відсутність регулярного моніторингу, аудиту, оцінки ефективності заходів ризик-менеджменту – без цього системи деградують.

5. Сьогодення: воєнний стан, високий рівень невизначеності, зовнішні загрози.

У сучасних умовах, коли Україна перебуває під впливом масштабної агресії, класичні моделі ризик-менеджменту виявляють свої обмеження: вони були розраховані на мирні умови, стабільність, передбачуваність. У військових реаліях потрібні адаптивні, динамічні підходи, з урахуванням фізичних, безпекових, інформаційних ризиків, нестабільних ресурсів, логістичних перешкод, стресу персоналу тощо. Темпи змін і кількість нових ризиків (кіберзагрози, атаки на інфраструктуру, раптові зміни обстановки) перевищують здатність традиційних процедур оперативно реагувати. Це потребує постійного перегляду, швидкої реакції, гнучкості – а для цього потрібні і ресурси, і управлінські дії.

6. Недостатня мотивація, корупційні ризики, низька підзвітність.

Якщо немає належного контролю, підзвітності та аудитів – система ризик-менеджменту може бути формальною, без реального впливу. У

публічному секторі існує ризик, що заходи з управління ризиками будуть використовуватися вибірково, лише там, де вигідно, або як «паперова» формальність, без реальних змін. Це підриває довіру і знецінює сам підхід.

Впровадження ризик-орієнтованого менеджменту в Україні – це необхідний і логічний крок для підвищення стійкості державних установ, підвищення їх спроможності працювати у кризових умовах і реагувати на загрози. Однак без комплексного підходу – нормативної бази, кваліфікованих кадрів, ресурсного забезпечення, організаційної структури, культури ризиків і політичної волі – такі системи ризикують залишитися декларативними або неефективними [11, 34, 35, 36, 37].

Щоб подолати ці обмеження, потрібно:

– розробити та ухвалити на національному рівні комплексні нормативні акти та методичні рекомендації для державного сектору;

– інвестувати в підготовку фахівців і розвиток «ризик-культури» в державному управлінні;

– забезпечити стабільне фінансування і ресурси для реалізації заходів;

– запровадити прозору систему відповідальності, моніторингу й аудиту;

– адаптувати моделі управління ризиками до умов воєнного стану – з урахуванням нестабільності, фізичних, інформаційних і безпекових загроз.

В сучасних умовах зазначені проблеми загострюються через високий рівень невизначеності тому особливого значення набуває впровадження системи забезпечення безперервності діяльності, ядром якої є процеси ідентифікації, аналізу та оцінювання ризиків.

Саме ці процеси дозволяють своєчасно виявляти загрози, оцінювати їх потенційний вплив на діяльність установи та формувати ефективні заходи реагування, спрямовані на збереження стійкості критичних процесів у разі кризових подій або надзвичайних ситуацій. Міжнародні стандарти з управління ризиками та безперервністю діяльності, зокрема ISO 31000:2018

та ISO 22301:2019, наголошують, що ефективна система BCM має починатися саме з системного та документованого аналізу ризиків [3; 4].

Ідентифікація ризиків є процесом виявлення всіх можливих подій, умов або чинників, які можуть негативно вплинути на виконання критичних функцій установи. Для органів державної влади цей етап має особливе стратегічне значення, оскільки переривання їх діяльності може призвести до порушення прав громадян, зниження якості публічних послуг та створення загроз національній безпеці [1].

Основними завданнями ідентифікації ризиків є:

– виявлення внутрішніх і зовнішніх загроз;

– визначення вразливостей організації;

– опис можливих сценаріїв розвитку подій;

– встановлення взаємозв’язку між ризиками та критичними процесами діяльності [3].

На практиці для ідентифікації ризиків застосовуються експертні опитування, мозкові штурми, аналіз попередніх інцидентів, перевірка нормативно-правових вимог, аналіз зовнішнього середовища (PEST/PESTLE), вивчення галузевих рекомендацій і використання моделей ризиків, адаптованих до потреб державного сектору [2; 6].

Для забезпечення системності аналізу ризиків у BCM доцільно здійснювати їх класифікацію за характером впливу на діяльність установи.

Фізичні ризики включають природні катастрофи, пожежі, повені, аварії інженерних мереж, а також руйнування будівель. В умовах воєнного стану в Україні особливої актуальності набувають ризики, спричинені бойовими діями та пошкодженням критичної інфраструктури [2].

Технічні та технологічні ризики пов’язані зі збоями IT-систем, відмовою обладнання, перебоями електропостачання та втратою даних. Для органів, що здійснюють діяльність із використанням електронних реєстрів і цифрових сервісів, такі ризики є критичними [3].

Кіберризики та інформаційні загрози охоплюють кібератаки, несанкціонований доступ до інформації, витік персональних даних та DDoS-атаки. В умовах гібридної війни ці ризики суттєво зросли, що підтверджується сучасними науковими дослідженнями [6].

Організаційні ризики пов’язані з кадровим дефіцитом, недостатнім рівнем компетентності персоналу, помилками працівників, неузгодженістю дій між підрозділами та недосконалістю внутрішніх процедур [1; 5].

Безпекові ризики включають терористичні загрози, диверсії, фізичні загрози персоналу та майну. Для органів публічної влади ці ризики є особливо значущими з огляду на їх суспільний статус [1].

Правові, корупційні та регуляторні ризики пов’язані зі змінами законодавства, недотриманням нормативних вимог або правовими спорами і порушеннями, що можуть призвести до блокування окремих функцій установи [2].

Після ідентифікації ризиків здійснюється їх аналіз, який передбачає оцінку ймовірності виникнення ризику та масштабу його впливу на діяльність установи. Такий підхід дозволяє визначити рівень ризику та пріоритетність реагування [3; 4].

Особливу роль у BCM відіграє встановлення прямого зв’язку між ризиками та критичними процесами. Наприклад, кібератака може призвести до зупинки роботи державних реєстрів, перебої з електропостачанням – до повної недоступності електронних сервісів, а кадровий дефіцит – до припинення надання адміністративних послуг. Саме такий підхід рекомендований стандартом ISO 22301 і широко застосовується у практиці державного управління [3].

Критичні процеси – це види діяльності, переривання яких може спричинити істотні негативні наслідки для зацікавлених сторін або самої установи. Відповідно до ISO 22301, процеси вважаються критичними, якщо вони забезпечують виконання основних функцій, мають законодавчі вимоги щодо безперервності або підтримують інші життєво важливі процеси [3; 4].

До типових критичних процесів у державних установах належать:

– надання ключових публічних послуг;
– обробка та зберігання даних і реєстрів;
– функціонування ІТ-інфраструктури та систем кібербезпеки;
– фінансові та кадрові процеси;
– управління безпекою та реагування на інциденти [1; 2; 3].

Оцінювання ризиків є наступним етапом після їх аналізу та полягає у визначенні рівня ризику шляхом поєднання показників ймовірності та впливу. Метою цього процесу є встановлення пріоритетів ризиків і визначення необхідності управлінського реагування [3; 4].

Основним інструментом ранжування ризиків є матриця ризиків, яка дозволяє візуалізувати ризики та поділити їх на високі, середні та низькі. Для державного сектору України широко застосовується також метод експертних оцінок, який дозволяє врахувати специфіку діяльності установи та поточні умови функціонування, зокрема в умовах воєнного стану [1; 6].

Додатковими інструментами стратегічного аналізу ризиків є SWOT- та PEST-аналізи, які дозволяють оцінити внутрішні та зовнішні чинники ризику, а також прогнозувати їхній розвиток у перспективі [5].

Використання комплексного підходу до ідентифікації, аналізу та оцінювання ризиків у межах BCM забезпечує:

– мінімізацію простоїв у діяльності установи;
– підвищення готовності до кризових подій;
– зменшення фінансових і репутаційних втрат;
– забезпечення безперервності критичних процесів;
– відповідність міжнародним стандартам управління ризиками [4].

Таким чином, системний і документований ризик-аналіз є фундаментом ефективної системи безперервності діяльності, особливо актуальної для державних установ України в умовах підвищеної невизначеності та безпекових загроз.

2.2 Професійна діяльність Державної служби України з лікарських засобів та контролю за наркотиками

В Україні управління ризиками та забезпечення безперервності діяльності регламентуються сукупністю законів, галузевих актів і постанов Кабінету Міністрів (КМУ), а також методичними документами і наказами профільних органів. У законодавстві поступово зростає увага до формалізації ризик-орієнтованих підходів (податкові ризики, ризики критичної інфраструктури, державні аудиторські процедури та ін.). Визначення терміну «забезпечення безперервності діяльності» вже фігурує в окремих нормативних актах (наприклад, у реєстрі законодавчих термінів).

КМУ формує загальну державну політику у сфері управління ризиками і безпеки критичної інфраструктури, затверджує ключові постанови й порядки, що задають рамки для секторних органів (наприклад – постанови щодо впровадження систем управління ризиками у окремих секторах та вимог до об’єктів критичної інфраструктури).

Через постанови КМУ впроваджуються експериментальні проекти та нові підходи (наприклад, запровадження системи управління податковими ризиками). Це свідчить про активну роль уряду в трансформації підходів від традиційних до ризик-орієнтованих [24; 25].

Практичний наслідок: стандартизація підходів і вимог на рівні державної політики; делегування виконання і деталізації на профільні органи (міністерства, служби).

Державна служба України з лікарських засобів та контролю за наркотиками (Держлікслужба) є центральним органом виконавчої влади, діяльність якого спрямовується і координується Кабінетом Міністрів України через Міністерство охорони здоров’я. Основною метою її професійної діяльності є реалізація державної політики у сфері забезпечення якості, безпеки та ефективності лікарських засобів (ЛЗ), медичних виробів, а також контролю за обігом наркотичних засобів, психотропних речовин і прекурсорів.

Основні напрями професійної діяльності Держлікслужби:

1. Державний контроль якості лікарських засобів. Держлікслужба здійснює державний нагляд (контроль) за дотриманням вимог законодавства щодо ЛЗ на всіх етапах їх обігу – від виробництва та імпорту до зберігання, транспортування і реалізації. Особлива увага приділяється запобіганню потраплянню на ринок фальсифікованих, неякісних або небезпечних препаратів.

2. Ліцензування видів господарської діяльності. До повноважень служби належить ліцензування:

– виробництва ЛЗ;

– імпорту ЛЗ;

– оптової та роздрібної торгівлі ЛЗ;

– діяльності з обігу наркотичних засобів, психотропних речовин і прекурсорів.

У межах ліцензійної діяльності Держлікслужба проводить перевірки дотримання ліцензійних умов, застосовує заходи впливу та приймає рішення про зупинення або анулювання ліцензій.

3. Інспектування та фармацевтичний нагляд. Служба здійснює планові та позапланові інспекції суб’єктів господарювання з метою перевірки відповідності вимогам:

– належної виробничої практики (GMP);

– належної дистриб’юторської практики (GDP);

– належної аптечної практики (GPP).

Це сприяє підвищенню рівня якості фармацевтичної діяльності та гармонізації національних вимог із міжнародними стандартами.

4. Контроль за обігом наркотичних засобів і прекурсорів. Одним із критично важливих напрямів діяльності Держлікслужби є контроль за законним обігом наркотичних засобів, психотропних речовин і прекурсорів, з метою:

– недопущення їх незаконного використання;

– забезпечення доступності таких засобів для медичних і наукових потреб;

– виконання міжнародних зобов’язань України у сфері контролю за наркотиками.

5. Реагування на ризики для здоров’я населення. У разі виявлення небезпечних або неякісних ЛЗ Держлікслужба приймає рішення про:

– заборону обігу;

– вилучення з ринку;

– інформування суб’єктів господарювання та населення.

Ця діяльність має виразний ризик-орієнтований характер і спрямована на мінімізацію загроз для громадського здоров’я.

6. Аналітична, методична та міжнародна діяльність Держлікслужби:

– бере участь у розробленні нормативно-правових актів у сфері обігу лікарських засобів;

– здійснює аналітичну оцінку ризиків у фармацевтичному секторі;

– співпрацює з міжнародними організаціями та регуляторними органами інших країн;

– сприяє впровадженню європейських і міжнародних стандартів у національну практику.

7. Діяльність Держлікслужби має стратегічне значення для:

– забезпечення фармацевтичної та біологічної безпеки держави;

– захисту життя і здоров’я населення;

– стабільного функціонування фармацевтичного ринку;

– підвищення довіри громадян до системи охорони здоров’я;

– забезпечення безперервності постачання якісних ЛЗ, зокрема в умовах воєнних і кризових загроз [26].

Проведений SWOT-аналіз свідчить, що Держлікслужба має значний інституційний потенціал та стратегічну роль у забезпеченні безпеки лікарських засобів і обігу контрольованих речовин (табл. 2.1).

SWOT-аналіз Державної служби України з лікарських засобів та контролю за наркотиками здійснено на основі узагальнення положень нормативно-правових актів, наукових досліджень у сфері публічного управління та регуляторної політики, міжнародних стандартів управління ризиками і безперервності діяльності, а також офіційних аналітичних і звітних матеріалів Держлікслужби [27, 28, 29, 30].

Таблиця 2.1.

SWOT-аналіз Державної служби України з лікарських засобів та контролю за наркотиками

Сильні сторони (Strengths)	**Слабкі сторони (Weaknesses)**
Чітко визначені законодавчі повноваження та регуляторний статус	Висока залежність від державного фінансування
Ключова роль у забезпеченні національної безпеки у сфері охорони здоров'я	Обмежені фінансові ресурси для модернізації IT- та лабораторної інфраструктури
Наявність територіальних органів та регіональної мережі	Кадрові ризики: дефіцит фахівців, плинність персоналу
Функціонування державних лабораторій контролю якості лікарських засобів	Недостатня формалізація системи безперервності діяльності (BCM)
Використання ризик-орієнтованого підходу в державному нагляді	Фрагментарність інформаційних систем та реєстрів
Досвід міжнародної співпраці та адаптації до стандартів ЄС	Високе адміністративне навантаження та складні бюрократичні процедури
Можливості (Opportunities)	**Загрози (Threats)**
Гармонізація з європейськими стандартами (ISO 31000, ISO 22301)	Воєнні дії та загрози фізичній інфраструктурі
Цифровізація державного управління та впровадження електронних реєстрів	Кіберзагрози та ризик втрати критичних даних
Залучення міжнародної технічної та фінансової допомоги	Зростання нелегального обігу лікарських засобів і наркотиків
Розвиток ризик-орієнтованого державного нагляду	Репутаційні ризики у разі регуляторних збоїв
Посилення міжвідомчої координації	Нестабільність нормативно-правового середовища
Впровадження системи BCM як елементу національної стійкості	Переривання логістики та постачання під час криз

Ключовими викликами залишаються кадрові, фінансові та інфраструктурні обмеження, а також зростання зовнішніх загроз в умовах воєнного стану. Реалізація можливостей, пов'язаних із цифровізацією, міжнародною підтримкою та впровадженням системи безперервності

діяльності, дозволить посилити стійкість служби та знизити вплив критичних ризиків.

Професійна діяльність Держлікслужби об’єктивно реалізується в умовах підвищеного рівня ризиків, що зумовлено соціальною значущістю сфери охорони здоров’я, складністю фармацевтичного ринку, жорсткими регуляторними вимогами, а також впливом кризових чинників, зокрема воєнного стану. У цьому контексті ризик-орієнтований менеджмент і концепція безперервності діяльності виступають методологічною основою ефективного її функціонування.

Українське нормативне поле щодо управління ризиками і забезпечення безперервності діяльності активно розвивається: КМУ встановлює рамки і ініціює експерименти (наприклад, у податковій сфері та захисті критичної інфраструктури), Держаудитслужба і секторні регулятори вводять методики та індикатори, а Національне агенство України з питань державної служби (НАДС) формує кадрові стандарти, необхідні для ефективного впровадження ризик-орієнтованих підходів. Проте для сталого результату потрібна краща уніфікація підходів, масштабніша підготовка персоналу та фінансові/технічні інвестиції [30, 31, 32].

2.3 Ризики діяльності Держлікслужби

З позиції ризик-орієнтованого менеджменту діяльність Держлікслужби спрямована на систематичну ідентифікацію, аналіз, оцінювання та мінімізацію ризиків, які можуть негативно впливати на якість, безпеку та доступність ЛЗ, а також на законність обігу наркотичних засобів і прекурсорів.

Основними групами ризиків у діяльності Держлікслужби є:

– ризики потрапляння на ринок неякісних, фальсифікованих або небезпечних лікарських засобів;

– ризики порушення ліцензійних умов суб’єктами господарювання;

– ризики незаконного обігу наркотичних засобів і психотропних речовин;

– операційні та кадрові ризики, пов’язані з виконанням контрольних функцій;

– корупційні, репутаційні та правові ризики, що можуть виникати внаслідок неефективного або несвоєчасного регуляторного реагування.

Ризик-орієнтований підхід реалізується через:

– пріоритизацію контрольно-наглядових заходів залежно від рівня ризику суб’єкта господарювання;

– використання аналітичних даних, результатів інспекцій та фармаконагляду;

– застосування превентивних заходів замість суто каральних;

– прийняття управлінських рішень на основі оцінки ймовірності та масштабів негативних наслідків [33, 34, 35, 36, 37].

Таким чином, Держлікслужба функціонує не лише як контролюючий орган, а як елемент системи управління ризиками у сфері обігу ЛЗ.

З позиції ВСМ Держлікслужба відіграє ключову роль у забезпеченні безперервності критично важливих процесів у фармацевтичній та медичній сферах, що мають безпосередній вплив на національну безпеку та здоров’я населення. Її діяльність спрямована на підтримання стабільного функціонування системи контролю якості лікарських засобів навіть в умовах кризових ситуацій.

Критично важливими процесами Держлікслужби з точки зору ВСМ є:

– державний контроль якості ЛЗ;

– ліцензування виробництва, імпорту та реалізації ЛЗ;

– контроль обігу наркотичних засобів і прекурсорів;

– оперативне реагування на загрози для здоров’я населення (заборона та вилучення препаратів з обігу);

– інформаційне забезпечення суб’єктів ринку та органів влади [29].

В умовах воєнного стану, надзвичайних ситуацій, кібератак або порушення логістичних ланцюгів реалізація ВСМ передбачає:

– забезпечення резервування інформаційних ресурсів і критичних даних;

– збереження спроможності виконання контрольних і дозвільних функцій;

– адаптацію регуляторних процедур до кризових умов без зниження рівня безпеки;

– координацію з Міністерством охорони здоров'я (МОЗ), іншими органами влади та міжнародними партнерами.

Ризик-орієнтований менеджмент і ВСМ у діяльності Держлікслужби перебувають у тісному взаємозв'язку та взаємодоповнюють один одного. Ризик-менеджмент забезпечує своєчасне виявлення загроз і визначення пріоритетів регуляторного впливу, тоді як ВСМ гарантує здатність служби зберігати функціональну спроможність і виконувати свої повноваження в умовах криз.

Аналіз ризиків безперервної діяльності Держлікслужби свідчить, що найбільш критичними є регуляторні, корупційні, операційні та інформаційні ризики, посилені впливом зовнішніх факторів, зокрема воєнного стану. Їх реалізація може призвести до порушення виконання ключових функцій державного контролю у сфері обігу лікарських засобів і наркотичних речовин [33, 34, 35].

Запровадження ризик-орієнтованого підходу та інструментів ВСМ дозволяє не лише мінімізувати негативні наслідки реалізації ризиків, але й забезпечити стійкість регуляторних процесів, безперервність надання публічних послуг та збереження довіри суспільства навіть в умовах криз і надзвичайних ситуацій (табл. 2.2).

Для забезпечення безперервної роботи Держлікслужба постійно впроваджує заходи, спрямовані на мінімізацію корупції, підвищення прозорості, адаптації до змін законодавства та підтримки функціональної

стійкості, що критично важливо для охорони здоров'я населення, особливо в умовах воєнного стану [38, 39, 40, 41].

Таблиця 2.2

Основні ризики діяльності Держлікслужби та заходи забезпечення безперервності діяльності (BCM)

№	Група ризиків	Характеристика ризику	Потенційні наслідки	Ключові заходи BCM
1	**Регуляторні ризики**	Затримки, помилки або складність адаптації до нових регуляторних вимог (ліцензування, контроль, імплементація актів)	Порушення доступності ЛЗ, зниження ефективності регулювання, недовіра стейкхолдерів	Резервування процедур ухвалення рішень, цифровізація регуляторних процесів, аналіз регуляторного впливу (АРВ), розподіл повноважень
2	**Корупційні ризики**	Потенційні корупційні прояви у процесах ліцензування, контролю якості, перевірок	Репутаційні втрати, правові санкції, зниження довіри суспільства	Робота комісії з оцінки корупційних ризиків, антикорупційні програми, ротація персоналу, внутрішній контроль
3	**Ризики якості лікарських засобів**	Потрапляння на ринок неякісних або фальсифікованих препаратів	Загроза життю та здоров'ю населення, міжнародні репутаційні втрати	Пріоритетний контроль високоризикових суб'єктів, лабораторний моніторинг, оперативне вилучення, кризові комунікації
4	**Операційні ризики**	Переривання роботи територіальних органів, лабораторій або ключових процесів	Зупинка контрольних функцій, затримки перевірок і рішень	Резервні локації, дистанційні формати роботи, міжрегіональний перерозподіл функцій, стандартизовані SOP
5	**Кадрові ризики**	Дефіцит кваліфікованого персоналу, перевантаження, плинність кадрів	Зниження якості контролю, зростання операційних помилок	Перехресне навчання персоналу, кадровий резерв, матриця заміщення, навчальні програми
6	**Інформаційні та кіберризики**	Втрата, компрометація даних, кібератаки, збої IT-систем	Порушення управління, витік конфіденційної інформації, зупинка сервісів	Резервне копіювання, кіберзахист, альтернативні канали доступу, план реагування на IT-інциденти
7	**Ризики обігу наркотичних засобів**	Незаконний обіг або зловживання контрольованими речовинами	Кримінальні, соціальні та міжнародні наслідки	Посилений моніторинг, міжвідомча взаємодія, аудит ланцюгів постачання

Продовження таблиці 2.2

8	**Логістичні ризики**	Порушення постачання лікарських засобів у кризових умовах	Дефіцит життєво необхідних препаратів	Координація з МОЗ та іншими органами, міжнародна допомога, спрощені процедури у кризових умовах
9	**Правові ризики**	Оскарження регуляторних рішень, невідповідність дій законодавству	Судові спори, блокування діяльності, затримка рішень	Юридичний супровід, правовий моніторинг, актуалізація нормативної бази
10	**Репутаційні ризики**	Негативне інформаційне висвітлення діяльності, суспільна критика	Втрата довіри громадян і партнерів	План кризових комунікацій, прозорість рішень, оперативне інформування
11	**Інформаційні ризики відкритості даних**	Недостатній обмін інформацією, проблеми з доступом до відкритих даних	Зниження прозорості, недовіра громадян	Аналіз запитів громадян, удосконалення системи звітування, контроль виконання вимог щодо оприлюднення
12	**Ризики надзвичайних ситуацій**	Воєнні дії, техногенні аварії, пандемії	Повна або часткова зупинка діяльності	Плани безперервності діяльності, сценарне планування, регулярне тестування BCM

Інтеграція цих підходів відповідає вимогам міжнародних стандартів ISO 31000:2018 та ISO 22301:2019 і сприяє:

– підвищенню стійкості державного регулятора;

– мінімізації системних ризиків у сфері обігу ЛЗ;

– забезпеченню безперервного доступу населення до безпечних і якісних ЛЗ;

– зміцненню довіри до системи державного контролю.

Отже, діяльність Держлікслужби з позиції ризик-орієнтованого менеджменту та безперервності діяльності є прикладом сучасного підходу до публічного управління, орієнтованого на проактивне управління загрозами, стійкість системи охорони здоров’я та захист інтересів суспільства. Запровадження та розвиток цих підходів є необхідною умовою ефективного функціонування державного регулятора в умовах високої невизначеності та кризових викликів.

Висновки до розділу 2

Проведений аналіз засвідчив, що впровадження ризик-орієнтованого менеджменту та ВСМ у державних установах України є об’єктивною необхідністю, зумовленою зростанням рівня невизначеності, кризовими викликами та впливом воєнного стану. Водночас цей процес ускладнюється низкою системних проблем. Традиційні управлінські підходи в публічному секторі не забезпечують належного рівня стійкості в умовах динамічних загроз, у цьому контексті міжнародні стандарти ISO 31000:2018 та ISO 22301:2019 визначають методологічні засади інтеграції управління ризиками та забезпечення безперервності діяльності як взаємопов’язаних елементів сучасного публічного управління. Ідентифікація, аналіз та оцінювання ризиків є базовими компонентами ВСМ, оскільки дозволяють встановити взаємозв’язок між загрозами та критичними процесами діяльності установи, визначити пріоритети реагування та мінімізувати негативні наслідки кризових подій.

Аналіз професійної діяльності Держлікслужби показав, що вона функціонує в умовах підвищеного рівня ризиків, пов’язаних із соціальною значущістю сфери охорони здоров’я, складністю фармацевтичного ринку, жорсткими регуляторними вимогами та зовнішніми кризовими чинниками. SWOT-аналіз підтвердив наявність у Держлікслужби значного інституційного потенціалу, водночас виявив кадрові, фінансові та інфраструктурні обмеження, які впливають на її стійкість.

Інтеграція ризик-орієнтованого менеджменту та системи безперервності діяльності є необхідною передумовою підвищення стійкості Держлікслужби, мінімізації системних ризиків у сфері обігу ЛЗ і зміцнення довіри суспільства до державного регулятора. Отримані результати створюють методологічне підґрунтя для практичної апробації та розроблення прикладних рекомендацій, що буде розглянуто в наступному розділі роботи.

РОЗДІЛ 3

ПРАКТИЧНІ РЕКОМЕНДАЦІЇ ЩОДО ВПРОВАДЖЕННЯ РИЗИК-ОРІЄНТОВАНОГО ПІДХОДУ В БЕЗПЕРЕРВНУ ДІЯЛЬНІСТЬ ДЕРЖЛІКСЛУЖБИ

3.1 Практичні рекомендації щодо впровадження ризик-орієнтованого підходу в безперервну діяльність Держлікслужби

Впровадження ризик-орієнтованого підходу в систему забезпечення безперервності діяльності Держлікслужби є необхідною умовою підвищення ефективності державного контролю якості лікарських засобів в умовах підвищеної нестабільності зовнішнього середовища. Такий підхід дозволяє зосередити управлінські та ресурсні зусилля на найбільш критичних процесах і загрозах, мінімізувати наслідки інцидентів та забезпечити стійке виконання регуляторних функцій.

Першочерговою практичною рекомендацією є інституціоналізація ризик-орієнтованого підходу на рівні управління Держлікслужби шляхом затвердження єдиної політики управління ризиками та безперервністю діяльності. Така політика повинна визначати принципи ідентифікації, оцінки та моніторингу ризиків, встановлювати критерії прийнятності ризику, а також забезпечувати інтеграцію вимог ISO 22301 із чинними системами управління якістю відповідно до ISO 9001 та ISO/IEC 17025.

Наступною важливою рекомендацією є впровадження системної оцінки ризиків для всіх критичних процесів Держлікслужби, включно з лабораторними випробуваннями, інспекційною діяльністю, регуляторними рішеннями, управлінням даними та комунікаціями. Оцінка ризиків має здійснюватися на основі уніфікованих шкал ймовірності та впливу, що забезпечить порівнюваність результатів і прозорість управлінських рішень. Особливу увагу доцільно приділяти воєнним, енергетичним, кібернетичним і кадровим ризикам як таким, що мають найбільший потенціал впливу на безперервність діяльності.

Практично значущим кроком є проведення регулярного аналізу впливу на діяльність для визначення критичних функцій, допустимого часу їх переривання та пріоритетів відновлення. Результати BIA повинні безпосередньо використовуватися для встановлення часових параметрів реагування, планування ресурсів і розробки планів безперервності та відновлення діяльності. Це дозволить перейти від формального управління ризиками до реального управління наслідками.

Окремою рекомендацією є інтеграція ризик-орієнтованого підходу в систему оповіщення та реагування на інциденти. Запровадження кількісної шкали оцінки рівня загроз і чітких алгоритмів ескалації інцидентів забезпечить своєчасну активацію відповідних планів реагування та зменшить залежність прийняття рішень від суб’єктивних факторів. Важливим є застосування принципу дублювання каналів комунікації та чітке визначення ролей і відповідальності.

З метою підвищення ефективності практичної реалізації ризик-орієнтованого підходу доцільно забезпечити його інтеграцію з управлінням ресурсами, зокрема з плануванням резервного електроживлення, дублюванням IT-систем, альтернативними логістичними ланцюгами та кадровим резервом. Пріоритетність інвестування має визначатися результатами оцінки ризиків і BIA, що сприятиме раціональному використанню обмежених державних ресурсів.

Важливою практичною рекомендацією є розвиток культури управління ризиками серед персоналу. Для цього необхідно впровадити регулярні навчання, тренування та симуляції інцидентів, адаптовані до специфіки діяльності Держлікслужби. Формування ризик-орієнтованого мислення персоналу сприятиме ранньому виявленню загроз, підвищенню відповідальності та ефективності реагування у кризових ситуаціях.

З метою забезпечення постійного вдосконалення системи рекомендується впровадити механізм моніторингу та перегляду ризиків, який включає аналіз інцидентів, аудит ефективності планів безперервності та

регулярний перегляд ризик-профілю організації. Отримані результати повинні використовуватися для коригування стратегій, оновлення планів та вдосконалення процедур реагування.

Таким чином, впровадження ризик-орієнтованого підходу в безперервну діяльність Держлікслужби має здійснюватися комплексно, шляхом поєднання стратегічного управління ризиками, практичних механізмів забезпечення безперервності та розвитку організаційної культури. Реалізація запропонованих рекомендацій дозволить підвищити стійкість Держлікслужби до кризових і надзвичайних ситуацій, забезпечити стабільність державного контролю якості лікарських засобів та зміцнити довіру суспільства до системи охорони здоров'я.

3.2 Розробка політики управління ризиками для установи

Політика управління ризиками є базовим документом, який визначає принципи, підходи, відповідальність та інструменти управління ризиками в установі. Вона створює формалізовану основу для впровадження ризик-орієнтованого менеджменту та забезпечує його відповідність міжнародним стандартам ISO 31000 та ISO 22301 [36]. Для державних установ України наявність такої політики стає не лише інструментом підвищення операційної стійкості, але й критичною умовою ефективного функціонування в умовах воєнного стану та постійних загроз (Додаток Г).

1. Основною метою політики є створення єдиного підходу до:

– ідентифікації ризиків,
– оцінювання та аналізу ризиків,
– визначення рівнів прийнятності ризику,
– впровадження заходів реагування,
– моніторингу та перегляду ризиків.

Політика дозволяє інтегрувати управління ризиками у щоденну діяльність установи, покращити координацію між підрозділами та підвищити ефективність прийняття рішень.

У документі мають бути визначені принципи, які регулюють підхід установи до роботи з ризиками. Відповідно до міжнародних стандартів до них належать:

1. Системність та послідовність – управління ризиками має бути невід'ємною частиною процесів установи.

2. Прозорість та відкритість – рішення щодо ризиків приймаються на основі об'єктивних даних.

3. Безперервність процесу – ризики переглядаються регулярно, враховуючи динамічні зміни середовища.

4. Адаптивність – політика враховує особливості діяльності установи та сучасні виклики (цифровізація, воєнні дії, кіберзагрози).

5. Організаційна відповідальність – визначені ролі та відповідальні особи за управління ризиками.

Нами пропонується наступна структура політики управління ризиками:

1. Загальні положення

Описуються:

– нормативно-правові підстави,

– сфера застосування політики,

– ключові терміни й визначення (відповідно до ISO 31000).

2. Мета та завдання політики

Визначаються конкретні цілі: зниження впливу ризиків, забезпечення безперервності діяльності, оптимізація ресурсів тощо.

3. Принципи управління ризиками

Формулюються підходи, на яких побудована система управління ризиками (комплексність, документованість, інтеграція в процеси, пріоритетність критичних процесів).

4. Організаційна структура та відповідальність

У політиці мають бути визначені:

– відповідальні особи та підрозділи,

– функції керівництва,

– відповідальність власників процесів,

– роль комітету з ризиків (якщо він створений).

Особлива увага приділяється ролі керівництва, оскільки від його підтримки залежить ефективність всієї системи.

5. Процес управління ризиками описуються наступними ключовими етапами:

Ідентифікація ризиків – виявлення внутрішніх і зовнішніх загроз.

Оцінювання ризиків – визначення ймовірності і впливу.

Ранжування та визначення прийнятності – встановлення рівнів ризиків.

Розроблення заходів реагування – уникнення, зменшення, передання, прийняття ризику.

Моніторинг і контроль – регулярна оцінка та оновлення реєстру ризиків.

6. Документування та звітність. Політика визначає:

– вимоги до ведення Реєстру ризиків,

– форму звітів,

– періодичність перегляду ризиків,

– взаємодію між підрозділами у процесі аналізу ризиків.

Політика управління ризиками повинна бути узгоджена з планом безперервності діяльності (BCP), планом відновлення після аварії (DRP), політикою інформаційної безпеки, антикорупційною програмою, планом реагування на надзвичайні ситуації.

Інтеграція забезпечує ефективний обмін інформацією й узгодженість управлінських дій [31, 34, 35].

Для ефективного впровадження політики нам необхідно затвердити її керівником установи та забезпечити ознайомлення всіх співробітників. провести навчання персоналу та впровадити інструменти оцінювання та контролю, забезпечити регулярний перегляд політики (щонайменше раз на рік).

У наукових дослідженнях підкреслюється, що культура управління ризиками та навчання персоналу відіграють ключову роль у формуванні ефективної системи ризик-менеджменту.

Політика має бути «живим» документом. Її актуальність повинна оцінюватися у разі змін у законодавстві, при структурних змінах в установі, після виникнення інцидентів та при появі нових загроз (кібератаки, зміни політичної ситуації, воєнні дії) [36].

Перегляд політики забезпечує її відповідність реальним викликам, що особливо актуально для України.

Політика будується на таких бізнес-процесах, що впливають на безперервність діяльності Держлікслужби наведених в таблиці 3.1.

Таблиця 3.1.

Бізнес-процеси, що впливають на безперервність діяльності Держлікслужби

№	Бізнес-процес	Умови виконання	Рівень критичності
1	Державний контроль якості лікарських засобів (лабораторні випробування)	Функціонування лабораторій, наявність електропостачання, реактивів, справного обладнання, кваліфікованого персоналу	**Критичний**
2	Приймання, реєстрація та ідентифікація зразків	Доступ до приміщень, робота LIMS, забезпечення простежуваності	
3	Зберігання зразків і реактивів	Безперебійне електропостачання, контроль температури, охорона приміщень	**Високий**
4	Оформлення протоколів випробувань та висновків	Доступ до інформаційних систем, наявність уповноважених фахівців	**Критичний**
5	Функціонування LIMS та IT-інфраструктури	Стабільна робота серверів, кібербезпека, резервне копіювання	**Високий**
6	Регуляторна діяльність і прийняття рішень	Наявність результатів випробувань, комунікація з підрозділами та МОЗ	**Високий**

Продовження таблиці 3.1.

7	Взаємодія з митними, правоохоронними та іншими органами	Доступність каналів зв’язку, уповноважений персонал	**Середній**
8	Логістика та постачання реактивів і матеріалів	Наявність постачальників, транспортна доступність, фінансування	**Високий**
9	Управління персоналом (кадрове забезпечення)	Доступність ключових фахівців, резерв персоналу	**Високий**
10	Забезпечення біобезпеки та охорони праці	Наявність ЗІЗ, справні системи вентиляції, навчений персонал	**Критичний**
11	Комунікація та система оповіщення	Функціонування каналів зв’язку, актуальні контакти	**Критичний**
12	Адміністративно-господарське забезпечення	Доступ до будівель, охорона, енергозабезпечення	**Середній**

Правильно розроблена політика дозволяє установі формалізувати і посилити культури управління ризиками, забезпечити виконання критично важливих функцій та покращити міжпідроздільну координацію й мінімізувати наслідки кризових ситуацій та відповідати міжнародним стандартам і рекомендаціям [38, 39, 41].

Алгоритм побудови системи управління ризиками СЗББ Держлікслужби (відповідно до ISO 22301, ISO 31000, ERM)

1. Визначення контексту

↓

2. Ідентифікація ризиків

↓

3. Аналіз впливу на діяльність (BIA)

↓

4. Оцінка ризиків (P × I)

↓

5. Пріоритизація критичних ризиків

↓

6. Визначення стратегій реагування

↓

7. Інтеграція в BCP / DRP / Crisis Management

↓

8. Реалізація заходів контролю

↓

9. Моніторинг, тестування, аудит

↓

10. Перегляд і постійне вдосконалення

Деталізований опис етапів алгоритму:

1. Визначення контексту діяльності. Метою етапу є формування загального середовища управління ризиками безперервності. Включає: визначення місії Держлікслужби як регуляторного органу, аналіз зовнішнього контексту (воєнний стан, законодавство, кіберзагрози), аналіз внутрішнього контексту (структура, ресурси, IT, кадри), ідентифікацію зацікавлених сторін (МОЗ, Уряд, лабораторії, громадськість). Результат: затверджений контекст управління ризиками СЗББ.

2. Ідентифікація ризиків безперервності. Виявляються події, що можуть порушити виконання регуляторних функцій. Категорії ризиків: безпекові та воєнні, управлінські та кадрові, IT та кіберризики, інфраструктурні та енергетичні, логістичні, правові та репутаційні. Результат: реєстр ризиків безперервності діяльності.

3. Аналіз впливу на діяльність (BIA). Визначається значущість кожного ризику для критичних функцій. Оцінюється: які процеси є критичними; наслідки їх зупинки; допустимий час переривання (MTPD); залежність від ресурсів та персоналу. Результат: перелік критичних процесів і часові параметри (MTPD, RTO, RPO).

4. Оцінка ризиків. Здійснюється кількісна або напівкількісна оцінка: $R = P \times I$, де: P – імовірність; I – вплив на діяльність Держлікслужби.

Використовується матриця ризиків. Результат: класифікація ризиків за рівнем (низький – критичний).

5. Пріоритизація критичних ризиків. Виділяються ризики: червоної зони (критичні), помаранчевої зони (високі). Саме вони: включаються до BIA та потребують обов'язкових планів реагування. Результат: перелік пріоритетних ризиків СЗББ.

6. Визначення стратегій реагування. Для кожного критичного ризику визначається стратегія: уникнення, зменшення, передача, прийняття (обґрунтоване). Формуються заходи: організаційні;, технічні, IT, кадрові, комунікаційні. Результат: план заходів управління ризиками безперервності.

7. Інтеграція в BCP, DRP та кризове управління. Ризики трансформуються у: сценарії інцидентів, плани реагування, плани відновлення діяльності, систему оповіщення. Результат: узгоджена система документів BCMS.

8. Реалізація заходів контролю впроваджуються за рахунок резервних каналів зв'язку, дублюванню управлінських функцій, резервуванню IT, альтернативним режими роботи. Результат: практична готовність до інцидентів.

9. Моніторинг, тестування та аудит проводиться: регулярний моніторинг ризиків; навчання персоналу; тестування BCP; внутрішні аудити BCMS. Результат: оцінка ефективності СЗББ.

10. Перегляд і постійне вдосконалення здійснюється на основі: інцидентів, навчань, змін контексту, результатів аудитів. Система коригується. Результат: динамічна, адаптивна система управління ризиками безперервності.

Запропонований алгоритм забезпечує системний, ризик-орієнтований та стандартизований підхід до побудови СЗББ Держлікслужби, поєднуючи ERM, BIA та BCMS в єдину логічну модель. Його впровадження дозволяє своєчасно ідентифікувати загрози, мінімізувати наслідки інцидентів та

забезпечити безперервне виконання державних регуляторних функцій навіть у кризових умовах.

2.3 Формування плану забезпечення безперервності діяльності

План забезпечення безперервності діяльності (Business Continuity Plan, BCP) є ключовим документом, що визначає порядок дій установи в умовах надзвичайних ситуацій, технічних збоїв, кібератак, воєнних дій та інших кризових подій. Його основна мета – забезпечити виконання критично важливих функцій та відновлення роботи установи у прийнятні терміни, відповідно до вимог стандартів ISO 22301 та ISO 22313 [42, 43, 44].

Для державних установ України наявність якісного BCP є критичною передумовою операційної стійкості, особливо в умовах воєнного стану та постійних загроз інфраструктурі.

1. Структура та зміст плану забезпечення безперервності діяльності повністю приведений у Додатку Д до роботи. BCP зазвичай включає такі ключові розділи:

- резервні процедури;
- система управління кризами;
- план реагування на надзвичайні ситуації;
- порядок відновлення IT-систем і даних;
- внутрішні та зовнішні комунікаційні стратегії.

Документ формується на основі аналізу ризиків та аналізу впливу на діяльність (BIA), що дозволяє встановити пріоритети для критичних процесів.

2. Резервні процедури – це заходи, спрямовані на забезпечення безперервності виконання важливих процесів у випадку збою або недоступності ресурсів. До них належать:

- створення резервних копій документів, реєстрів, баз даних;
- резервування обладнання, робочих місць, каналів зв’язку;

– впровадження альтернативних процедур виконання критичних функцій (наприклад, перехід на паперовий документообіг у разі відмови IT-систем);

– дублювання ключових ролей персоналу;

– організація альтернативних локацій для роботи (back-up site), що рекомендовано ISO 22301.

Резервні процедури забезпечують мінімальний рівень функціонування установи навіть у разі значних порушень у роботі.

3. Система управління кризами описує процеси прийняття рішень та координації дій у разі реалізації серйозного інциденту.

Елементи системи управління кризами:

– Створення кризової команди. До її складу входять керівники підрозділів, IT-спеціалісти, фахівці з безпеки, юристи та відповідальні за комунікації.

– Чіткий розподіл ролей і відповідальності. Це включає порядок виклику членів команди, перелік їхніх обов’язків та рівні доступу до ресурсів.

– Процедури прийняття рішень. Описуються механізми визначення пріоритетів, впровадження тимчасових заходів та затвердження ключових рішень.

– Оцінювання ситуації та ескалація. Визначаються рівні загроз і критерії переходу до планів реагування.

Ефективна система управління кризами дозволяє уникати хаотичних дій та забезпечує узгодженість реагування.

4. План реагування на надзвичайні ситуації визначає послідовність дій персоналу у разі виникнення конкретних інцидентів, таких як:

– пожежа;

– техногенні аварії;

– кібератаки;

– обстріли, диверсії, воєнні загрози;

– відмови обладнання;

– відключення електроенергії, зв’язку, інтернету.

План реагування включає:

– інструкції для працівників;

– схеми евакуації та оповіщення;

– доступ до аварійних ресурсів;

– механізми взаємодії з ДСНС, поліцією, енергетичними й комунальними службами;

– критерії переходу до плану відновлення (DRP).

Цей план є обов’язковим для державних установ відповідно до національних вимог цивільного захисту.

5. Відновлення IT-систем і даних (Disaster Recovery Plan, DRP) є критичним етапом BCP, особливо для установ, які значною мірою залежать від електронних реєстрів, систем документообігу та цифрових ресурсів.

DRP включає:

– пріоритетність відновлення систем відповідно до критичних процесів;

– визначення Recovery Time Objective (RTO) та Recovery Point Objective (RPO);

– процедури відновлення серверів, мереж, інформаційних систем;

– порядок доступу до резервних копій;

– сценарії перенесення роботи в «хмарні» середовища або на резервні сервери;

– перевірку цілісності даних після відновлення.

У сучасних умовах особливо актуальними є заходи захисту від кібератак та забезпечення стійкості до відключень електроенергії.

6. Комунікаційні стратегії є ключовим компонентом BCP і має охоплювати:

6.1. Внутрішні комунікації включають оперативне інформування персоналу; альтернативні канали зв’язку (месенджери, супутниковий зв’язок, радіозв’язок); повідомлення про зміни в режимах роботи.

6.2. Зовнішні комунікації повинні забезпечувати інформування громадян про актуальний порядок надання послуг; координацію з органами влади, ДСНС, військовими адміністраціями; офіційні заяви та оновлення на вебсайтах і соцмережах; роботи зі ЗМІ.

Комунікації мають бути чіткими, своєчасними та узгодженими, що відповідає рекомендаціям ISO 22301 [42, 43, 44].

7. Тестування, навчання та актуалізація BCP. BCP має бути документом, що постійно актуалізується. Обов’язковими є:

– навчання персоналу;
– тренування та моделювання інцидентів;
– щорічний перегляд та коригування плану;
– звіти про результати тестування.

Регулярна перевірка планів підвищує їхню ефективність і дозволяє виявити слабкі місця.

2.4 Показники ефективності системи управління ризиками та безперервністю діяльності

Ефективність системи управління ризиками та безперервністю діяльності BCM визначається здатністю установи своєчасно і результативно відповідати на загрози, зменшувати їхній вплив і забезпечувати виконання критично важливих функцій. Міжнародні стандарти ISO 31000 та ISO 22301 наголошують на необхідності формування кількісних та якісних показників ефективності – KPI (Key Performance Indicators) та KRI (Key Risk Indicators) [42, 43, 44].

У державних установах ці показники мають особливе значення, оскільки відображають не лише внутрішню стійкість організації, а й здатність забезпечувати безперервність публічних послуг у кризових умовах.

1. Загальні підходи до оцінювання ефективності. Оцінювання ефективності передбачає:

– вимірювання здатності установи мінімізувати вплив інцидентів;

– оцінку швидкості та результативності реагування;

– визначення рівня зрілості системи управління ризиками;

– аналіз готовності персоналу;

– перевірку відповідності міжнародним стандартам.

Ефективність системи оцінюється на основі кількісних та якісних показників, із регулярним моніторингом і звітністю.

2. Ключові показники результативності управління ризиками (KPI)

2.1. Операційні показники: час виявлення ризику (Detection Time) – середній час між появою ризику та його ідентифікацією та час реакції на ризик (Response Time) – швидкість ухвалення рішень щодо заходів реагування. Кількість реалізованих ризиків за певний період порівняно з попередніми роками. Частка ризиків, рівень яких зменшився внаслідок впроваджених заходів.

2.2. Показники впливу: сума або масштаб збитків, яких вдалося уникнути завдяки заходам менеджменту, кількість критичних процесів, стійкість яких було підвищено та тривалість перерв у роботі установи (чим менша, тим вищий рівень стабільності).

3. Показники ефективності плану безперервності діяльності (BCP).

3.1. Показники часу відновлення: RTO (Recovery Time Objective) – цільовий час відновлення процесу; RPO (Recovery Point Objective) – рівень допустимої втрати даних; Фактичний час відновлення послуг після інцидентів. Чим менша різниця між плановими (RTO/RPO) і фактичними значеннями, тим ефективнішим є BCP.

3.2. Готовність установи:

– наявність резервних каналів зв’язку, серверів, альтернативних майданчиків;

– відсоток актуальних резервних копій даних;

– частота тестування BCP.

Міжнародні рекомендації вказують на необхідність тестування не рідше одного разу на рік

4. Показники ефективності у сфері IT та кібербезпеки: кількість кіберінцидентів, що успішно заблоковані завдяки заходам безпеки, тривалість відновлення IT-систем після збою чи атаки, відсоток оновленого ПЗ і систем захисту.

Наявність сертифікованих систем інформаційної безпеки, що підвищує стійкість установи.

5. Показники готовності персоналу: оцінюються рівень обізнаності працівників щодо процедур реагування на ризики, участь у навчаннях і тренінгах, кількість проведених навчань за рік, показники дисципліни виконання процедур (наприклад, дотримання інструкцій під час тестувань) та якість взаємодії між підрозділами під час інцидентів.

Навчання персоналу називається одним із ключових факторів формування дієвої системи ризик-менеджменту.

6. Показники зрілості системи управління ризиками

– Показники зрілості визначають, наскільки система інтегрована у діяльність установи. Зазвичай оцінюють такі рівні:

– Первинний рівень – ризики визначаються епізодично.

– Базовий рівень – є процедури, але відсутня їхня системність.

– Стандартизований рівень – процес інтегровано у діяльність установи.

– Управлінський рівень – ризик-менеджмент впливає на стратегічні рішення.

– Оптимізаційний рівень – система постійно вдосконалюється.

Оцінювання зрілості визначається у відповідності до моделей, рекомендованих ISO 22301.

7. Показники для зовнішньої оцінки. Для державних установ важливі також: виконання вимог законодавства і стандартів, наявність аудиторських

перевірок, які підтверджують надійність системи, оцінки громадськості щодо стабільності надання послуг, статистичні показники часу обслуговування громадян у кризових умовах.

Ці показники визначають, наскільки система управління ризиками ефективна з погляду зовнішніх стейкґолдерів.

8. Комплексна система оцінювання ефективності. Найефективніші моделі передбачають:

– комбінацію кількісних і якісних показників;

– регулярний моніторинг виконання KPI і KRI;

– щорічні звіти з управління ризиками;

– перегляд цілей та методів реагування залежно від результатів оцінювання.

Такі моделі допомагають установам адаптуватися до змін, у тому числі до воєнних умов і динамічного середовища функціонування.

3.5 Організаційні зміни: створення робочих груп, визначення ролей і відповідальності

Ефективне впровадження ризик-орієнтованого менеджменту та забезпечення безперервності діяльності потребує не лише методичних і технічних рішень, а й суттєвих організаційних змін. Центральним елементом цих змін є формування спеціалізованих робочих груп та чітке визначення ролей і відповідальності персоналу, що дає змогу забезпечити скоординованість дій, підвищити оперативність та уникнути дублювання функцій (Додаток Е та Додаток Ж).

1. Формування робочих груп з управління ризиками та безперервністю діяльності.

Спеціальна робоча група (Risk Management Team або Business Continuity Team) створюється з метою: координації процесів ідентифікації, аналізу та оцінювання ризиків, розроблення політики управління ризиками та планів безперервності діяльності, моніторингу змін у внутрішньому та

зовнішньому середовищі установи, організації навчань, тренінгів і тестування BCP, реагування на інциденти та управління кризами.

Наявність робочої групи є ключовою вимогою системи управління відповідно до стандартів ISO 22301 та ISO 31000.

2. Структура та склад робочої групи

До складу зазвичай входять: керівник установи або його заступник (керівник BCP/ризик-менеджменту), керівники структурних підрозділів, фахівці з IT та кібербезпеки, спеціалісти з кадрової роботи та комунікацій, представники юридичного відділу, експерти з цивільного захисту, відповідальні за документообіг та критичні процеси.

Важливо, щоб у команді були представлені всі критично важливі напрями діяльності.

3. Ролі та відповідальність у системі ризик-менеджменту.

Керівник системи управління ризиками / BCP-координатор ідповідальний за:

– загальну організацію процесів;
– затвердження політик і планів;
– взаємодію з керівництвом та зовнішніми органами;
– контроль виконання заходів;
– координацію роботи підрозділів у кризовій ситуації.

3.2. Члени робочої групи (фахівці підрозділів) виконують:

– аналіз ризиків у межах свого напрямку;
– розроблення та впровадження заходів;
– надання звітності та даних для моніторингу;
– участь у тестуваннях та навчаннях;
– оперативну взаємодію під час інцидентів.

3.3. IT-підрозділ відповідає за:

– кіберзахист;
– резервування даних;

– відновлення ІТ-систем;

– забезпечення альтернативних каналів зв’язку;

– підтримку інформаційної інфраструктури під час інцидентів.

3.4. Юридичний відділ забезпечує відповідність:

– законодавству України;

– вимогам захисту персональних даних;

– нормативам у сфері цивільного захисту;

– міжнародним стандартам (за наявності сертифікації).

3.5. Підрозділ комунікацій забезпечує:

– внутрішнє інформування персоналу;

– зовнішні офіційні повідомлення;

– координацію із ЗМІ та громадськістю;

– правильність і своєчасність інформаційних повідомлень.

4. Формалізація відповідальності.

Для ефективного управління ролі та відповідальність мають бути зафіксовані в організаційно-розпорядчій документації: положенні про робочу групу; наказі керівника установи про її створення; посадових інструкціях і регламентах; плані забезпечення безперервності діяльності; матриці відповідальності (RACI-матриця).

4.2. RACI-матриця. У ній вказується, хто: R (Responsible) – виконує; A (Accountable) – несе відповідальність; C (Consulted) – консультується; I (Informed) – інформується.

Цей інструмент забезпечує прозорість виконання всіх процедур.

Реалізація організаційних змін сприяє:

– підвищенню готовності персоналу до дій у кризових умовах;

– скороченню часу прийняття рішень;

– узгодженості заходів на рівні всієї установи;

– підвищенню ефективності BCP та управління ризиками;

– відповідності кращим світовим практикам.

Дослідження українських і зарубіжних експертів підтверджують, що саме організаційна структура, а не технічні рішення, часто є вирішальним фактором ефективності ризик-менеджменту [31, 36].

3.3 Навчання персоналу та підвищення ризик-культури

Формування ефективної системи управління ризиками та забезпечення безперервності діяльності неможливе без підготовленого персоналу та належної організаційної культури. Саме ризик-культура визначає, як працівники сприймають ризики, реагують на них, дотримуються процедур і беруть участь у впровадженні заходів щодо стабільності діяльності установи.

Міжнародні стандарти ISO 31000 та ISO 22301 підкреслюють, що людський фактор є ключовим елементом успішного ризик-менеджменту. Українські дослідження також підтверджують, що недостатня обізнаність персоналу та слабка ризик-культура є типовими бар’єрами для впровадження сучасних управлінських практик [31, 36].

Навчання персоналу спрямоване на формування знань, навичок і компетенцій, необхідних для:

– ідентифікації та аналізу ризиків;
– виконання процедур плану безперервності діяльності (BCP);
– реагування на інциденти;
– взаємодії з іншими підрозділами під час криз;
– підтримання інформаційної безпеки;
– дотримання стандартів і внутрішніх регламентів.

У міжнародній практиці навчання визначене як обов’язковий компонент системи управління ризиками, який підлягає регулярному оновленню.

2. Основні форми навчання персоналу

Базове навчання (introductory training) проводиться для всіх працівників організації й охоплює загальні принципи ризик-менеджменту питання

ознайомлення з політикою управління ризиками, порядок дій у кризових ситуаціях, правила кібергігієни та огляд планів реагування та BCP.

Поглиблене навчання для відповідальних осіб – це спеціальна підготовка для членів робочих груп з ризик-менеджменту, IT-персоналу, відповідальних за процеси цивільного захисту, керівників підрозділів. Вона включає практичні кейси, аналіз сценаріїв, моделювання ризиків і кризових подій.

Одним із найефективніших методів підготовки персоналу є тренування та симуляції:

- рольові моделі кризових ситуацій;
- навчальні евакуації;
- симуляції кібератак;
- тестування BCP (table-top і functional testing).

Симуляції дозволяють перевірити готовність працівників та знайти слабкі місця в реальних умовах.

Ризик-культура – це система цінностей, норм і поведінкових моделей, що визначають ставлення працівників до ризиків. Вона охоплює готовність відкрито повідомляти про інциденти, дисципліну виконання процедур, відповідальність за власні дії, підтримку безпеки організації на щоденному рівні.

Елементами розвитку ризик-культури є комунікація та інформування, внутрішні розсилки, регулярні наради, доступні інструкції, відкритість керівництва до зворотного зв’язку.

Керівники підрозділів задають стандарти поведінки та сприяють створенню середовища, де ризик-менеджмент – це щоденна практика яка базується на мотивації та стимулюванню, преміюванню за участь у навчаннях, визнанню високих показників безпеки, включенню компетенцій у службові оцінювання, регулярній оцінці ризик-культури де використовуються опитування, інтерв’ю, аналіз інцидентів.

При цьому HR-менеджери виконують важливі функції з інтеграції ризик-компетенцій у програму адаптації нових співробітників, проведення навчань та сертифікацій, забезпечення внутрішніх комунікацій та участь у формуванні корпоративних стандартів поведінки.

Керівництво установи відповідає за стратегічне закріплення ризик-культури через відповідні політики, інструкції та організаційну підтримку.

Наявність підготовленого персоналу з високою ризик-культурою забезпечує: швидке реагування на інциденти, зменшення кількості помилок, ефективне використання ресурсів, кращу координацію дій між підрозділами, зниження загального рівня операційних, фінансових і кіберризиків.

Проведений SWOT-аналіз свідчить, що Держлікслужба загалом має інституційну, кадрову та нормативну основу для впровадження BCMS. Наявність діючих систем управління якістю, досвіду роботи в умовах криз та централізованої структури управління створює сприятливі передумови для інтеграції вимог ISO 22301 у поточну діяльність (табл. 3.2.).

Водночас встановлено, що основними обмеженнями є фрагментарність управління ризиками, відсутність єдиного формалізованого підходу до безперервності на рівні всієї служби, залежність критичних процесів від окремих фахівців та обмеженість ресурсів. За умов воєнних, енергетичних і кібернетичних загроз ці чинники можуть суттєво знижувати стійкість діяльності.

Аналіз можливостей і загроз показує, що впровадження BCMS є не лише управлінською необхідністю, а й стратегічною можливістю для підвищення операційної стійкості, довіри суспільства та відповідності європейським стандартам. Не реалізувавши цю можливість суттєво підвищуємо ризик зупинки критичних регуляторних функцій у кризових умовах.

Таким чином, результати SWOT-аналізу підтверджують, що Держлікслужба перебуває на етапі інституційної готовності до впровадження

системи, однак потребує формалізації, стандартизації та системної інтеграції управління ризиками.

Таблиця 3.2.

SWOT-аналіз готовності Держлікслужби до впровадження системи безперервності бізнесу

Сильні сторони (Strengths)	**Слабкі сторони (Weaknesses)**
Наявність законодавчо визначених повноважень та чітко окресленої регуляторної ролі	Відсутність формалізованої та уніфікованої BCMS на рівні всієї служби
Функціонування систем управління якістю відповідно до ISO 9001 та ISO/IEC 17025	Фрагментарний підхід до управління ризиками в окремих підрозділах
Досвід роботи в умовах кризових ситуацій та воєнного стану	Обмежені фінансові та кадрові ресурси
Наявність кваліфікованого персоналу у критичних напрямах діяльності	Залежність окремих процесів від ключових фахівців
Процесний та ризик-орієнтований підхід у лабораторній діяльності	Недостатній рівень інтеграції IT, інформаційної безпеки та безперервності
Централізована структура управління	Нерівномірний рівень підготовки персоналу з питань BCM
Можливості (Opportunities)	**Загрози (Threats)**
Гармонізація з європейськими стандартами управління та вимогами ISO 22301	Воєнні дії, ракетні обстріли, загрози фізичній інфраструктурі
Інтеграція BCM з наявними системами управління (ERM, СУЯ, ІБ)	Відключення електропостачання та зв’язку
Залучення міжнародної технічної допомоги та експертної підтримки	Кіберзагрози, атаки на державні інформаційні ресурси
Цифровізація процесів та розвиток резервних IT-рішень	Перебої у постачанні реактивів, обладнання, IT-компонентів
Формування сталої ризик-культури та підвищення компетентності персоналу	Кадрові втрати, мобілізація, професійне вигорання
Підвищення довіри суспільства та міжнародних партнерів	Часті зміни нормативно-правового середовища

Реалізація дозволить підвищити стійкість служби до кризових подій, мінімізувати наслідки інцидентів та забезпечити безперервне виконання регуляторних функцій навіть в умовах надзвичайних ситуацій.

Наступним кроком нашої реалізації результатів дослідження буде пілотне впровадження BCMS яке є ключовим практичним етапом розвитку системи управління ризиками та забезпечення безперервності діяльності установи. Воно дозволяє оцінити реальну ефективність процедур, визначити можливі недоліки, перевірити готовність персоналу та забезпечити адаптацію регламентів до практичних умов. Значення пілотного впровадження особливо велике для державних органів, діяльність яких прямо впливає на національну безпеку та стабільність критично важливих секторів.

Висновки до розділу 3

У розділі доведено, що впровадження ризик-орієнтованого підходу в систему забезпечення безперервності діяльності Держлікслужби є необхідною умовою її стійкого функціонування в умовах воєнних, техногенних, кібернетичних та організаційних загроз. Інтеграція принципів управління ризиками відповідно до ISO 31000 із вимогами ISO 22301 формує цілісну модель управління, спрямовану на збереження критичних регуляторних функцій та мінімізацію наслідків інцидентів.

Розроблені практичні рекомендації, політика управління ризиками, алгоритм побудови системи СЗББ, а також підходи до формування плану безперервності діяльності створюють методологічну й організаційну основу для підвищення операційної стійкості Держлікслужби. Визначення критичних бізнес-процесів, часових параметрів відновлення, системи оповіщення та показників ефективності забезпечує керованість реагування та відновлення діяльності.

Обґрунтовано, що ефективність системи безперервності значною мірою залежить від організаційних змін, чіткого розподілу ролей, підготовки персоналу та розвитку ризик-культури. Таким чином, реалізація запропонованого підходу дозволяє забезпечити стабільне виконання функцій Держлікслужби, відповідність міжнародним стандартам та підвищення довіри до системи державного контролю якості лікарських засобів.

ЗАГАЛЬНІ ВИСНОВКИ

У результаті проведеного аналізу встановлено, що ризик-орієнтований менеджмент (Risk-Based Management) є ключовим інструментом сучасного управління організаціями в умовах підвищеної невизначеності та зростаючих загроз. Його суть полягає у системному та проактивному підході до ідентифікації, оцінювання та управління ризиками з метою забезпечення стійкості, безперервності та ефективності діяльності.

Доведено, що ризики мають комплексний і багатовимірний характер, формуються під впливом внутрішніх і зовнішніх чинників, а їх реалізація може призводити до фактичних втрат. Це обґрунтовує необхідність використання класифікації ризиків за джерелом, сферою впливу, масштабом, ймовірністю та наслідками, відповідно до ISO 31000:2018.

Аналіз показав, що ефективне управління ризиками потребує належної ідентифікації загроз та використання спеціалізованого інструментарію оцінювання, що забезпечує прийняття обґрунтованих управлінських рішень і мінімізацію негативних наслідків. Особливого значення ризик-орієнтований підхід набуває у публічному секторі, де ризики можуть мати суспільно значущі наслідки.

Концепція безперервності діяльності (BCM) розглядається як логічне продовження ризик-менеджменту, забезпечуючи здатність організації підтримувати та відновлювати критично важливі функції у кризових ситуаціях. Аналіз міжнародних стандартів ISO 22301:2019 та ISO 31000:2018 підтвердив доцільність інтеграції ризик-менеджменту та систем безперервності діяльності для формування єдиної моделі управління стійкістю.

SWOT-аналіз та дослідження діяльності Держлікслужби показали, що вона має значний інституційний потенціал, але стикається з кадровими, фінансовими та інфраструктурними обмеженнями, які впливають на її стійкість. Інтеграція ризик-орієнтованого менеджменту та BCM є необхідною

для мінімізації системних ризиків у сфері обігу лікарських засобів і зміцнення довіри суспільства до державного регулятора.

Розроблені практичні рекомендації, політика управління ризиками, алгоритм побудови системи управління ризиками та план безперервності діяльності створюють організаційну і методологічну основу для забезпечення стабільного виконання критично важливих функцій Держлікслужби. Визначення критичних бізнес-процесів, часових параметрів відновлення, системи оповіщення та показників ефективності підвищує керованість процесів і мінімізує наслідки інцидентів.

Особлива роль належить організаційним змінам, чіткому розподілу ролей, створенню робочих груп, навчанням персоналу та розвитку ризик-культури, що визначають ефективність впроваджених механізмів безперервності.

Таким чином, впровадження запропонованого ризик-орієнтованого підходу забезпечує підвищення стійкості Держлікслужби, збереження функціональної спроможності в кризових умовах, відповідність міжнародним стандартам та зміцнення довіри держави, професійної спільноти та суспільства. Запропоновані рішення можуть слугувати моделлю практичної реалізації BCMS для інших органів державної влади України.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Штангрет А. М., Караїм М. М., Караїм О. В. Безпекові аспекти застосування ризик-орієнтованого управління підприємством в умовах воєнного стану. *Економіка та суспільство*. 2024. № 60. DOI: 10.32782/2524-0072/2024-60-8.

2. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Київ : УкрНДНЦ, 2019. 24 с.

3. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT ; ISO 22301:2019, IDT) ; чинний від 01.09.2022. Офіц. вид. Київ : УкрНДНЦ, 2022. 18 с.

4. Про затвердження Положення про вимоги до системи управління ризиками надавача нефінансових платіжних послуг та внесення зміни до Положення про вимоги до системи управління надавача фінансових платіжних послуг : Постанова Міністерства фінансів України від 02 лип. 2025 р. № 73. URL: https://zakon.rada.gov.ua/laws/show/v0073500-25#Text (дата звернення: 08.12.2025).

5. Про безперервність функціонування представницьких органів місцевого самоврядування (сільських, селищних, міських, районних у містах, районних, обласних рад, сільських, селищних, міських голів) в Україні в умовах збройної агресії російської федерації : Постанова Верховної Ради України від 08.10.2025 р. № 4621-IX. URL: https://ips.ligazakon.net/document/t254621?ed=2025_10_08 (дата звернення: 08.12.2025).

6. Щодо забезпечення безперервної роботи : Наказ МОЗ України від 07 берез. 2022 р. № 427. URL: https://moz.gov.ua/uk/decrees/nakaz-moz-ukraini-vid-07032022--427-schodo-zabezpezpechennja--bezperervnoi-roboti (дата звернення: 08.12.2025).

7. Забезпечуємо безперебійну роботу. *Державна служба України з лікарських засобів та контролю за наркотиками* : офіційний сайт. 2022. URL:

https://www.dls.gov.ua/news (дата звернення: 08.12.2025).

8. Данілова Е. І. Методологія ризик-орієнтованого підходу до управління економічною безпекою підприємства. *Modern Economics*. 2018. № 12. P. 61–68.

9. ISO 9001:2015. Quality management systems – Requirements. Geneva : ISO, 2015. 29 p.

10. Hopkin P. Fundamentals of Risk Management: Understanding, Evaluating and Implementing Effective Risk Management. 5th ed. London : Kogan Page, 2021. 512 p.

11. Гобела В. В., Леськів Г. З., Фляк В. М. Моделювання системи ризик-орієнтованого управління підприємством. *Науковий вісник Львівського державного університету внутрішніх справ. Серія економічна*. 2023. Вип. 2. С. 10–20. URL: http://nbuv.gov.ua/UJRN/Nvldu_e_2023_2_4 (дата звернення: 08.12.2025).

12. Вербицька Г. Л. Управління економічним ризиком. *Фінанси України*. 2019. № 4. С. 34–41.

13. Управління кризовими ситуаціями : навч. посіб. / В. В. Гобела та ін. Львів : ЛьвДУВС, 2022. 227 с.

14. Ріщук Л. І. Підхід щодо розробки програми управління ризиками на підприємстві. *Проблеми і перспективи розвитку підприємництва*. 2015. № 1(2). С. 77–82.

15. Кузьмак О. М. Ефективна система ризик-менеджменту як дієвий засіб забезпечення стійкості фінансових установ. *Наука і Європа*. 2015. № 10. С. 94−101. URL: https://journals.khnu.km.ua/vestnik/pdf/ekon/2011_2_2/164-166.pdf (дата звернення: 08.12.2025).

16. Лук’янова В. В. Оцінювання ризику і стійкість економічної системи. *Вісник Хмельницького національного університету. Серія : Економічні науки*. 2014. Т. 2, № 3. С. 33–39.

17. Управління конкурентоспроможністю підприємства : навч. посіб. / Г. З. Леськів.та ін. Львів : ЛьвДУВС, 2022. 220 с.

18. Сосновська О. О. Ризик-менеджмент як інструмент забезпечення стійкого функціонування підприємства в умовах невизначеності. *Європейський науковий журнал економічних та фінансових інновацій*. 2019. № 1(3). С. 70–79.

19. Гречаніченко О. О. Сутність та особливості застосування ризик-орієнтованого підходу в публічному управлінні. *Інвестиції: практика та досвід*. 2020. № 23. С. 151–156.

20. Луганова І. А. Сутність та принципи концепції ризик-менеджменту. *Актуальні проблеми державного управління*. 2018. Вип. 1(53). URL: https://surl.li/txtsfs (дата звернення: 08.12.2025).

21. Кібік О., Слободянюк О., Кузнецова Л. Ризик-менеджмент : навч.-метод. посіб. / Нац. ун-т «Одес. юрид. академія». Одеса : Фенікс, 2024. 84 с.

22. Herbane B. Business Continuity Management: A Crisis Management Approach. London : Routledge, 2019. 224 p.

23. Mohamed N., Alharthi A. N., Khalifa G. S. A. Business Continuity Management and Crisis Leadership: An Approach to ReEngineer Crisis Performance within Abu Dhabi Governmental Entities. *International Journal on Emerging Technologies*. 2019. № 10(1a). P. 32–40.

24. Про реалізацію експериментального проєкту щодо функціонування системи управління податковими ризиками (комплаєнс-ризиками) в Державній податковій службі : Постанова Кабінету Міністрів України від 25 лип. 2024 р. № 854. URL: https://zakon.rada.gov.ua/laws/show/854-2024-%D0%BF#Text (дата звернення: 08.12.2025).

25. Про затвердження вимог щодо управління ризиками безпеки на об'єктах критичної інфраструктури I категорії критичності : Постанова Кабінету Міністрів України від 1 квіт. 2025 р. № 367. URL: https://zakon.rada.gov.ua/laws/show/367-2025-%D0%BF#Text (дата звернення: 08.12.2025).

26. Про Державну службу України з лікарських засобів та контролю

за наркотиками. *Державна служба України з лікарських засобів та контролю за наркотиками* : офіційний сайт. 2023. URL: https://surl.li/watuqj (дата звернення: 08.12.2025).

27. Жук О. М., Ліпенцев А. В. Інституційна спроможність центральних органів виконавчої влади України в умовах реформування. *Вісник НАДУ при Президентові України*. 2022. № 2. С. 34–42.

28. Кравченко С. О. Безперервність діяльності органів державної влади в умовах криз та надзвичайних ситуацій. *Публічне управління та адміністрування*. 2023. № 1. С. 66–74.

29. Система якості Держлікслужби. *Державна служба України з лікарських засобів та контролю за наркотиками* : офіційний сайт. URL: https://surl.li/unhlef (дата звернення: 08.12.2025).

30. Про організацію роботи підприємств, установ та організацій, що належать до сфери управління Міністерства охорони здоров'я України на період воєнного стану : Наказ МОЗ України від 05 трав. 2022 р. № 751. URL: https://moz.gov.ua/uk/decrees/nakaz-moz-ukraini-vid-05052022--751-pro-organizaciju-roboti-pidpriemstv-ustanov-ta-organizacij-scho-nalezhat-do-sferi-upravlinnja-ministerstva-ohoroni-zdorov%E2%80%99ja-ukraini-na-period-voennogo-stanu (дата звернення: 08.12.2025).

31. Ризик-орієнтований підхід до перевірок бізнесу. *Державна регуляторна служба України* : офіційний сайт. 2024. URL: https://drs.gov.ua/press-room/ryzyk-oriyentovanyj-pidhid-do-perevirok-biznesu/ (дата звернення: 08.12.2025).

32. Управління персоналом на державній службі. Оцінювання результатів службової діяльності : метод. рек. *Національне агентство України з питань державної служби*. 2024. URL: https://nads.gov.ua/diyalnist/upravlinnya-personalom-na-derzhavnij-sluzhbi/ocinyuvannya-rezultativ-sluzhbovoyi-diyalnosti/metodychni-rekomendatsii (дата звернення: 08.12.2025).

33. Білоус В. М. Ризик-орієнтований підхід у діяльності органів

державного нагляду та контролю. *Державне управління: удосконалення та розвиток.* 2021. № 4. DOI: 10.32702/2307-2156.2021.4.

34. Бугаїчук К. Л. Administrative-Legal Regulation of the Implementation of Risk-Oriented Access in the Security Sector of Ukraine. *Вісник ХНУВС*. 2025. № 2(109). URL: https://visnyk.univd.edu.ua/index.php/VNUAF/article/view/879/809 (дата звернення: 08.12.2025).

35. Ярмусь Д. В. Ризик-менеджмент в умовах воєнного стану: адаптація моделей управління. *Вісник Херсонського національного технічного університету*. 2025. № 2(93), ч. 1. С. 337–343. URL: https://journals.kntu.kherson.ua/index.php/visnyk_kntu/article/view/1010/973 (дата звернення: 08.12.2025).

36. Токмакова І. В., Чорнобровка І. В., Зуб М. В. Формування системи управління ризиками підприємств України в сучасних умовах. *Вісник економіки транспорту і промисловості*. 2024. № 85. С. 83–92.

37. Чорнодід І. С., Іващенко Т. О., Шолудченко С. В. Ризикоорієнтований підхід у системі сучасного менеджменту організацій. *Проблеми сучасних трансформацій. Серія : Економіка та управління*. 2023. № 7. URL: https://reicst.com.ua/pmt/article/view/2023-7-04-18/2023-7-04-18 (дата звернення: 08.12.2025).

38. ДСТУ EN ISO 22313:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Настанови щодо застосування ISO 22301 (EN ISO 22313:2020, IDT ; ISO 22313:2020, IDT). На заміну ДСТУ EN ISO 22313:2014 ; чинний від 01.09.2022. Київ : ДУкрНДНЦ, 2022. URL: https://zakon.isu.net.ua/sites/default/files/normdocs/dstu_en_iso_22313_2021_bezpeka_ta_stabilnist._sistemi_upravli.pdf (дата звернення: 08.12.2025).

39. Еггерс Г. Управління безперервністю бізнесу – система менеджменту стійкістю. *DQS Україна*. 2022. URL: https://www.dqsglobal.com/uk/doslidzhujte/blog/upravlinnya-bezperervnistyu-biznesu-%E2%80%93-sistema-menedzhmentu-stijkistyu (дата звернення:

10.12.2025).

40. ДСТУ ISO 22300:2020. Безпека і стійкість. Словник (ISO 22300:2018, IDT). Київ : УкрНДНЦ, 2021. 34 с.

41. Зборовська Т. В., Губін Ю. І., Благун О. Д. Оцінка ризиків, що впливають на безперервність діяльності фармацевтичних підприємств України. *Управління, економіка та забезпечення якості в фармації*. 2020. № 2(62). С. 38–44.

42. Зборовська Т. В. Обґрунтування актуальності впровадження стандарту ISO 22301 у фармацевтичному секторі України. *Управління, економіка та забезпечення якості в фармації*. 2017. № 2(50). С. 4–10.

43. Ситайло У. В. Безперервність бізнесу в Україні: виклики та можливості в умовах війни. *Економіка та суспільство*. 2024. № 62. URL: https://economyandsociety.in.ua/index.php/journal/article/view/3887 (дата звернення: 08.12.2025).

44. Олійник М. Інструментарій забезпечення безперервності бізнесу: управлінський аспект. *Acta Academiae Beregsasiensis. Economics*. 2025. № 10. P. 456–466. DOI: 10.58423/2786-6742/2025-10-456-466.

ДОДАТКИ

ДОДАТОК А


Міністерство охорони здоров'я України
Національний фармацевтичний університет
СЕРТИФІКАТ
Цим засвідчується, що
Проняєва К.В., Крутських Т.В.
Науковий керівник:
Зборовська Т.В.
брав(ла) участь у роботі VI Всеукраїнської науково-практичної конференції з міжнародною участю
YOUTH PHARMACY SCIENCE
Ректор НФаУ,
д. фарм. н., проф.
Олександр КУХТЕНКО
10-11 грудня 2025 р.
м. Харків
Україна

ДОДАТОК Б

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ГРАМОТА

нагороджується

ПРОНЯЄВА Катерина

у секційному засіданні студентського наукового товариства кафедри

менеджменту, маркетингу та забезпечення якості у фармації

VI Всеукраїнська науково-практична конференція з міжнародною участю

«YOUTH PHARMACY SCIENCE»

Ректор закладу вищої освіти **Олександр КУХТЕНКО**

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ Національний фармацевтичний університет №02010936

10-11 грудня 2025 р. м. Харків

ДОДАТОК В

МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

YOUTH PHARMACY SCIENCE

МАТЕРІАЛИ
VI ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

10-11 грудня 2025 року
м. Харків

Харків
НФаУ
2025

У результаті було сформульовано концептуальний підхід до удосконалення державної системи контролю, що ґрунтується на превентивному управлінні ризиками, стандартизації технологічних процесів та гармонізації національних вимог із європейськими стандартами GACP.

Висновки. Дослідження продемонструвало, що ефективне вирощування медичного канабісу в Україні можливе лише за умови створення комплексної та формалізованої системи державного контролю, яка забезпечує дотримання стандартів GACP. Ключовим висновком є встановлення того, що існуюча нормативно-правова база після легалізації медичного канабісу потребує доповнення спеціалізованими процедурами інспектування, моніторингу та сертифікації, які повинні бути чітко закріплені на рівні нормативно-правових актів підзаконного рівня.

Встановлено, що державний контроль має бути спрямований на перевірку трьох критично важливих блоків: походження та якість генетичного матеріалу, дотримання технологічних параметрів культивування та належну подальшу обробку рослинної сировини. Саме ці етапи найбільш суттєво впливають на стабільність хімічного складу канабіноїдів та безпечність кінцевої продукції. З'ясовано, що без систематичної державної перевірки цих параметрів неможливо гарантувати відповідність сировини вимогам фармакопейних стандартів та забезпечити подальшу відповідність процесів виробництва вимогам GMP.

Результати дослідження також підтвердили важливість функціонування централізованої державної системи простежуваності, яка забезпечить фіксацію всіх виробничих операцій – від вибору посадкового матеріалу до сушіння, стабілізації та зберігання рослинної сировини. Такі механізми підвищують прозорість виробництва, унеможливлюють незаконне використання сировини та забезпечують доказову базу для перевірки відповідності GACP.

Установлено, що результативність системи контролю значною мірою залежить від запровадження регулярних державних перевірок відповідності GACP, які мають супроводжуватися обов'язковим лабораторним тестуванням якісних показників рослинної сировини, включно з визначенням канабіноїдного профілю, мікробіологічної безпеки та залишкових кількостей потенційно небезпечних хімічних речовин. Водночас, доцільним є спрямування державної системи нагляду на узгодження з європейськими регуляторними практиками, а також використання принципу оцінки ризиків та уніфікованих методичних підходів для пріоритизації відповідних перевірок.

Отримані результати формують підґрунтя для розроблення та впровадження державної політики, спрямованої на побудову високотехнологічного та контрольованого сектору виробництва медичного канабісу відповідно до принципів якості, стандартизації та сертифікації.

ПРИНЦИПИ ЗАСТОСУВАННЯ РИЗИК-ОРІЄНТОВАНОГО МЕНЕДЖМЕНТУ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ДІЯЛЬНОСТІ ДЕРЖАВНОЇ УСТАНОВИ

Проняєва К.В., Крутських Т.В.
Науковий керівник: Зборовська Т.В.
Національний фармацевтичний університет, Харків, Україна
katiakobak1107@gmail.com

Вступ. У сучасних умовах функціонування державних органів, особливо у період воєнного стану, нестабільності постачання, кіберзагроз та постійних змін регуляторного середовища, питання забезпечення безперервності діяльності набуває критичної актуальності.

Будь-яке порушення їхньої роботи може призвести до збоїв у наданні послуг та здійсненні функції контролю, втрати або недоступності даних, порушення прав суб'єктів господарювання і, як наслідок, зниження довіри до державних інституцій. У таких умовах особливо важливо забезпечити безперервність діяльності, що можливе лише через реалізацію ризик-орієнтованого підходу на системній основі. Використання принципів ризик-менеджменту дозволяє своєчасно виявляти та зменшувати загрози різної природи, формувати ефективні протоколи швидкого реагування і створювати стійку інституційну інфраструктуру. Для органів, що відповідають за контроль лікарських засобів і обіг наркотичних речовин, безперервність роботи напряму впливає на безпеку пацієнтів, стабільність системи охорони здоров'я та національну безпеку.

Мета дослідження. Для наших досліджень ми використовували аналіз принципів ризик-орієнтованого підходу та визначили механізми їх застосування для забезпечення безперервності діяльності державної установи в умовах внутрішніх і зовнішніх загроз. Тому метою роботи є визначення шляху реалізації ризик-орієнтованого підходу в формуванні комплексу заходів з забезпечення безперервності діяльності Державної служби України з лікарських засобів та контролю за наркотиками (Держлікслужби).

Матеріали та методи. При виконанні дослідження застосовано: аналіз нормативно-правових документів, положень стандартів ДСТУ ISO 31000:2018 «Менеджмент ризиків. Принципи та настанови», ДСТУ EN ISO 22301:2021 «Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги», статистичних даних щодо впливів у діяльності державних установ.

Результати дослідження. Ризик-орієнтований підхід є одним із ключових інструментів, що дає можливість завчасно виявляти загрози, оцінювати їхній вплив та формувати дієві заходи з попередження та корегування їх руйнівної сили. Його застосування у Держлікслужбі забезпечує оперативність, надійність і стійкість у виконанні державних функцій, особливо з позиції безперервності роботи під час військового стану в країні. Ключові принципи ризик-орієнтованого менеджменту полягають у впровадженні комплексного підходу до аналізу загроз на всіх рівнях управління – стратегічному, тактичному й операційному. При цьому враховується структура служби, особливості роботи її територіальних підрозділів, а також взаємодія з іншими державними інституціями та учасниками фармацевтичного ринку.

Процес управління ризиками здійснюється безперервно і інтегрований у щоденну діяльність Держлікслужби, включаючи планування, моніторинг, контроль і проведення внутрішнього аудиту. Це дозволяє своєчасно виявляти зміни у зовнішньому середовищі та оперативно на них реагувати.

Пріоритет надається тим ризикам, що можуть найбільше вплинути на виконання критично важливих функцій служби, зокрема державного контролю якості лікарських засобів, ліцензування діяльності, контролю за обігом наркотичних засобів і прекурсорів, а також забезпечення стабільної роботи державних реєстрів та інформаційних систем.

Прийняття управлінських рішень базується на доказовості та аналітичних даних. Для оцінки ризиків використовуються результати лабораторних досліджень, статистика, дані моніторингу фармацевтичного ринку, інформація про інциденти у сфері кібербезпеки та інші достовірні джерела.

Важливим принципом є інклюзивність та чіткий розподіл відповідальності. До процесу ризик-менеджменту залучаються всі необхідні структурні підрозділи – експертні, IT,

юридичні, аналітичні – а також зовнішні партнери. Для кожного етапу визначаються відповідальні особи та механізми взаємодії.

Система управління ризиками має бути адаптивною, тобто здатною швидко перебудовуватися відповідно до нових викликів. Це особливо важливо в умовах військових загроз, порушень логістики, кіберзагроз, змін у законодавстві та епідеміологічних ризиків. Гнучкість системи дозволяє забезпечувати безперервність діяльності навіть у кризових ситуаціях.

Результати дослідження показали, що ефективне забезпечення безперервності діяльності можливе лише за умови ідентифікації та оцінки всіх потенційних загроз і формування стратегії швидкого реагування на інциденти, яку інтегровано в управлінські процеси державної установи.

Нами проведено аналіз та встановлено наступну структуру ризиків, притаманних державним установам наведених в таблиці 1.

Оцінка цих ризиків дає змогу сформувати реалістичний профіль загроз та дає змогу сформувати пріоритетні зони уваги у реалізації заходів захисту від них.

Таблиця 1. Групи ризиків безперервності діяльності

Структура ризиків	Фактори впливу
Операційні ризики	Відмова обладнання, перебої в IT-інфраструктурі, затримки у документообігу
Кадрові ризики	Відсутність критично важливих спеціалістів, плинність кадрів, збої в комунікаціях
Інфраструктурні та енергетичні ризики	Відключення електропостачання, аварії інженерних та комунікаційних мереж
Ризики фізичної та кібербезпеки	Кібератаки, несанкціонований доступ, пошкодження майна
Законодавчо-регуляторні ризики	Ризики, пов'язані з частими змінами норм та процедур.

Для кожного ризику було визначено його ймовірність виявлення та настання, критичність наслідків, проведено ранжування рівня тяжкості впливу на діяльність, визначено можливості зниження руйнівної дії. Аналіз засвідчив, що найбільш небезпечними є ризики, пов'язані з інформаційними системами: навіть короткочасне їх вимкнення призводить до порушення доступу до реєстрів, електронних документів і сервісів для суб'єктів господарювання.

Держлікслужба має забезпечити реалізацію культури ризиків безперервності діяльності, яку можна реалізувати за рахунок наступних кроків:

- регулярне навчання персоналу з питань виконання протоколів швидкого реагування на інциденти відносно кожної групи ризиків;
- залучення працівників до процесів ідентифікації та оцінювання потенційних загроз та наслідків відмов в роботі кожного департаменту;
- підготовку до реагування на інциденти через тренування, симуляції, аудит готовності на постійній основі;
- безперервне удосконалення процедур після кожного інциденту або тренування для вдосконалення як процедур так і раціонального використання ресурсних складових реалізації планів реагування.

Висновки. Застосування ризик-орієнтованого підходу сприяє підвищенню ефективності управління державною установою, а саме: скороченню простоїв, покращенню якості процесів в департаментах, зменшенню витрат на усунення наслідків інцидентів та підвищенню довіри суб'єктів господарювання фармацевтичного сектору. Він дозволяє своєчасно ідентифікувати загрози, оцінити їх наслідки та сформувати ефективні механізми реагування. Розробка та впровадження плану безперервності діяльності, побудова культури управління ризиками, удосконалення процесів взаємодії та комунікації є необхідними умовами стійкого функціонування в сучасних умовах.

НАУКОВО-ПРАКТИЧНІ ПІДХОДИ ЩОДО РОЗРОБКИ СИСТЕМИ ІННОВАЦІЙНОГО УПРАВЛІННЯ В ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я

Пузирьов Д.А.
Науковий керівник: Літвінова О.В.
Національний фармацевтичний університет, Харків, Україна
mrpuzyrevd@ukr.net

Вступ. Сучасний сектор охорони здоров'я стикається з викликами, які зумовлені старінням населення, технологічними змінами та обмеженням фінансування. Інновації стають критичним фактором адаптації медичних закладів до змін, проте їх впровадження залишається складним процесом. Стратегічне управління інноваціями є необхідною передумовою підвищення якості медичної допомоги та оптимізації використання ресурсів.

Мета дослідження. Аналіз та систематизація науково-практичних підходів щодо розробки системи інноваційного управління в закладах охорони здоров'я.

Матеріали та методи. Дослідження проводилося з використанням систематичного аналізу наукових публікацій у наукометричних базах даних.

Результати дослідження. Систематичний аналіз літературних джерел показав, що ефективне інноваційне управління в закладах охорони здоров'я формується на основі поєднання кількох взаємопов'язаних підходів, які забезпечують узгодженість стратегічних, організаційних та людських аспектів управління. Одним із ключових напрямів є організаційний підхід, що передбачає побудову гнучкої структури управління, здатної швидко адаптуватися до змін зовнішнього середовища, оптимізувати процеси прийняття рішень та інтегрувати інновації у повсякденну діяльність. Гнучкість організаційної структури, відкритість комунікацій та прозорість управлінських процесів створюють передумови для ефективного впровадження нових технологій і методів лікування, а також підвищують загальний рівень управлінської ефективності.

Водночас культурний підхід відіграє важливу роль у формуванні інноваційного середовища. Він передбачає розвиток організаційної культури, орієнтованої на навчання, обмін досвідом, довіру та підтримку ініціативності. Така культура створює психологічну безпеку для персоналу, стимулює колективну творчість і сприяє трансформації закладу охорони здоров'я в динамічну, навчальну організацію. Практика показує, що саме культура відкритості до нового визначає, наскільки швидко інновації переходять із теоретичного рівня до практичної реалізації.

Не менш суттєвим є лідерський підхід, який підкреслює значення стратегічного бачення керівництва, його здатності мотивувати персонал і підтримувати інноваційні

ДОДАТОК Г

Політика управління ризиками безперервності діяльності Державної служби України з лікарських засобів та контролю за наркотиками

1. Сфера застосування

Цей документ встановлює єдині підходи, принципи, цілі, та загальні вимоги до організації, функціонування та постійного вдосконалення системи управління безперервністю бізнесу Державної служби України з лікарських засобів та контролю за наркотиками (далі – Держлікслужба).

Політика управління безперервністю діяльністю (скорочено – Політика) поширюється на всі процеси та діяльність всіх працівників Держлікслужби, зокрема, що мають вплив на якість надання державних послуг щодо обігу лікарських засобів, екологічну та енергетичну безпеку, охорону праці, охорону здоров'я, фізичний захист, інформаційну безпеку, соціально-економічні фактори, доброчесність тощо.

Політика направлена на забезпечення безперервності діяльності, збільшення ефективності діяльності підприємства шляхом зниження негативного впливу факторів ризику, а також підвищення швидкості реагування на виникаючі ризикові ситуації та надзвичайні події.

Політика є невід'ємною частиною системи управління якістю та спрямована на забезпечення відповідності вимогам ДСТУ ISO 9001:2015, ДСТУ ISO 31000:2018, ДСТУ EN ISO 22301:2021.

Політика та нормативні документи Держлікслужби узгоджуються між собою та не суперечать один одному.

Головною метою Політики є: створення ефективної системи управління безперервністю діяльності, яка забезпечує впевненість у досягненні стратегічних цілей Держлікслужби при дотриманні високих стандартів безпеки та національного законодавства в випадках порушення роботи в надзвичайних ситуаціях, які можуть приводити до повної зупинки виконання регуляторних функцій державним органом.

Організація чіткого процесу з ефективного управління безперервністю діяльності сприяє досягненню стратегічних цілей Держлікслужбою шляхом своєчасної та повної ідентифікації, проведення оцінки ризиків, забезпечення їх всебічного аналізу, розробкою заходів з мінімізації їх впливу, дотриманням і контролем за прийняттям відповідного рівня ризику та формуванням інструкцій щодо реагування і відновлення після його реалізації.

Управління ризиками безперервності діяльності є невід'ємною складовою ефективного кризового управління, процесів планування заходів безпеки та прийняття рішень в кризових ситуаціях, відповідно управління ризиками інтегровано в усі процеси Держлікслужби та сприяє підвищенню дієвості та стійкості функціонування системи управління діяльністю (якістю).

Політика є обов'язковою для виконання всіма працівниками Держлікслужби.

2. Культура управління ризиками

Культура управління ризиками є складовою загальної корпоративної культури Держлікслужби та сприяє формуванню достатнього рівня обізнаності всіх працівників щодо важливості та правил функціонування системи управління ризиками. Розвиток культури управління ризиками здійснюється шляхом проведення навчань, виробничих нарад, тематичних зустрічей з метою популяризації процесу управління ризиками та максимальної залученості працівників до цього процесу. Культура управління ризиками в Держлікслужбі сприяє підвищенню обізнаності працівників щодо:

– важливості управління ризиками;

– функціонування системи управління ризиками. Розвиток культури управління ризиками досягається через: навчальні програми;

– обговорення на нарадах;

– ініціативи із залученням працівників.

Мета впровадження культури ризиків полягає в тому, щоб керівництво і працівники Держлікслужби приймали рішення та здійснювали операційну

діяльність, обираючи оптимальне співвідношення ризиків і можливостей, зокрема: відмову від рішень, що призводять до невиправдано високих ризиків;

– вжиття заходів для зменшення впливу ризиків;

– усвідомлення важливості управління ризиками на всіх рівнях.

Держлікслужба забезпечує впровадження норм, визначених В Антикорупційній програмі, зокрема в частині оцінки корупційних ризиків у всіх процесах діяльності Держлікслужби.

3. Цілі і завдання політики з управління ризиками Основними цілями Політики є:

– створення ефективної системи та структури управління і контролю за ризиками, розвитку можливостей, що включає ідентифікацію (виявлення), аналіз, оцінку, обробку, розробку заходів, контроль та моніторинг, звітування і подальший контроль заходів, що сприятиме керівництву Держлікслужби, керівникам структурних підрозділів в досягненні стратегічних цілей Держлікслужби, підвищенню ефективності управління;

– забезпечення цілісності, повноти та достовірності інформації щодо управління ризиками, яка використовується для ухвалення управлінських рішень; створення інформаційних потоків як за вертикаллю, так і за горизонталлю організаційної структури Держлікслужби; забезпечення керівництва та зацікавлених сторін достовірною звітністю;

– впровадження та формалізація уніфікованих підходів до управління ризиками в Держлікслужбі з метою обмеження негативних наслідків, ефективного використання ресурсів та оптимізації процесів; сприяння безперервності операційної діяльності Держлікслужби;

– забезпечення ефективного розподілу ресурсів на основі рейтингу впливу ризику та схильності до ризику; впровадження практики управління ризиками в ділову культуру Держлікслужби;

– сприяння сталому розвитку Держлікслужби шляхом створення та захисту цінностей через ефективне управління ризиками та можливостями;

– забезпечення зростання довіри зацікавлених сторін за рахунок створення прозорої системи управління ризиками та можливостями та ефективності її впровадження;

– забезпечення ефективного визначення та врахування ризиків і можливостей, які можуть впливати на відповідність продукції, а також на здатність підвищувати задоволеність замовника;

– забезпечення повного дотримання вимог законодавства України (включаючи податкове та антикорупційне), міжнародних стандартів безпеки, зовнішніх та внутрішніх нормативних документів. Держлікслужба визнає, що управління ризиками є невід'ємною частиною належного управління, системи менеджменту якості та ключовим елементом прийняття рішень.

Система управління ризиками інтегрована в загальну систему управління та спрямована на забезпечення стабільності діяльності, захист персоналу, населення, безперервності діяльності, енергетичної стійкості, інформаційної безпеки та навколишнього середовища від екологічних ризиків, а також забезпечення ефективного використання державного майна та коштів.

Ключові завдання:

Безпека – забезпечення мінімізації або усунення ризиків, пов'язаних із військовою небезпекою, зокрема запобігання аваріям, несанкціонованому доступу до процесів, витокам інформації та забрудненню навколишнього середовища.

Комплаєнс – забезпечення повного дотримання вимог законодавства України (включаючи податкове та антикорупційне), міжнародних стандартів безпеки та внутрішніх нормативних документів.

Ефективність – оптимізація використання ресурсів шляхом пріоритезації заходів контролю та запобігання фінансовим втратам.

Якість – підтримка високої якості продукції та послуг відповідно до вимог системи менеджменту якості.

4. Порядок та принципи управління ризиками Управління ризиками здійснюється відповідно до принципів ДСТУ ISO 31000:2018 та деталізується у внутрішньому документі Держлікслужби – Положенні про управління ризиками. Яке установлює порядок ідентифікації ризиків, аналізу їх оброблення в рамках системи менеджменту якості (далі – СУЯ), а також порядок роботи комісії з управління ризиками. Загальні принципи управління ризиками:

Інтегрованість – управління ризиками є невід'ємною частиною всіх процесів Держлікслужби.

Структурованість та комплексність – застосування послідовного та всеохоплюючого підходу забезпечує стабільні, зіставні та надійні результати.

Адаптивність – система управління ризиками динамічна та реагує на зміни зовнішнього та внутрішнього середовища (зміни в законодавстві, технологіях, ринкових умовах тощо).

5. Процес управління ризиками (цикл) Процес управління ризиками – це систематичний процес, що включає ідентифікацію, аналіз, оцінку, обробку, моніторинг та перегляд потенційних загроз, які можуть вплинути на фінансово-господарські , організаційно-управлінські цілі Держлікслужби.

Управління ризиками сприяє досягненню цілей і поліпшенню діяльності Держлікслужби, зокрема запобігання та протидії корупції, забезпеченню відповідності діяльністю Держлікслужби законодавчим й іншим обов'язковим вимогам, захисту інформації, навколишнього середовища, ефективності та результативності управління проєктами, оптимізації функцій структурних підрозділів і посадових осіб, забезпечення високої репутації Держлікслужби. Найвище керівництво Держлікслужби сприяє використання процесного підходу та ризик-орієнтованого мислення.

Основні процеси управління ризиками:

Ідентифікація ризиків – систематичний процес пошуку, розпізнавання та опису ризиків. Включає аналіз потенційних небезпек, пов'язаних із нормативною діяльністю як виконавчого органу, фінансовою діяльністю, дотриманням законодавства тощо а також аналіз ризиків, пов'язаних з виконанням функцій регулятора та діяльністю зовнішніх стейкхолдерів, з метою забезпечення якості виконання функцій регулятора в галузі.

Аналіз та оцінка ризиків – використання методології, для визначення рівня ризику (ймовірність та вплив).

Встановлення пріоритетів ризиків. Розробка заходів реагування на ризики – розробка та впровадження заходів контролю для:

– уникнення ризику;

– зменшення ризику (впровадження додаткових технічних, організаційних засобів безпеки, посилення контролю діяльності, тощо);

– передавання ризику (страхування, аутсорсинг);

– прийняття ризику (свідоме рішення, якщо ризик знаходиться в межах можливості виконання функцій).

Моніторинг та перегляд – регулярний контроль за ефективністю впроваджених заходів та змінами у профілі ризиків Держлікслужби, аналіз результативності дій, виконаних щодо ризиків і можливостей. Аналіз та оцінка системи управління ризиками – ефективність системи управління ризиками Держлікслужби підлягає регулярному моніторингу та оцінці. Внутрішній аудит проводить планові та позапланові перевірки дотримання процедур, встановлених цією Політикою.

Керівництво Держлікслужби проводить аналіз системи управління ризиками (в рамках аналізу СУЯ з боку керівництва) не рідше одного разу на рік для забезпечення її постійної придатності, адекватності та ефективності. Результати аналізу системи управління ризиками є підставою для ініціювання коригувальних та запобіжних дій відповідно до Положення про невідповідності та коригувальні дії.

Зобов'язання керівництва: забезпечити необхідні ресурси (людські, фінансові, технічні) для ефективного функціонування системи управління ризиками; демонструвати лідерство та прихильність до культури управління ризиками; забезпечити відповідність діяльності Держлікслужби законодавству. Зобов'язання працівників: дотримуватися вимог цієї Політики та інших внутрішніх документів, що регулюють процес управління ризиками; повідомляти свого безпосереднього керівника або відповідальну особу про виявлені ризики, інциденти або потенційні небезпеки, в порядку, визначеному процедурою; інформувати про виявлені невідповідності у порядку, встановленому в процедурі.

Всі записи, що стосуються системи управління ризиками (реєстри ризиків, протоколи, звіти, записи про коригувальні дії, результати аудитів, протоколи аналізу керівництва), є документацією СУЯ. Записи, що документують результативність дій, виконаних щодо ризиків і можливостей, зберігаються та підлягають аналізуванню згідно з аналітичною документацією, забезпечуючи підтвердження вимогам ДСТУ ISO 9001:2015.

ДОДАТОК Д

План безперервності діяльності (BCP) Державної служби України з лікарських засобів та контролю за наркотиками

1. Загальні положення

План безперервності діяльності Держлікслужби (далі – План) визначає комплекс організаційних, управлінських і технічних заходів, спрямованих на забезпечення безперервного виконання критично важливих функцій служби у разі виникнення кризових ситуацій, надзвичайних подій або реалізації значущих ризиків.

План розроблено з урахуванням вимог стандартів ISO 31000:2018 «Risk Management» та ISO 22301:2019 «Business Continuity Management Systems», а також специфіки діяльності центрального органу виконавчої влади у сфері державного контролю якості, безпеки та обігу лікарських засобів.

2. Мета та завдання Плану

Мета Плану – забезпечення стійкості та безперервності діяльності Держлікслужби, мінімізація негативного впливу кризових подій на здоров’я населення, фармацевтичний ринок та систему державного управління.

Основні завдання:

– збереження виконання критично важливих регуляторних і контрольних функцій;

– мінімізація часу простою підрозділів;

– зниження фінансових, репутаційних та соціальних втрат;

– забезпечення готовності персоналу до дій у кризових умовах;

– підвищення рівня довіри з боку суспільства та міжнародних партнерів.

3. Сфера застосування Плану

План поширюється на:

– центральний апарат Держлікслужби;

– територіальні органи;

– підпорядковані лабораторії та установи;

– інформаційні системи та реєстри;

– процеси взаємодії з МОЗ, митними органами, правоохоронними структурами та міжнародними організаціями.

4. Ідентифікація критично важливих функцій

До критично важливих функцій Держлікслужби належать:

– державний контроль якості лікарських засобів;

– ліцензування діяльності з виробництва, імпорту, оптової та роздрібної торгівлі;

– контроль обігу наркотичних, психотропних речовин і прекурсорів;

– реагування на виявлення неякісних та фальсифікованих лікарських засобів;

– ведення державних реєстрів і інформаційних баз;

– міжвідомча та міжнародна координація у сфері фармацевтичної безпеки.

5. Аналіз впливу на діяльність (Business Impact Analysis, BIA)

BIA передбачає оцінювання:

– допустимого часу переривання кожної функції (MTPD);

– критичності наслідків для здоров’я населення;

– впливу на виконання державних зобов’язань;

– правових і репутаційних ризиків.

На основі BIA встановлюються пріоритети відновлення функцій:

– Контроль якості та безпеки лікарських засобів.

– Регулювання обігу наркотичних засобів.

– Ліцензування та дозвільні процедури.

– Інформаційно-аналітичне забезпечення.

– Адміністративно-управлінські функції.

6. Основні сценарії кризових ситуацій

План враховує такі сценарії:

– воєнні дії або терористичні загрози;
– техногенні аварії та пожежі;
– кібератаки та відмова ІТ-систем;
– пандемії та біологічні загрози;
– втрату доступу до приміщень або інфраструктури;
– критичний дефіцит персоналу.

7. Заходи забезпечення безперервності діяльності

7.1 Організаційні заходи

– створення кризового штабу;
– визначення заступників на ключові посади;
– чіткий розподіл повноважень у кризовий період;
– використання спрощених процедур ухвалення рішень.

7.2 Кадрові заходи

– формування кадрового резерву;
– перехресне навчання персоналу;
– дистанційні формати роботи;
– психологічна підтримка працівників.

7.3 Інформаційно-технічні заходи

– резервне копіювання даних;
– альтернативні канали зв’язку;
– захист критичних ІТ-систем;
– доступ до реєстрів з резервних майданчиків.

7.4 Операційні заходи

– резервні локації для роботи підрозділів;
– перерозподіл функцій між територіальними органами;
– пріоритетне обслуговування критичних процесів;
– залучення міжнародної технічної допомоги.

8. План реагування та відновлення

План реагування включає:

– порядок активації BCP;

– інформування керівництва та персоналу;

– взаємодію з МОЗ, ДСНС, правоохоронними органами;

– зовнішні комунікації з громадськістю та ЗМІ.

План відновлення визначає:

– поетапне повернення до штатного режиму;

– оцінювання збитків;

– коригування процедур;

– оновлення реєстрів і баз даних.

9. Комунікації та управління інформацією

Комунікаційна політика передбачає:

– централізоване інформування;

– прозорість рішень;

– запобігання дезінформації;

– координацію з міжнародними партнерами та регуляторами.

10. Тестування, моніторинг і вдосконалення Плану

План підлягає:

регулярному тестуванню (навчання, тренування, симуляції);

щорічному перегляду;

актуалізації з урахуванням змін ризиків;

інтеграції з системою управління ризиками.

11. Висновок

Запровадження Плану безперервності діяльності Держлікслужби є необхідною умовою забезпечення стабільного функціонування системи державного контролю у сфері обігу лікарських засобів. Інтеграція BCM з ризик-орієнтованим менеджментом дозволяє службі діяти проактивно, знижувати негативний вплив кризових подій і гарантувати захист здоров’я населення навіть в умовах підвищеної невизначеності.

ДОДАТОК Е

ПРОЄКТ НАКАЗУ

ДЕРЖАВНА СЛУЖБА УКРАЇНИ З ЛІКАРСЬКИХ ЗАСОБІВ ТА КОНТРОЛЮ ЗА НАРКОТИКАМИ

НАКАЗ

м. Київ

№ ___

від «» _____ 20__ р.

Про затвердження Положення про систему безперервності діяльності Державної служби України з лікарських засобів та контролю за наркотиками.

З метою забезпечення стійкого та безперервного виконання Державною службою України з лікарських засобів та контролю за наркотиками покладених на неї функцій у разі виникнення кризових ситуацій, надзвичайних подій, воєнних загроз, техногенних аварій або інших факторів ризику, відповідно до принципів ризик-орієнтованого менеджменту, стандартів ISO 31000:2018 та ISO 22301:2019,

НАКАЗУЮ:

Затвердити Положення про систему безперервності діяльності Державної служби України з лікарських засобів та контролю за наркотиками (додається).

Керівникам структурних підрозділів та територіальних органів забезпечити впровадження вимог Положення у межах повноважень.

Визначити відповідальними за координацію системи безперервності діяльності:

– керівника апарату Держлікслужби;
– керівників відповідних структурних підрозділів.

Забезпечити щорічний перегляд та актуалізацію Плану безперервності діяльності з урахуванням змін ризиків.

Контроль за виконанням цього наказу залишаю за собою.

Голова Держлікслужби _____

ДОДАТОК Ж

ПОЛОЖЕННЯ

про систему безперервності діяльності

Державної служби України з лікарських засобів

та контролю за наркотиками

1. Загальні положення

1.1. Це Положення визначає організаційні та методологічні засади функціонування системи безперервності діяльності (Business Continuity Management, BCM) Держлікслужби.

1.2. Система BCM є складовою ризик-орієнтованого менеджменту та інтегрується у загальну систему управління.

1.3. Дія Положення поширюється на центральний апарат, територіальні органи, підпорядковані установи та інформаційні системи.

2. Мета і завдання

Метою BCM є забезпечення:

– безперервності критично важливих функцій;
– мінімізації негативного впливу кризових подій;
– захисту життя і здоров’я населення;
– виконання міжнародних та національних зобов’язань.

3. Основні принципи

– проактивність;
– системність;
– пріоритетність критичних функцій;
– відповідальність;
– постійне вдосконалення.

4. Критично важливі функції

До критично важливих функцій належать:

– державний контроль якості лікарських засобів;
– контроль обігу наркотичних і психотропних речовин;

– ліцензування фармацевтичної діяльності;

– ведення державних реєстрів;

– міжвідомча координація у кризових умовах.

5. Активація та реалізація BCM

5.1. Рішення про активацію BCM приймається керівництвом Держлікслужби.

5.2. Створюється кризовий штаб.

5.3. Застосовуються визначені плани реагування та відновлення.

6. Моніторинг і перегляд

BCM підлягає:

– регулярному тестуванню;

– аналізу ефективності;

– коригуванню на основі нових ризиків.

Додаток 1

Матриця RACI системи безперервності діяльності Держлікслужби

Процес / Функція	**Керівництво**	**Кризовий штаб**	**IT-підрозділ**	**Юридичний**	**Територіальні органи**
Ідентифікація ризиків	A	R	C	C	I
BIA-аналіз	A	R	C	C	I
Активація BCM	A	R	I	I	I
Реагування на інцидент	C	R	R	C	R
Відновлення діяльності	A	R	R	C	R
Інформування громадськості	A	C	I	R	I

A – Accountable, R – Responsible, C – Consulted, I – Informed

Додаток 2

BIA-таблиця (аналіз впливу на діяльність)

Функція	**Потенційні наслідки зупинки**	**MTPD**	**Пріоритет**	**Ключові ресурси**
Контроль якості ЛЗ	Загроза здоров'ю населення	24 год	Критичний	Лабораторії, фахівці
Контроль обігу наркотиків	Порушення безпеки	48 год	Критичний	Реєстри, ІТ
Ліцензування	Затримка ринку	5 діб	Високий	Персонал
Інформаційні реєстри	Втрата даних	12 год	Критичний	Сервери
Адміністративні функції	Зниження ефективності	10 діб	Середній	Документообіг

Додаток 3

Чек-лист реагування на кризову ситуацію

1. Активація

- ☐ Ідентифіковано інцидент
- ☐ Повідомлено керівництво
- ☐ Активовано BCM

2. Управління

- ☐ Створено кризовий штаб
- ☐ Визначено відповідальних
- ☐ Задіяно резервні ресурси

3. Комунікація

- ☐ Повідомлено персонал
- ☐ Поінформовано МОЗ / КМУ
- ☐ Підготовлено публічну позицію

4. Відновлення

- ☐ Оцінено збитки
- ☐ Відновлено IT-системи

- ☐ Повернення до штатної роботи

Запровадження формалізованої системи ВСМ у Держлікслужбі забезпечує інституційну стійкість, відповідність міжнародним стандартам та здатність держави гарантувати фармацевтичну безпеку навіть у кризових умовах.

Додаток 4

Ризик-реєстр Державної служби України з лікарських засобів

та контролю за наркотиками

Ризик-реєстр є систематизованим переліком ідентифікованих ризиків, що можуть впливати на виконання функцій Держлікслужби, із визначенням їх характеристик, рівня пріоритетності та заходів реагування.

Таблиця 1. Ризик-реєстр Держлікслужби

№	Опис ризику	Джерело	Сфера впливу	Ймовірність	Вплив	Рівень ризику	Ключові наслідки	Заходи управління (ВСМ)
1	Переривання роботи лабораторій контролю якості	Воєнні дії, аварії	Операційна	Висока	Критичний	**Високий**	Загроза здоров'ю населення	Резервні лабораторії, релокація, альтернативні маршрути
2	Втрата доступу до держреєстрів	Кібератаки, збої ІТ	Інформаційна	Висока	Критичний	**Високий**	Зупинка ліцензування, контролю	Резервне копіювання, DRP, хмарні рішення
3	Нестача кваліфікованого персоналу	Міграція, мобілізація	Кадрова	Середня	Значний	**Середній**	Зниження якості контролю	Крос-функціональне навчання, резерв кадрів

4	Порушення ланцюгів постачання ЛЗ	Логістичні обмеження	Зовнішня	Середня	Значний	**Середній**	Дефіцит препаратів	Моніторинг постачальників, альтернативні канали
5	Невиконання регуляторних функцій	НС, зупинка установ	Правова	Низька	Критичний	**Середній**	Правові наслідки	Делегування, дистанційні процедури
6	Репутаційні втрати	Дезінформація, кризи	Репутаційна	Середня	Значний	**Середній**	Втрата довіри	План кризових комунікацій
7	Фінансові обмеження	Скорочення бюджету	Фінансова	Середня	Помірний	**Низький**	Обмеження програм	Пріоритизація критичних функцій
8	Збої взаємодії з МОЗ та КМУ	Комунікаційні збої	Управлінська	Низька	Значний	**Низький**	Затримка рішень	Регламент взаємодії, контактні групи

Додаток 5

Карта ризиків Держлікслужби

Карта ризиків відображає співвідношення **ймовірності реалізації ризику** та **масштабу його впливу** на діяльність служби і використовується для пріоритизації управлінських рішень.

Таблиця 2. Матриця ризиків (Risk Map)

Вплив \ Ймовірність	**Низька**	**Середня**	**Висока**
Критичний	🟠	🔴	🔴
Значний	🟡	🟠	🔴
Помірний	🟢	🟡	🟠

Умовні позначення:

- 🟢 – прийнятний ризик (моніторинг);
- 🟡 – контрольований ризик (управління);
- 🟠 – значний ризик (плани реагування);
- 🔴 – критичний ризик (BCM, негайні дії).

Розміщення ключових ризиків на карті

- 🔴 **Критична зона**:
  - втрата IT-реєстрів;
  - зупинка лабораторій;
  - масштабні кібератаки.
- 🟠 **Зона підвищеної уваги**:
  - кадрові ризики;
  - порушення логістики;
  - репутаційні загрози.
- 🟡 **Контрольована зона**:
  - фінансові ризики;
  - організаційні затримки.

Ризик-реєстр і карта ризиків Держлікслужби свідчать, що найвищу загрозу безперервності діяльності становлять операційні та інформаційні ризики, пов’язані з воєнними діями та кіберзагрозами. Саме ці ризики мають бути пріоритетними для впровадження BCM-планів, резервування ресурсів і сценарного планування.

Інтеграція ризик-реєстру з BIA та планами безперервності діяльності дозволяє:

- підвищити готовність до криз;
- мінімізувати втрати;
- забезпечити фармацевтичну безпеку держави.

1. Графічна карта ризиків Держлікслужби

Таблиця 3

Матриця «Імовірність – Вплив» для Держлікслужби

Імовірність \ Вплив	1 Незначний	2 Малий	3 Середній	4 Високий	5 Критичний
5 Дуже висока	🟡	🟠	🔴 Повітряні тривоги	🔴 Порушення регуляторних процесів	🔴 Воєнні загрози
4 Висока	🟡	🟠	🟠 Кадровий дефіцит	🔴 Відмова IT-систем	🔴 Зупинка регуляторної діяльності
3 Середня	🟢	🟡	🟠 Затримка управлінських рішень	🟠 Кібератака	🔴 Втрата даних
2 Низька	🟢	🟡	🟡	🟠 Пожежа	🟠
1 Дуже низька	🟢	🟢	🟡	🟡	🟠

Ключові ризики безперервності діяльності Держлікслужби

Ризик	Імовірність (P)	Вплив (I)	Рівень ризику
Воєнні дії, повітряні тривоги	5	5	🔴 Критичний
Відключення електроенергії	4	4	🔴 Критичний
Кібератака на державні IT-системи	3	5	🔴 Критичний
Недоступність ключових посадових осіб	4	4	🔴 Критичний
Втрата або компрометація даних	3	5	🔴 Критичний
Зрив виконання регуляторних функцій	4	5	🔴 Критичний
Кадровий дефіцит / мобілізація	4	3	🟠 Високий
Порушення взаємодії з лабораторіями	3	4	🟠 Високий
Затримка нормативних рішень	3	3	🟠 Високий
Репутаційні ризики	2	4	🟠 Високий

Карта ризиків побудована за двовимірною моделлю, де по осі абсцис відображено ймовірність реалізації ризиків, а по осі ординат – масштаб їх впливу на безперервність діяльності та виконання регуляторних функцій Держлікслужби.

У межах карти виділено чотири зони ризику:

Зелена зона (прийнятні ризики) – ризики з низькою ймовірністю та помірним впливом, що не потребують негайного реагування та підлягають періодичному моніторингу (фінансові та окремі управлінські ризики).

Жовта зона (контрольовані ризики) – ризики середньої ймовірності та впливу, що вимагають планових управлінських заходів (кадрові та організаційні ризики).

Помаранчева зона (значні ризики) – ризики, які можуть істотно вплинути на діяльність служби й потребують розроблення планів реагування (логістичні та репутаційні ризики).

Червона зона (критичні ризики) – ризики з високою ймовірністю та критичним впливом, реалізація яких може призвести до повного або часткового припинення виконання ключових функцій Держлікслужби (зупинка лабораторій, втрата ІТ-систем, кібератаки, воєнні загрози).

Карта ризиків використовується як інструмент пріоритизації заходів BCM, розподілу ресурсів і визначення критичних процесів для аналізу впливу на діяльність (BIA).

2. Зв’язок ризик-реєстру з BIA

Таблиця 4

Відповідність ключових ризиків критичним процесам Держлікслужби (BIA)

№	Ризик	Критичний процес (BIA)	Максимально допустимий час простою (MTPD)	Власник процесу	BCM-реагування
1	Зупинка лабораторій	Контроль якості лікарських засобів	24–48 год	Департамент контролю якості	Резервні лабораторії, релокація
2	Втрата ІТ-реєстрів	Ліцензування та реєстрація ЛЗ	12–24 год	ІТ-підрозділ	DRP, резервне копіювання
3	Кадровий дефіцит	Інспекційна діяльність	72 год	Кадрова служба	Перерозподіл функцій
4	Логістичні збої	Контроль обігу ЛЗ	48–72 год	Операційний підрозділ	Альтернативні канали
5	Репутаційні загрози	Комунікація з МОЗ та громадськістю	24 год	Пресслужба	План кризових комунікацій
6	Правові обмеження	Регуляторні рішення	72 год	Юридичний департамент	Делегування повноважень

BIA дозволяє чітко визначити, які ризики безпосередньо загрожують критичним процесам, та забезпечує обґрунтованість рішень щодо пріоритетності впровадження заходів BCM.

3. Підрозділ

Оцінка зрілості BCM Держлікслужби здійснювалася на основі п’ятирівневої моделі зрілості, що відповідає підходам ISO 22301:2019 та практиці публічного управління. Рівні зрілості BCM

1. Початковий (Initial) – реагування ad hoc, відсутність системності.
2. Повторюваний (Repeatable) – окремі регламентовані дії.
3. Визначений (Defined) – формалізовані політики та плани BCM.
4. Керований (Managed) – системний моніторинг і тестування.
5. Оптимізований (Optimized) – інтеграція BCM у стратегічне управління.

Таблиця 5

Оцінка зрілості BCM Держлікслужби

Компонент BCM	**Рівень зрілості**	**Коментар**
Ідентифікація ризиків	3	Використовується ризик-орієнтований підхід
Аналіз впливу (BIA)	2–3	Застосовується фрагментарно
Плани безперервності	2	Потребують уніфікації
Навчання персоналу	2	Нерегулярне
Тестування планів	1–2	Обмежене
Інтеграція в управління	2	Часткова

Станом на сьогодні система BCM Держлікслужби перебуває на перехідному етапі від рівня «повторюваний» до «визначений». Наявні окремі елементи ризик-орієнтованого управління та реагування на надзвичайні ситуації, однак вони потребують:

- формалізації в єдину систему BCM;
- регулярного проведення BIA;
- навчання персоналу;
- інтеграції BCM у стратегічне та оперативне управління.

Подальший розвиток BCM дозволить підвищити організаційну стійкість Держлікслужби, забезпечити безперервність фармацевтичного регулювання та відповідність міжнародним стандартам.