

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

КВАЛІФІКАЦІЙНА РОБОТА

на тему: РОЗРОБКА ПЛАНІВ ЗАБЕЗПЕЧЕННЯ
БЕЗПЕРЕРВНОСТІ БІЗНЕСУ ДЛЯ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ З
КОНТРОЛЮ ЯКОСТІ ЛІКАРСЬКИХ ЗАСОБІВ

Виконала:

здобувачка вищої освіти
2 курсу, групи 1
спеціальності 073 Менеджмент
освітньої програми
Якість, стандартизація та
сертифікація
Інна ТКАЧУК

Керівник:

професор закладу вищої освіти
кафедри
менеджменту, маркетингу та
забезпечення якості у фармації,
д. фармац. наук, професор
Тетяна КРУТСЬКИХ

Рецензент:

доцент ЗВО кафедри аналітичної
хімії, хімічного факультету
Київського національного
університету імені Тараса
Шевченка, к. хім. наук, доцент
Тетяна КЕДА

АНОТАЦІЯ

Розробка та впровадження плану безперервності бізнесу дає можливість лабораторії з контролю якості встановити критичність своїх бізнес-процесів та пропрацювати алгоритми швидкого реагування та поетапного відновлення після настання інциденту, розрахувати ресурси та визначити сферу відповідальності керівництва щодо забезпечення безперервності діяльності.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 46 найменувань, 2 додатки, і містить 7 таблиць. Повний обсяг кваліфікаційної роботи складає 70 сторінок, з яких перелік посилань займає 5 сторінок, додатки – 16 сторінок.

Ключові слова: лабораторія з контролю якості, план безперервності бізнесу.

ABSTRACT

The development and implementation of a business continuity plan enables a quality control laboratory to determine the criticality of its business processes and work out algorithms for rapid response and phased recovery after an incident, calculate resources and determine the scope of management responsibility for ensuring business continuity.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references of 46 items, 2 appendices, and contains 7 tables. The full scope of the qualification work is 70 pages, of which the list of references takes up 5 pages, appendices - 16 pages.

Keywords: quality control laboratory, business continuity plan.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП	5
РОЗДІЛ 1 ЛАБОРАТОРНИЙ КОНТРОЛЬ ЯКОСТІ. ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ МЕНЕДЖМЕНТУ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ	9
1.1 Роль лабораторій у забезпеченні якості та безпеки лікарських засобів	9
1.2 Концепція безперервності бізнесу: базові поняття, підходи та завдання	11
1.3 Роль інтегрованих систем ERM та BCM у забезпеченні стійкості організацій в умовах невизначеності	17
Висновки до розділу 1	20
РОЗДІЛ 2 АНАЛІЗ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ	21
2.1 Загальна характеристика діяльності лабораторії контролю якості Державної служби України з лікарських засобів та контролю за наркотиками	21
2.2 Оцінка ризиків, загроз та вразливостей у діяльності лабораторії	26
2.3 Сучасні загрози безперервності бізнес-процесів у діяльності Лабораторії контролю якості лікарських засобів та медичної продукції Держлікслужби України	28
Висновки до розділу 2	31
РОЗДІЛ 3 ПРАКТИЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ	33
3.1 Розробка системи оповіщення як елементу забезпечення безперервності діяльності лабораторії	33
3.2 Розрахунок ключових часових параметрів реагування на інциденти	37
3.3 Розробка проєкту планів безперервності бізнесу та управління інцидентами та надзвичайними ситуаціями	40
Висновки до розділу 3	47
ЗАГАЛЬНІ ВИСНОВКИ	49
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	51
ДОДАТКИ	56

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BCM – Business Continuity Management – управління безперервністю бізнесу.

BCMS – системами управління неперервністю бізнесу

BCP – Business Continuity Planning – планування безперервності бізнесу.

BIA – Business impact analysis

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

ERM – Enterprise Risk Management – управління корпоративними ризиками

ISO – International Organization for Standardization (міжнародна організація зі стандартизації)

PDCA Plan-Do-Check-Act – Цикл Шухарта-Демінга: планування – виконання запланованого – перевірка і аналіз – коригування та удосконалення

QRM – Quality Risk Management (Система управління ризиками)

ЛЗ – лікарський засіб

СОП – стандартна операційна процедура

СУЯ – система управління якістю

ВСТУП

Управління безперервністю бізнесу (Business Continuity Management, BCM) є системним підходом до забезпечення стійкості підприємства, який спрямований на збереження його функціонування в умовах кризових і непередбачуваних подій. У сучасному динамічному середовищі, де ризики можуть раптово порушити операційну діяльність, BCM набуває особливої актуальності як інструмент підтримання стабільності та запобігання критичним втратам.

З огляду на поточні соціально-економічні та безпекові виклики в Україні, управління безперервністю бізнесу стає невід'ємною складовою стратегічного управління організаціями. Зростання рівня невизначеності підсилює потребу у впровадженні міжнародних стандартів, зокрема ISO 22301, які встановлюють вимоги до систем управління безперервністю та сприяють підвищенню готовності компаній до кризових ситуацій.

BCM орієнтоване на ідентифікацію потенційних загроз, оцінювання їх впливу та розроблення превентивних і коригувальних заходів, що дозволяють мінімізувати негативні наслідки для ключових бізнес-процесів. Такий проактивний підхід сприяє збереженню операційної стабільності, захисту ділової репутації та формуванню довіри з боку клієнтів і партнерів. Фактично, управління безперервністю бізнесу передбачає підготовку організації до несприятливих сценаріїв з метою забезпечення її адаптивності та довгострокової життєздатності [1, 2].

Основними перевагами впровадження BCM є:

- ідентифікація та управління ризиками, що дозволяє завчасно виявляти загрози та розробляти механізми їх нейтралізації;
- забезпечення безперервності операційної діяльності шляхом наявності планів реагування на різні кризові сценарії;
- формування організаційної стійкості, що дає змогу швидко відновлюватися після порушень і підтримувати стабільний розвиток;

- захист репутації компанії через демонстрацію готовності ефективно діяти в умовах кризи;
- дотримання законодавчих і регуляторних вимог, що знижує ризики юридичних санкцій і фінансових втрат;
- підвищення операційної ефективності завдяки оптимізації процесів і впровадженню сучасних управлінських та цифрових рішень;
- зміцнення довіри клієнтів і партнерів, які отримують гарантії стабільності рівня послуг;
- стимулювання інноваційного мислення, оскільки аналіз ризиків сприяє пошуку нових рішень і можливостей розвитку;
- захист інвестиційної привабливості компанії, адже наявність системи ВСМ свідчить про відповідальне управління ризиками;
- покращення взаємодії в ланцюгах постачання, що забезпечує узгодженість дій із постачальниками та партнерами в кризових умовах [1].

Таким чином, управління безперервністю бізнесу є не лише інструментом антикризового реагування, а й важливою складовою стратегічного розвитку організації, яка забезпечує її стійкість, конкурентоспроможність та довгострокове зростання.

Лабораторії контролю якості лікарських засобів є критично важливими об'єктами фармацевтичної інфраструктури, оскільки забезпечують перевірку якості, безпеки та відповідності лікарських засобів (ЛЗ) фармакопейним вимогам. З огляду на їхню роль та високу відповідальність, важливо забезпечити неперервність їхньої роботи навіть під час кризових подій.

Міжнародний стандарт ISO 22301:2019 визначає вимоги до системи управління безперервністю бізнесу (BCMS) і може застосовуватися для організації стійкої діяльності лабораторій критичної інфраструктури [3; 4].

1. Значення впровадження ISO 22301 у лабораторії контролю якості

Лабораторія контролю якості лікарських засобів залежить від безперебійного функціонування обладнання, інформаційних систем, постачання реактивів та безпечного середовища персоналу.

Інциденти, такі як перебої електропостачання, кібератаки, руйнування інфраструктури, аварії або надзвичайні ситуації, можуть повністю зупинити роботу лабораторії та створити ризики для обігу лікарських засобів [2].

Впровадження системи управління неперервністю діяльності за ISO 22301 дозволяє:

- забезпечити стабільне функціонування критичних лабораторних процесів;
- зменшити час простою;
- захистити дані лабораторних досліджень;
- гарантувати відповідність результатів вимогам фармакопеї [3, 4].

Організація діяльності лабораторії контролю якості лікарських засобів відповідно до ISO 22301 забезпечує її здатність працювати безперебійно навіть у складних або кризових ситуаціях. Завдяки впровадженню системи управління безперервністю діяльності лабораторія отримує підвищений рівень стійкості, зменшує операційні ризики та зміцнює свою роль у фармацевтичній системі. ISO 22301 допомагає лабораторіям виконувати критично важливі функції, гарантуючи якість та безпеку лікарських засобів незалежно від зовнішніх обставин.

Мета роботи. Враховуючи антикризову тенденцію розвитку організацій в Україні, метою нашого дослідження стала розробка планів забезпечення безперервності бізнесу для діяльності лабораторії з контролю якості лікарських засобів.

Об'єкт та предмет дослідження. Об'єкт в цьому дослідженні обрано діяльність лабораторії з контролю якості лікарських засобів, а предметом відповідно є підходи до розробки планів забезпечення безперервності бізнесу.

Основні завдання наших досліджень:

- проаналізувати нормативно-правову базу та літературні джерела щодо питання системи менеджменту безперервності бізнесу;
- визначити ризики, які впливають на безперервність діяльності лабораторії з контролю якості лікарських засобів;
- розробити план забезпечення безперервності діяльності лабораторії з контролю якості лікарських засобів та відповідні інструкції зі швидкого реагування.

Методи дослідження: як методи ми використали статистичний аналіз для оцінювання ризиків що дало нам змогу визначити найбільш уразливі ділянки діяльності та можливі наслідки порушення функціонування лабораторії. Також ми використали метод аналізу наукових джерел літератури та нормативної бази, метод вивчення причинно-наслідкових зв'язків та метод контент-аналізу разом з математичним моделюванням.

Практичне значення отриманих результатів. Результати дослідження будуть нами використовуватися для формування стабільної роботи лабораторії та виконання вимог законодавства щодо безперервності діяльності державних органів.

Дослідження і публікації. Павлюк О.В., Ткачук І.В., Зборовська Т.В., Крутьських Т.В. Підходи до організації діяльності лабораторії з контролю якості відповідно до вимог стандарту ISO 22301. YOUTH PHARMACY SCIENCE : матеріали VI Всеукраїнської науково-практичної конференції з міжнародною участю (10-11 грудня 2025 р., м. Харків). – Харків: НФаУ, 2025. – С.521-523 (Додаток А).

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 46 найменувань, 2 додатки, і містить 7 таблиць. Повний обсяг кваліфікаційної роботи складає 70 сторінок, з яких перелік посилань займає 5 сторінок, додатки – 16 сторінок.

РОЗДІЛ 1

ЛАБОРАТОРНИЙ КОНТРОЛЬ ЯКОСТІ. ТЕОРЕТИЧНІ АСПЕКТИ СИСТЕМИ МЕНЕДЖМЕНТУ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

1.1 Роль лабораторій у забезпеченні якості та безпеки лікарських засобів

Лабораторії контролю якості є ключовою ланкою системи забезпечення безпеки та ефективності лікарських засобів. Саме у лабораторних умовах відбувається аналіз сировини, допоміжних компонентів, проміжної та готової продукції, а також здійснюється державний контроль якості ліків перед їхнім надходженням у продаж. Робота лабораторій регламентується Державною фармакопеею України, вимогами GMP та законодавством у сфері лікарських засобів [5, 6, 7, 8].

Лабораторії відіграють центральну роль у гарантуванні того, що ЛЗ відповідають усім встановленим стандартам безпеки, якості та ефективності.

Основні функції лабораторій:

1. Контроль якості сировини та допоміжних речовин.

Перевірка ідентичності, чистоти, наявності домішок, відповідності фармакопейним нормам є обов'язковою вимогою перед початком виробництва.

2. Аналіз проміжної продукції.

Під час виробництва лабораторії контролюють критичні параметри технологічних процесів, що відповідає стандартам GMP.

3. Контроль якості готової продукції.

Визначаються фізико-хімічні, біологічні, мікробіологічні показники, відповідність нормативній документації та фармакопеї.

4. Дослідження стабільності препаратів.

Лабораторії здійснюють довгострокові та прискорені дослідження стабільності для визначення терміну придатності й умов зберігання лікарських засобів.

5. Постмаркетинговий лабораторний контроль.

Після реалізації ЛЗ лабораторії Держлікслужби перевіряють якість лікарських засобів, що перебувають у обігу, відповідно до Закону України «Про лікарські засоби» [8].

Державні лабораторії мають особливе значення, оскільки здійснюють незалежний контроль серій лікарських засобів, включно з імпортованими. Їх основними функціями є:

- експертиза якості зразків, відібраних у межах державного нагляду;
- лабораторне підтвердження фактів фальсифікації та невідповідності;
- моніторинг побічних реакцій і підозр на неякісні серії спільно з системою фармаконагляду.

Це забезпечує захист населення від небезпечних або фальсифікованих ліків та підтримує стабільність фармацевтичного ринку.

Принципи діяльності лабораторій контролю якості базується на таких характеристиках [5, 6, 9]:

1. Наукова обґрунтованість методів аналізу. Усі методики мають бути валідованими та відповідати фармакопейним вимогам.
2. Об'єктивність та незалежність результатів. Державні лабораторії зобов'язані забезпечувати неупереджений аналіз зразків.
3. Стандартизація та відповідність GMP. Лабораторії виробника та контролю якості повинні діяти відповідно до вимог належної виробничої практики.

4. Високий рівень точності та відтворюваності. Всі результати повинні бути перевірюваними та відтворюваними за міжнародними стандартами.

5. Системний ризик-орієнтований підхід. Пріоритетність надається аналізу критичних параметрів, що найбільше впливають на безпеку препарату.

6. Простежуваність і документування. Усі стадії аналізу супроводжуються детальною документацією, що формує повну історію контролю.

Від якості роботи лабораторій залежить [8, 9]:

- своєчасне виявлення неякісних чи небезпечних препаратів;
- запобігання потраплянню на ринок фальсифікованих медикаментів;
- підтримання довіри суспільства до фармацевтичної галузі;
- підвищення рівня фармакотерапевтичної безпеки пацієнтів.

Регулярний лабораторний контроль є гарантією того, що ЛЗ, які продаються в аптеках, відповідають вимогам національних і міжнародних стандартів.

Лабораторії контролю якості є фундаментальним елементом системи забезпечення безпеки та ефективності ЛЗ. Вони здійснюють багаторівневий контроль – від перевірки сировини до аналізу серій, що перебувають в обігу. Роль лабораторій полягає у забезпеченні достовірності, об'єктивності та відповідності якості ЛЗ установленим стандартам. Саме завдяки їхній діяльності гарантується безпечність фармакотерапії та зберігається довіра населення до системи охорони здоров'я.

1.2 Концепція безперервності бізнесу: базові поняття, підходи та завдання

У сучасному глобалізованому середовищі організації стикаються з численними загрозами: технічними збоями, кібератаками, природними

катаклізмами, геополітичними кризами та пандеміями. У таких умовах особливе значення набуває концепція безперервності бізнесу (Business Continuity), що спрямована на забезпечення здатності організації продовжувати свою діяльність у кризових ситуаціях з мінімальними втратами. Стандартизовані підходи до побудови системи безперервності бізнесу викладені у міжнародному стандарті ISO 22301 [4], а також у працях провідних дослідників з управління ризиками та кризами [1, 2, 10].

Концепція безперервності бізнесу є складовою сучасної системи управління організацією та спрямована на забезпечення її стійкості й здатності функціонувати в умовах порушень, криз і надзвичайних ситуацій. Вона ґрунтується на усвідомленні того, що будь-яка організація піддається впливу внутрішніх і зовнішніх загроз, а повна відсутність ризиків є неможливою. Тому ключовим завданням стає не лише запобігання інцидентам, а й підготовленість до них та здатність швидко відновлювати діяльність.

У центрі концепції безперервності бізнесу перебуває забезпечення безперервного виконання критично важливих процесів або їх оперативного відновлення до прийняттого рівня у разі виникнення деструктивних подій. До таких подій можуть належати техногенні аварії, природні катастрофи, кіберінциденти, збої в ланцюгах постачання, епідеміологічні загрози, а також соціально-політичні та воєнні ризики. Особливої актуальності концепція набуває в умовах високої невизначеності та нестабільності зовнішнього середовища.

Базовим поняттям у межах концепції є безперервність бізнесу (Business Continuity), яка означає здатність організації підтримувати або швидко відновлювати свою діяльність відповідно до задалегідь визначених цільових параметрів. На відміну від традиційного кризового реагування, підхід безперервності бізнесу має проактивний характер і передбачає системне планування дій до настання інцидентів.

Безперервність бізнесу – це здатність організації підтримувати виконання критично важливих функцій під час надзвичайних ситуацій та швидко відновлюватися після них [11].

Інцидент – будь-яка подія, що порушує нормальне функціонування організації або створює ризик такого порушення (технічна аварія, втрата персоналу, кібератака тощо).

Ключовим методологічним інструментом реалізації концепції є система управління безперервністю бізнесу (Business Continuity Management System, BCMS). Вона охоплює політику, процеси, процедури, ресурси та відповідальність персоналу, необхідні для ідентифікації загроз, оцінювання їх впливу та розроблення ефективних заходів реагування. BCMS інтегрується у загальну систему управління організацією та узгоджується зі стратегічними цілями.

Важливим елементом концепції є аналіз впливу на бізнес, який дозволяє визначити критичні процеси, допустимі строки їх простою та пріоритети відновлення. Business Impact Analysis (BIA) – аналіз впливу на бізнес – метод оцінювання того, як зупинка певних процесів вплине на організацію. BIA визначає:

- критичні функції,
- допустимий час простою,
- наслідки збоїв.

Доповненням до нього виступає оцінка ризиків, що спрямована на виявлення ймовірності настання загроз та масштабу їх потенційних наслідків. Сукупність цих інструментів забезпечує обґрунтованість управлінських рішень у сфері безперервності.

Risk Assessment – оцінювання ризиків – підхід, який визначає потенційні загрози, їхню імовірність і наслідки для діяльності організації.

Recovery Time Objective (RTO) і Recovery Point Objective (RPO):

- RTO – максимальний допустимий час відновлення діяльності.

– RPO – допустима втрата даних у часі (наприклад, не більше 30 хвилин) [12, 13].

Особливу роль відіграє формування культури безперервності, за якої кожен працівник усвідомлює свою відповідальність за підтримання стійкості організації. Для застосовують ряд підходів, що допомагають сформувати відповідну культуру управління в організації.

Процесний підхід передбачає аналіз і оптимізацію всіх бізнес-процесів з точки зору їхньої критичності та залежностей. Це дозволяє визначити найуразливіші ланки організації.

Ризик-орієнтований підхід зосереджується на виявленні загроз і побудові стратегій реагування відповідно до рівня ризику. Він широко використовується в управлінні безпекою та згідно зі стандартом ISO 22301.

Стратегічний підхід дає змогу формувати довгострокові плани та резервні рішення: дублювання інфраструктури, альтернативні джерела постачання, партнерські майданчики, резервні IT-центри.

Підхід кризового менеджменту зосереджений на оперативному реагуванні, комунікаціях і взаємодії між командами під час надзвичайних ситуацій. Одним із ключових елементів є створення Кризового штабу [12].

Підхід управління знаннями та навчання передбачає навчання персоналу, регулярні тренування, симуляції кризових ситуацій, аудит планів та їхнє періодичне оновлення [13].

Концепція безперервності бізнесу також передбачає розроблення планів безперервності та відновлення, регулярне їх тестування, навчання персоналу й постійне вдосконалення системи на основі результатів моніторингу та аудитів.

Відповідно до ISO 22301 та класичних концепцій business continuity, система безперервності включає такі елементи:

- Аналіз контексту організації та визначення зацікавлених сторін.
- Оцінювання ризиків та BIA.

- Розроблення стратегій забезпечення безперервності.
- Плани реагування та відновлення діяльності (Emergency Response Plan, Disaster Recovery Plan).
- Забезпечення ресурсами – альтернативні майданчики, резервне електроживлення, дублюючі ІТ-системи.
- Тестування, навчання та тренування персоналу.
- Моніторинг, аудит і вдосконалення системи.

Концепція безперервності бізнесу відіграє ключову роль у забезпеченні стійкості організацій до внутрішніх і зовнішніх загроз. Вона базується на аналізі критичних функцій, оцінюванні ризиків, стратегічному плануванні та готовності до оперативного реагування. Стандарт ISO 22301 забезпечує уніфікований підхід до створення ефективною системи безперервності діяльності, що дозволяє організаціям мінімізувати втрати, зберігати стабільність і швидко відновлюватися у разі інцидентів.

Основні завдання BCMS полягають у забезпеченні стійкості організації до внутрішніх і зовнішніх загроз, мінімізації негативних наслідків надзвичайних ситуацій та підтриманні здатності компанії виконувати свої критично важливі функції у будь-яких умовах. BCMS є інструментом превентивного управління, який поєднує стратегічні, тактичні та операційні рішення.

Передусім одним із ключових завдань BCMS є ідентифікація загроз і вразливостей, що можуть призвести до порушення діяльності. Йдеться про систематичне виявлення ризиків техногенного, природного, інформаційного, кадрового, регуляторного та соціального характеру з урахуванням специфіки діяльності організації та зовнішнього середовища.

Наступним важливим завданням є визначення критично важливих бізнес-процесів та їхніх взаємозв'язків. Це дозволяє встановити, які функції є пріоритетними для збереження життєздатності організації та які ресурси необхідні для їх підтримки або відновлення у разі інцидентів.

Суттєвим завданням BCMS є проведення аналізу впливу на бізнес ВІА, що дає змогу оцінити допустимі строки простою процесів, фінансові, операційні, репутаційні та регуляторні наслідки збоїв, а також визначити цільові показники відновлення (RTO, RPO). Це створює основу для обґрунтованого планування заходів реагування [4, 10, 11, 12, 13].

Система управління безперервністю бізнесу також спрямована на розроблення та впровадження планів безперервності і відновлення діяльності. До таких планів належать плани реагування на надзвичайні ситуації, плани відновлення ІТ-систем, логістичних ланцюгів, виробничих і управлінських процесів. Вони мають бути чіткими, практичними та адаптованими до різних сценаріїв розвитку подій.

Важливим завданням BCMS є забезпечення готовності персоналу до дій у кризових ситуаціях. Це досягається шляхом проведення навчань, тренувань, симуляцій і тестувань планів безперервності, що дозволяє перевірити їх ефективність і підвищити рівень обізнаності працівників.

Окреме місце посідає завдання підтримки ефективної системи комунікацій під час кризових подій. BCMS має забезпечувати своєчасне інформування персоналу, керівництва, партнерів, клієнтів і регуляторних органів, що сприяє зниженню паніки, збереженню довіри та репутації організації.

Не менш важливим є завдання моніторингу, аналізу та постійного вдосконалення системи безперервності бізнесу. BCMS повинна регулярно переглядатися з урахуванням змін у внутрішньому середовищі, законодавстві, технологіях і ризиковому профілі організації. Аудити, аналіз інцидентів і коригувальні дії забезпечують її актуальність і дієвість.

Основні завдання системи управління безперервністю бізнесу зводяться до створення цілісного механізму підготовки, реагування та відновлення, який дозволяє організації зберігати стабільність, відповідати вимогам стандартів (зокрема ISO 22301), зменшувати ризики та забезпечувати сталий розвиток у довгостроковій перспективі [10, 14, 15, 16, 17].

Отже, концепція безперервності бізнесу є комплексним управлінським підходом, що поєднує стратегічне мислення, ризик-орієнтоване планування та операційну готовність. Її впровадження дозволяє організаціям не лише мінімізувати втрати від кризових подій, а й зберігати довіру зацікавлених сторін, забезпечувати стабільність діяльності та довгострокову конкурентоспроможність.

1.3 Роль інтегрованих систем ERM та BCM у забезпеченні стійкості організацій в умовах невизначеності

Інтеграція управління безперервністю бізнесу (Business Continuity Management, BCM) та системи управління корпоративними ризиками (Enterprise Risk Management, ERM) у сучасних умовах набуває критичного значення для організацій, які прагнуть забезпечити стійкість, адаптивність і довгострокову життєздатність. Узгодження цих двох стратегічних підходів дозволяє сформувати цілісну систему управління загрозами, підвищити готовність до кризових ситуацій та мінімізувати негативні наслідки для ключових бізнес-процесів.

Особливої актуальності інтеграція BCM і ERM набуває в умовах України, де бізнес-середовище характеризується підвищеним рівнем невизначеності, зумовленим воєнними діями, руйнуванням інфраструктури, перебоями енергопостачання, логістичними обмеженнями, кіберзагрозами та регуляторними змінами. За таких обставин поєднання системного управління ризиками з плануванням безперервності діяльності стає не лише інструментом підвищення ефективності, а й необхідною умовою виживання організацій, зокрема у фармацевтичному, медичному та критично важливому секторах економіки [18, 19, 20, 21, 22].

Ефективна система ERM у поєднанні з дієвими планами безперервності бізнесу (BCP) сприяє зниженню сукупного рівня ризиків, підвищує якість управлінських рішень і забезпечує раціональний розподіл ресурсів. Інтеграція цих підходів дозволяє уникнути фрагментарності, дублювання

функцій і неузгодженості дій, створюючи прозору та підзвітну систему управління ризиками на всіх рівнях організації. Важливою передумовою цього є наявність стандартизованої інфраструктури управління ризиками, що відповідає вимогам міжнародних стандартів (зокрема ISO 22301 та ISO 31000).

Ключовим завданням організацій є розробка уніфікованих стратегій реагування на різні типи ризиків – від операційних і фінансових до кібернетичних, репутаційних та регуляторних. У сучасних умовах це включає активацію планів аварійного відновлення, резервування критичних ресурсів, забезпечення альтернативних ланцюгів постачання, а також використання цифрових рішень для оперативного управління в надзвичайних ситуаціях. Важливим елементом є впровадження ефективних механізмів моніторингу та регулярного звітування, що забезпечують безперервне вдосконалення системи управління ризиками.

Поєднання BCM та ERM дозволяє більш точно ідентифікувати загрози, оцінювати їх імовірність та потенційний вплив на діяльність, а також визначати пріоритети реагування з урахуванням критичності бізнес-процесів. В умовах цифровізації та зростання кіберзагроз така інтеграція є особливо важливою. За даними міжнародних аналітичних звітів, середній час виявлення інцидентів інформаційної безпеки залишається значним, що підкреслює необхідність завчасної підготовки, наявності актуальних BCP і використання інструментів раннього попередження .

Ефективна інтеграція BCM та ERM потребує чіткого розподілу ролей і відповідальності. У зрілій системі управління ризиками кожен працівник — від вищого керівництва до операційного персоналу — усвідомлює свою роль у забезпеченні безперервності діяльності. Провідна роль належить топ-менеджменту, який визначає прийнятний рівень ризику, затверджує політику управління ризиками та забезпечує ресурсну підтримку. Директор з управління ризиками трансформує стратегічні цілі у практичні інструменти, менеджер з безперервності бізнесу відповідає за актуальність і тестування

планів, а фахівці з інформаційної безпеки – за захист даних і відповідність нормативним вимогам.

Важливим інструментом інтегрованої системи є ключові індикатори ризику (KRI), які виконують функцію раннього попередження та дозволяють виявляти негативні тенденції ще до виникнення кризових подій. Для підвищення ефективності KRI необхідно забезпечити їх розуміння та використання на всіх рівнях організації, а також інтеграцію з системами моніторингу та управлінської звітності [14, 18, 19].

Процес управління ризиками та безперервністю бізнесу починається з ідентифікації наявних і потенційних загроз, подальшої оцінки їх імовірності та наслідків, проведення аналізу впливу на бізнес (BIA) і розроблення відповідних заходів реагування. Оцінювання ризиків має безперервний характер, оскільки зовнішнє середовище постійно змінюється, а нові загрози виникають динамічно. Регулярне тестування планів, навчання персоналу та оновлення процедур є необхідними умовами ефективної підготовки до надзвичайних ситуацій.

Моніторинг і прозора звітність є критично важливими складовими інтегрованої системи. Вони передбачають постійне відстеження ризиків, оцінку ефективності контрольних заходів і реалізацію стратегій пом'якшення наслідків. Використання інформаційних панелей у режимі реального часу дозволяє оперативно інформувати керівництво та персонал про поточний стан ризиків і підвищує загальну керованість системи [20, 21, 22].

Таким чином, управління корпоративними ризиками та управління безперервністю бізнесу є взаємодоповнюючими елементами єдиної стратегії забезпечення стійкості організації. ERM забезпечує комплексне бачення ризиків і підтримку прийняття стратегічних рішень, тоді як BCM фокусується на збереженні та відновленні критичних функцій у кризових умовах. Їх інтеграція дозволяє організаціям в Україні підвищити рівень готовності до надзвичайних ситуацій, зменшити втрати та забезпечити стабільність діяльності в умовах високої турбулентності зовнішнього середовища.

Висновки до розділу 1

У розділі доведено визначальну роль лабораторій контролю якості у забезпеченні безпеки, ефективності та відповідності лікарських засобів національним і міжнародним вимогам. Лабораторії є ключовою ланкою фармацевтичної системи, оскільки здійснюють багаторівневий контроль якості на всіх етапах життєвого циклу лікарських засобів, що сприяє захисту пацієнтів і підтриманню довіри суспільства до фармацевтичного ринку. Їх діяльність ґрунтується на принципах наукової обґрунтованості, стандартизації, об'єктивності, простежуваності та ризик-орієнтованого підходу.

Обґрунтовано значення концепції безперервності бізнесу як сучасного інструменту управління, спрямованого на забезпечення стійкості організацій в умовах криз і надзвичайних ситуацій. Встановлено, що система управління безперервністю бізнесу забезпечує системний підхід до ідентифікації загроз, проведення аналізу впливу на бізнес, планування реагування та відновлення критичних процесів, а також формування культури готовності персоналу до кризових подій.

Показано, що інтеграція управління корпоративними ризиками та безперервністю бізнесу створює цілісну модель забезпечення організаційної стійкості, що є особливо актуальним в умовах високої невизначеності та воєнних викликів в Україні. Поєднання цих підходів дозволяє мінімізувати наслідки криз, підвищити ефективність управлінських рішень і забезпечити стабільне функціонування критично важливих установ, зокрема лабораторій контролю якості лікарських засобів.

РОЗДІЛ 2

АНАЛІЗ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ

2.1 Загальна характеристика діяльності лабораторії контролю якості Державної служби України з лікарських засобів та контролю за наркотиками

Лабораторія контролю якості лікарських засобів та медичної продукції Державної служби України з лікарських засобів та контролю за наркотиками у Київській області є ключовим елементом національної системи державного контролю якості та безпеки лікарських засобів і медичних виробів. Основною метою діяльності лабораторії є забезпечення захисту здоров'я населення шляхом проведення незалежного, об'єктивного та науково обґрунтованого контролю якості продукції, що перебуває в обігу на території регіону.

Стратегічна роль лабораторії полягає у забезпеченні стабільного функціонування державного нагляду за дотриманням вимог законодавства у сфері обігу лікарських засобів, а також у підвищенні рівня довіри до системи регуляторного контролю в умовах євроінтеграційних процесів та воєнного стану.

До ключових напрямів діяльності лабораторії належать:

- проведення лабораторних випробувань лікарських засобів та медичної продукції відповідно до вимог Державної фармакопеї України;
- контроль якості зразків, відібраних у рамках державного нагляду;
- участь у заходах фармаконагляду та реагуванні на повідомлення про неякісні або фальсифіковані лікарські засоби;
- методичне та експертне забезпечення діяльності територіальних органів Держлікслужби.

Лабораторія здійснює свою діяльність відповідно до принципів належної лабораторної практики, вимог ISO/IEC 17025 та з урахуванням

положень стандарту ISO 22301 у частині забезпечення безперервності критично важливих процесів.

Основними пріоритетами лабораторії є:

- якість і достовірність результатів досліджень;
- стійкість та безперервність лабораторної діяльності;
- відповідність національним і міжнародним нормативним вимогам;
- прозорість, незалежність і професійна етика.

Особлива увага приділяється підготовці та підвищенню кваліфікації персоналу, оскільки людський фактор є визначальним для забезпечення точності аналітичних досліджень та оперативного реагування в умовах кризових ситуацій.

Політика якості лабораторії спрямована на:

- забезпечення об'єктивного та своєчасного виконання лабораторних досліджень відповідно до затверджених методик;
- постійне вдосконалення компетентності персоналу через навчання та внутрішні аудити;
- дотримання вимог біобезпеки, охорони праці та екологічної відповідальності;
- ідентифікацію, оцінку та мінімізацію ризиків, що можуть впливати на результати випробувань або безперервність діяльності.

У лабораторії впроваджено ризик-орієнтований підхід, який охоплює як ризики для якості результатів, так і ризики операційного характеру (перебої електропостачання, кадрові втрати, збої в постачанні реактивів, кіберзагрози).

Лабораторія функціонує в межах системи управління якістю, побудованої на процесному підході, який дозволяє чітко визначити взаємозв'язки між управлінськими, основними та допоміжними процесами.

Це створює основу для інтеграції системи управління безперервністю діяльності відповідно до вимог ISO 22301.

Планування безперервності діяльності включає:

- аналіз загроз і ризиків;
- визначення критичних лабораторних процесів;
- розробку процедур реагування та відновлення;
- навчання персоналу й регулярне тестування планів.

Сучасний підхід до управління безперервністю діяльності лабораторії виходить за межі суто технічних аспектів і охоплює кадрові, інформаційні, організаційні та регуляторні складові.

Таким чином, Лабораторія контролю якості лікарських засобів та медичної продукції Держлікслужби у Київській області є системоутворюючим елементом державного контролю у сфері охорони здоров'я, діяльність якого базується на принципах якості, ризик-орієнтованого управління та забезпечення безперервності. В умовах підвищеної невизначеності сучасного середовища саме інтеграція систем управління якістю, ризиками та безперервністю діяльності є запорукою стабільного виконання покладених на лабораторію функцій.

Система управління якістю (СУЯ) є ключовим елементом діяльності будь-якої організації, яка прагне забезпечити стабільність процесів, відповідність продукції або послуг встановленим вимогам, а також постійне вдосконалення. Особливо важливою СУЯ є у лабораторіях та фармацевтичних установах, де якість результатів має критичне значення для здоров'я і безпеки споживачів. Основні міжнародні стандарти, на яких ґрунтується система якості, – ISO 9001:2015 та ISO/IEC 17025:2017 [23, 24].

Сучасна система управління якістю включає політику у сфері якості, документовані процедури, стандартизовані процеси та інструменти моніторингу ефективності. Основними її принципами є орієнтація на клієнта,

лідерство керівництва, процесний підхід, управління ризиками та постійне вдосконалення [25]. У лабораторії СУЯ забезпечує:

- достовірність і точність результатів;
- відтворюваність випробувань;
- відповідність методик вимогам стандартизації;
- належне управління персоналом і обладнанням;
- прозоре документування процесів.

Політика якості лабораторії визначає стратегічні її наміри та підкреслює її відповідальність за забезпечення точності, неупередженості та технічної компетентності. Відповідно до ISO 9001, політика повинна бути документованою, комунікованою персоналу та регулярно переглядатися [25].

СУЯ передбачає чітку систему документів:

- стандартні операційні процедури (СОП);
- методики аналізу;
- інструкції;
- протоколи випробувань;
- записи щодо навчання персоналу.

ISO/IEC 17025 підкреслює важливість контролю змін у документах, захисту від втрат та забезпечення доступності актуальних версій [9].

Одна з ключових вимог контроль лабораторного обладнання – забезпечення калібрування, валідації та технічного обслуговування обладнання. Метрологічна служба контролює точність вимірювальних приладів та веде відповідну документацію [25].

Контроль якості досліджень проводиться основними інструментами до яких належать внутрішній лабораторний контроль (контрольні зразки, проби-сліди, бланкові вимірювання), міжлабораторні порівняння, участь у програмах професійного тестування (РТ) [23].

Відповідно до ISO/IEC 17025, лабораторія повинна підтвердити придатність аналітичних методів для конкретних досліджень. Оцінюються

такі характеристики, як точність, відтворюваність, межа виявлення, специфічність [9].

СУЯ передбачає ідентифікацію ризиків, що можуть негативно вплинути на якість результатів, та впровадження заходів їх мінімізації. Ризик-орієнтований підхід є обов'язковим елементом сучасних стандартів [26].

Регулярні внутрішні аудити дозволяють оцінити відповідність процедур вимогам стандартів і внутрішньої документації. Звітність перед керівництвом забезпечує ухвалення рішень щодо коригувальних і запобіжних дій [25].

Аналіз СУЯ показує, що ефективність управління якістю залежить від таких факторів:

1. Компетентність персоналу – постійне навчання та атестація.
2. Стан лабораторного обладнання – дотримання графіків калібрування і сервісу.
3. Чіткість документації – актуальність СОП, прозорість процедур.
4. Регулярність контролю – проведення аудиту, перевірок, контролю умов зберігання зразків [25].
5. Наявність системи вдосконалення – робота з невідповідностями, аналіз причин, коригувальні дії.

Завдяки системному підходу лабораторія може забезпечити високу якість та достовірність результатів, відповідність вимогам регуляторів і міжнародним стандартам.

Аналіз наявної системи управління якістю в лабораторії демонструє її ключову роль у забезпеченні достовірності, точності та відтворюваності результатів. Процедури контролю – включно з управлінням обладнанням, валідацією методів, проведенням внутрішніх аудитів і контролем документів – формують комплексний механізм підтримання високих стандартів якості. Ефективна СУЯ сприяє мінімізації ризиків, підвищенню довіри до результатів досліджень та безперервному вдосконаленню діяльності лабораторії.

2.2 Оцінка ризиків, загроз та вразливостей у діяльності лабораторії

Сучасні лабораторії відіграють ключову роль у системах контролю якості, охорони здоров'я, фармації, екологічного моніторингу та промислової безпеки. Їхня діяльність має високу критичність, тому будь-яке переривання процесів може спричинити серйозні наслідки – від затримок у випуску лікарських засобів до порушення регуляторних вимог і загрози безпеці споживачів.

Міжнародний стандарт ISO 22301:2019, що регулює систему BCMS, визначає ризик-орієнтований підхід як один із основних інструментів забезпечення стійкості організації [26, 27].

Оцінка ризиків та вразливостей дозволяє лабораторії:

- визначити події, що можуть призвести до переривання діяльності;
- проаналізувати можливі наслідки технічних, організаційних або зовнішніх загроз;
- розробити плани реагування та відновлення;
- підвищити рівень стійкості відповідно до вимог ISO 22301.

Таблиця 2.1.

Основні категорії ризиків у діяльності лабораторії

Види ризиків	Характеристика
Технічні ризики	<ul style="list-style-type: none"> – відмова лабораторного обладнання (хроматографів, спектрометрів тощо); – поломка систем контролю навколишнього середовища (кліматичні камери, інкубатори); – збій у роботі допоміжної інфраструктури (вентиляції, водопостачання, електромереж); – втрати чи пошкодження зразків внаслідок технічних збоїв.
Інформаційні ризики (LIMS, ERP).	<ul style="list-style-type: none"> – кібератаки (шифрувальники, фішинг, витік даних); – збій серверів; – недоступність лабораторних баз даних; – втрата результатів досліджень.

Продовження таблиці 2.1.

Логістичні ризики	<ul style="list-style-type: none"> – затримок у постачанні реактивів, стандартів, витратних матеріалів; – порушення холодового ланцюга при транспортуванні зразків; – пошкодження матеріалів у дорозі.
Ризики, пов'язані з персоналом	<ul style="list-style-type: none"> – дефіцит кваліфікованого персоналу; – раптова недоступність співробітників (хвороби, надзвичайні ситуації); – низький рівень підготовки або порушення СОП.
Фізичні та екологічні загрози	<ul style="list-style-type: none"> – пожежі; – паводки; – землетруси; – екстремальні температурні режими; – техногенні аварії у зоні розташування лабораторії.
Загрози безпеці приміщень	<ul style="list-style-type: none"> – несанкціонований доступ, – крадіжки, – вандалізм, – порушення цілісності зразків чи обладнання.

Методологія оцінки ризиків та вразливостей полягає в наступних кроках:

1. Для ідентифікації ризиків використовується опитування персоналу, аналіз історії інцидентів, дані метрології та аудити.

2. Аналіз впливу на діяльність проводиться для визначення критичних функцій лабораторії, часу їх відновлення та можливих втрат у разі зупинки роботи.

3. Аналіз ймовірності та серйозності наслідків проводиться на основі матриць ризику оцінюють імовірність настання події та масштаб впливу (від незначного до катастрофічного).

4. Оцінка вразливостей – це слабкі місця у процесах, інфраструктурі або організації роботи. Наприклад: відсутність резервного обладнання, недостатня кібербезпека, відсутність дублювання даних, нестача автоматизованих систем контролю температури.

5. Формування карти ризиків дає змогу визначити пріоритетні загрози і спрямувати ресурси на їх мінімізацію.

На основі оцінки лабораторія формує програму заходів мінімізації ризиків, що включає:

- стратегії резервування (дублююче обладнання, UPS, генератори);
- процедури реагування на інциденти;
- програми кіберзахисту (ISO 27001);
- плани безперервності діяльності та сценарії відновлення;
- навчання персоналу та регулярні тренування [26, 27].

Оцінка ризиків та вразливостей у діяльності лабораторії є невід’ємною складовою системи управління неперервністю діяльності. Вона дозволяє своєчасно виявляти потенційні загрози, прогнозувати їх наслідки та впроваджувати заходи, що мінімізують вплив інцидентів на критично важливі процеси. Комплексний підхід, заснований на вимогах ISO 22301 та ISO/IEC 17025, забезпечує лабораторії стійкість, надійність і готовність до роботи в умовах невизначеності.

2.3 Сучасні загрози безперервності бізнес-процесів у діяльності Лабораторії контролю якості лікарських засобів та медичної продукції Держлікслужби України

Функціонування Лабораторії контролю якості лікарських засобів та медичної продукції є критично важливим для забезпечення державного нагляду у сфері охорони здоров’я. Безперервність її діяльності напряму впливає на своєчасність прийняття регуляторних рішень, безпеку пацієнтів та стабільність фармацевтичного ринку. У сучасних умовах лабораторія функціонує в середовищі підвищеної невизначеності, що зумовлює наявність комплексу взаємопов’язаних загроз безперервності бізнес-процесів.

1. Безпекові та воєнні загрози. В умовах збройної агресії проти України лабораторія перебуває під впливом безпекових ризиків, серед яких:

- загроза ракетних та дронівих атак;

- руйнування або пошкодження лабораторних приміщень;
- необхідність евакуації персоналу;
- обмеження доступу до об'єктів критичної інфраструктури.

Такі загрози можуть призвести до повної або часткової зупинки лабораторних досліджень, втрати зразків, документації та обладнання, що безпосередньо впливає на безперервність основних процесів контролю якості.

2. Енергетичні та інфраструктурні загрози. Лабораторні дослідження значною мірою залежать від стабільного енергопостачання та функціонування інженерних систем. До ключових загроз належать:

- аварійні та планові відключення електроенергії;
- збої у роботі систем вентиляції, кондиціонування та водопостачання;
- нестабільність температурно-вологісного режиму зберігання зразків і реактивів.

Порушення інфраструктурного забезпечення може спричинити псування дослідних зразків, зупинку приладів, втрату результатів аналізів і необхідність повторного відбору зразків.

3. Кадрові загрози. Кадровий потенціал є критичним ресурсом лабораторії. Основними загрозами у цій сфері є:

- дефіцит висококваліфікованих фахівців;
- мобілізація персоналу або його вимушене переміщення;
- професійне вигорання в умовах тривалого стресу;
- залежність окремих процесів від ключових експертів.

Втрата або тимчасова недоступність персоналу може призвести до зниження пропускнуєї спроможності лабораторії, затримок у виконанні досліджень і ризику помилок.

4. Технологічні та інформаційні загрози. Сучасна лабораторія значною мірою залежить від цифрових технологій та інформаційних систем. Основні ризики включають:

- кібератаки та несанкціонований доступ до даних;
- збої лабораторних інформаційних систем (LIMS);
- втрату або пошкодження електронних баз даних;
- відсутність резервного копіювання або віддаленого доступу.

Реалізація таких загроз може призвести до втрати простежуваності результатів досліджень, порушення вимог акредитації та зниження довіри до лабораторних висновків.

5. Загрози ланцюгів постачання. Безперервність діяльності лабораторії залежить від своєчасного постачання:

- реактивів і стандартних зразків;
- витратних матеріалів;
- запасних частин до аналітичного обладнання.

Сучасні логістичні ризики включають:

- порушення імпорتنих поставок;
- обмеження митного оформлення;
- подорожчання або дефіцит критичних матеріалів.

Ці загрози можуть призвести до зупинки окремих видів аналізів і зниження загальної результативності лабораторії.

6. Регуляторні та організаційні загрози. До цієї групи належать:

- часті зміни нормативно-правових вимог;
- обмеженість бюджетного фінансування;
- затримки в затвердженні процедур або оновленні методик;
- залежність від рішень центральних органів влади.

Організаційні обмеження можуть негативно впливати на оперативність реагування лабораторії на кризові ситуації.

7. Біологічні та епідеміологічні загрози. Пандемії та спалахи інфекційних захворювань створюють додаткові виклики:

- ризик захворювання персоналу;
- необхідність впровадження спеціальних режимів роботи;
- зменшення доступності персоналу та приміщень.

Такі загрози впливають на стабільність кадрового забезпечення та організацію робочих процесів [26, 27, 28, 29, 30, 31].

Таким чином, сучасні загрози безперервності бізнес-процесів у діяльності Лабораторії контролю якості лікарських засобів та медичної продукції Держлікслужби України мають комплексний і взаємопов'язаний характер. Вони охоплюють безпекові, інфраструктурні, кадрові, технологічні, логістичні та регуляторні аспекти діяльності.

У цих умовах впровадження системи управління безперервністю бізнесу відповідно до вимог стандарту ISO 22301 є необхідною передумовою забезпечення стійкості лабораторії, своєчасного виконання її функцій та збереження рівня державного контролю якості лікарських засобів навіть у кризових ситуаціях.

Висновки до розділу 2

Проведений аналіз підтверджує, що Лабораторія Держлікслужби є критично важливим елементом державної системи забезпечення якості та безпеки ЛЗ. Її діяльність безпосередньо впливає на регуляторні рішення, стабільність фармацевтичного ринку та рівень захисту здоров'я населення, особливо в умовах воєнного стану й підвищеної невизначеності.

Встановлено, що функціонування лабораторії ґрунтується на системі управління якістю, що забезпечує достовірність і відтворюваність результатів досліджень. Водночас ідентифіковано широкий спектр ризиків і загроз безперервності діяльності, зокрема безпекові, інфраструктурні, кадрові, технологічні, інформаційні, логістичні та регуляторні, які можуть призводити до порушення критичних бізнес-процесів. Доведено, що застосування ризик-

орієнтованого підходу та системної оцінки вразливостей створює передумови для підвищення стійкості лабораторії. У цьому контексті впровадження системи управління безперервністю бізнесу відповідно до стандарту ISO 22301 є необхідною умовою забезпечення стабільності діяльності, збереження функціональної спроможності лабораторії та виконання нею державних контрольних функцій навіть у кризових ситуаціях.

РОЗДІЛ 3

ПРАКТИЧНІ ЗАХОДИ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ

3.1 Розробка системи оповіщення як елементу забезпечення безперервності діяльності лабораторії

Система оповіщення в межах управління безперервністю бізнесу – це сукупність організаційних, технічних і процедурних засобів, призначених для своєчасного інформування персоналу, керівництва та відповідальних осіб про настання або загрозу надзвичайної події з метою швидкої активації планів реагування і відновлення.

Відповідно до стандарту ISO 22301, ефективна система оповіщення є критичним елементом реагування на інциденти та управління кризами і забезпечує безпеку персоналу та впливає на оперативність запуску плану безперервності та мінімізації часу простою критичних процесів [28, 29].

Для лабораторії контролю якості лікарських засобів система оповіщення має особливе значення, оскільки затримки у комунікаціях можуть призвести до:

- втрати зразків і результатів досліджень;
- порушення вимог ISO/IEC 17025;
- зупинки державного контролю якості лікарських засобів.

Основними цілями впровадження системи оповіщення є негайне інформування персоналу про загрозу або інцидент, активація груп швидкого реагування та кризового штабу і відповідно увімкнення режиму координації дій між структурними підрозділами та захист персоналу, зразків, даних і обладнання, зменшення RTO та MTRD для критичних процесів.

До ключових завдань системи оповіщення належать:

- передача сигналу оповіщення протягом визначеного часу;
- доведення чітких інструкцій щодо дій;

- підтвердження отримання повідомлення;
- документування події та дій персоналу.

Система оповіщення в Лабораторії має охоплювати, щонайменше, такі сценарії на сьогодні:

- повітряна тривога та воєнні загрози;
- аварійне відключення електропостачання;
- пожежа, задимлення, витік небезпечних речовин;
- кіберінциденти (атаки на LIMS, витік даних);
- порушення умов зберігання зразків і реактивів;
- затримка постачання критичних матеріалів;
- епідеміологічні загрози.

Нами запропонована багаторівнева система оповіщення для лабораторії, яка включає:

1. Організаційний рівень. Координатор BCMS / відповідальний за оповіщення активує систему, приймає рішення щодо рівня інциденту. Кризовий штаб лабораторії керує реагуванням, приймає управлінські рішення. Групи швидкого реагування виконують оперативні дії (евакуація, збереження зразків, резервування даних).

2. Технічні канали оповіщення (з принципом дублювання). Основні канали:

- корпоративна електронна пошта;
- SMS / месенджери (Signal, WhatsApp, Viber);
- телефонні дзвінки ключовим особам;
- сповіщення через LIMS або внутрішню IT-систему.

Резервні канали:

- гучномовці у приміщеннях;
- паперові списки контактів;
- оповіщення через керівників змін;
- державна система цивільного захисту (повітряна тривога).

Таблиця 3.1.

Рівні оповіщення

Рівень	Характер події	Дії
Інформаційний	потенційна загроза	моніторинг, підготовка
Операційний	порушення процесу	активація процедур реагування
Кризовий	повна/часткова зупинка	активація ВСР, евакуація

Ми пропонуємо наступний алгоритм процедури оповіщення:

1. Виявлення інциденту.
2. Оцінка рівня загрози (≤ 30 хв). Оцінка ризиків здійснюється за двома ключовими параметрами: Імовірність настання події (P) та Рівень впливу на діяльність лабораторії (I). Загальний рівень загрози визначається як: $R = P \times I$

Шкали оцінки рівня загрози для діяльності лабораторії наведені в табл. 3.2, табл. 3.3, табл. 3.4., табл. 3.5

Таблиця 3.2.

Шкала імовірності (P)

Бал	Рівень імовірності	Характеристика
1	Дуже низька	Подія майже неможлива, поодинокі випадки
2	Низька	Можлива раз на кілька років
3	Середня	Виникає періодично (1 раз на рік)
4	Висока	Виникає регулярно
5	Дуже висока	Очікувана або постійна загроза

Таблиця 3.3.

Шкала впливу (I)

Бал	Рівень впливу	Наслідки для лабораторії
1	Незначний	Короткочасні збої без впливу на результати
2	Малий	Локальна затримка, без втрати зразків
3	Середній	Зупинка окремих процесів до 24 год
4	Високий	Втрата зразків, порушення стандартів
5	Критичний	Повна зупинка діяльності, регуляторні наслідки

Таблиця 3.4.

Матриця оцінки рівня загрози

R = P×I	Рівень загрози	Інтерпретація
1–4	Низький	Контроль у межах процедур
5–9	Помірний	Потрібні коригувальні дії
10–14	Високий	Обов'язкові заходи реагування
15–25	Критичний	Активація BCP / BCMS

Таблиця 3.5.

Приклад оцінки ключових ризиків лабораторії

Ризик	P	I	R	Рівень
Відключення електроенергії	4	4	16	Критичний
Кібератака на LIMS	3	5	15	Критичний
Затримка постачання реактивів	4	3	12	Високий
Недоступність ключового персоналу	3	4	12	Високий
Пожежа	2	5	10	Високий
Повітряна тривога	5	3	15	Критичний

Результати оцінки використовуються для визначення критичних процесів, встановлення RTO та MTPD, пріоритизації заходів реагування, формування планів безперервності та відновлення, прийняття управлінських рішень керівництвом [28, 29, 32, 33].

Запропонована шкала оцінки рівня загроз дозволяє системно, кількісно та прозоро оцінювати ризики для діяльності лабораторії контролю якості лікарських засобів. Її застосування відповідає вимогам ISO 22301 та забезпечує обґрунтоване планування заходів реагування, підвищуючи стійкість лабораторії до технічних, кадрових, інформаційних та безпекових загроз.

3. Активація системи оповіщення.
4. Інформування персоналу та відповідальних осіб.
5. Підтвердження отримання повідомлення.
6. Виконання дій згідно з планами реагування.
7. Фіксація інциденту та аналіз ефективності.

Система оповіщення є невід'ємною частиною BCMS та має регулярно тестуватися (не рідше 1 разу на рік), бути інтегрованою з BIA, BCP і DRP та супроводжуватися постійним навчанням персоналу та інструктажами й відповідно переглядатися після кожного інциденту або навчань.

Система оповіщення є критично важливим елементом забезпечення безперервності діяльності лабораторії контролю якості лікарських засобів. Її ефективність визначає швидкість реагування на надзвичайні події, рівень захисту персоналу та збереження результатів досліджень. Запропонована багаторівнева модель оповіщення, побудована за принципами ISO 22301, дозволяє суттєво зменшити час реагування, мінімізувати наслідки інцидентів та забезпечити стійке виконання регуляторних функцій лабораторії навіть в умовах криз і надзвичайних ситуацій.

3.2 Розрахунок ключових часових параметрів реагування на інциденти

Ефективність системи управління безперервністю діяльності лабораторії значною мірою визначається правильним встановленням часових параметрів реагування на інциденти. Від своєчасності виявлення події, прийняття управлінського рішення та відновлення критичних процесів залежить збереження зразків, достовірність результатів досліджень і виконання регуляторних функцій. У межах стандарту ISO 22301 ключові часові параметри формуються на основі BIA та оцінки ризиків.

Базовим показником є максимально допустимий період переривання діяльності (MTPD), який визначає граничний час, протягом якого лабораторний процес може бути зупинений без неприйнятних наслідків для безпеки, відповідності нормативним вимогам і репутації органу державного контролю. Для критичних лабораторних процесів (приймання зразків, проведення випробувань, збереження результатів) MTPD, як правило, становить від 24 до 72 годин залежно від характеру досліджень [33, 34, 35].

На основі МТРД встановлюється цільовий час відновлення (Recovery Time Objective, RTO) – період, упродовж якого процес повинен бути відновлений після інциденту. Значення RTO завжди є меншим за МТРД і враховує необхідність резерву часу для стабілізації роботи. Для більшості критичних процесів лабораторії доцільним є встановлення RTO у межах 4-24 годин, що дозволяє уникнути втрати зразків та порушення вимог стандартів.

Важливим параметром для інформаційних та цифрових процесів є цільова точка відновлення (Recovery Point Objective, RPO), яка визначає максимально допустимий обсяг втрати даних у часі. Для лабораторних інформаційних систем (LIMS, електронні протоколи, бази результатів) RPO має бути мінімальним і, залежно від технічних можливостей, становити від 15 хвилин до 1 години. Це забезпечує збереження простежуваності та цілісності даних досліджень.

Окремо визначається час виявлення інциденту (Detection Time) та час реагування (Response Time), що охоплює період від моменту настання події до запуску плану безперервності. Для лабораторії оптимальним є виявлення інцидентів протягом 5-30 хвилин (для технічних і ІТ-збоїв) та негайне інформування відповідальних осіб. Час прийняття управлінського рішення і активації плану реагування не повинен перевищувати 1 години.

Розрахунок зазначених часових параметрів здійснюється з урахуванням:

- критичності процесу для виконання регуляторних функцій;
- можливості фізичного збереження зразків і матеріалів;
- залежності від інфраструктури та персоналу;
- наслідків для відповідності вимогам стандартів і законодавства.

Найкоротші МТРД мають процеси, пов'язані з безпекою персоналу, зберіганням зразків та підтриманням контрольованих умов.

ІТ-системи (LIMS) мають жорсткі RPO через вимоги простежуваності та акредитації.

Аналітичні дослідження допускають довший простій, але лише за умови збереження зразків та даних.

Регуляторна звітність критична з точки зору репутаційних і правових наслідків, але має більшу толерантність у часі [33, 34, 35].

Таблиця 3.6.

Часові рамки для критичних процесів лабораторії

№	Критичний процес	Потенційні наслідки зупинки	MTPD	RTO	RPO
1	Приймання, реєстрація та ідентифікація зразків	Втрата простежуваності, порушення фармаконагляду	24 год.	8 год.	1 год.
2	Фізико-хімічні та фармакопейні випробування	Затримка регуляторних рішень, ризик дефіциту ЛЗ	72 год.	24 год.	4 год.
3	Мікробіологічні та біологічні дослідження	Неможливість випуску серій, ризик для пацієнтів	48 год.	24 год.	2 год.
4	Зберігання зразків і реактивів (температурний контроль)	Псування зразків, повторний відбір	6-12 год.	4 год.	0-1 год.
5	Робота LIMS та електронних баз даних	Втрата результатів, порушення акредитації	12 год.	6 год.	0,5 год.
6	Оформлення протоколів випробувань і висновків	Затримка рішень Держлікслужби	48 год.	24 год.	4 год.
7	Комунікація з регуляторними органами	Втрата керованості, репутаційні ризики	24 год.	8 год.	2 год.
8	Забезпечення біобезпеки та охорони праці	Ризик для персоналу, зупинка діяльності	6 год.	2 год.	0 год.

Ці часові рамки можуть бути безпосередньо використані для:

- розроблення Плану безперервності діяльності (BCP);

- формування Disaster Recovery Plan (DRP) для IT;
- визначення потреб у резервному живленні, дублюванні обладнання;
- підготовки до аудиту ISO 22301.

Таким чином, встановлення та обґрунтування часових параметрів реагування на інциденти є ключовим елементом BCMS лабораторії. Вони забезпечують структурований підхід до управління кризовими ситуаціями, дозволяють пріоритизувати ресурси та створюють основу для ефективного планування безперервності й відновлення діяльності відповідно до вимог ISO 22301.

3.3 Розробка проєкту планів безперервності бізнесу та управління інцидентами та надзвичайними ситуаціями

Розробка плану безперервності бізнесу – BCP для лабораторії контролю якості лікарських засобів є системним і поетапним процесом, спрямованим на забезпечення стійкого виконання критично важливих функцій у разі надзвичайних ситуацій. Відповідно до вимог стандарту ISO 22301.

Першим етапом є визначення контексту діяльності лабораторії та зацікавлених сторін. На цьому етапі аналізуються внутрішні й зовнішні фактори, що впливають на безперервність діяльності, зокрема нормативно-правові вимоги, роль лабораторії у системі державного контролю, очікування регуляторних органів, пацієнтів та фармацевтичного ринку. Формується перелік зацікавлених сторін і визначаються їхні потреби у кризових умовах.

Другим етапом є ідентифікація загроз і оцінка ризиків, які можуть призвести до порушення лабораторної діяльності. Аналіз охоплює технічні, інфраструктурні, кадрові, інформаційні, логістичні та безпекові ризики, включно з воєнними та кіберзагрозами. Оцінка ризиків здійснюється з урахуванням імовірності їх настання та масштабу впливу на критичні процеси [36, 37, 38, 39].

Третім ключовим етапом є проведення аналізу впливу на діяльність. Його метою є визначення критичних лабораторних процесів, допустимого часу їх переривання, пріоритетів відновлення та необхідних ресурсів. На основі ВІА встановлюються часові параметри реагування, зокрема MTPD, RTO та RPO, що формують основу для подальшого планування заходів відновлення.

Наступним етапом є розроблення стратегій забезпечення безперервності та відновлення діяльності. Для кожного критичного процесу визначаються альтернативні рішення, такі як резервне електроживлення, дублювання обладнання, альтернативні постачальники реактивів, резервне зберігання зразків і даних, можливість перерозподілу функцій між підрозділами або тимчасове скорочення обсягу робіт.

П'ятий етап передбачає безпосереднє формування плану безперервності бізнесу, який документує порядок дій персоналу у разі інциденту. План містить опис сценаріїв надзвичайних ситуацій, процедури оповіщення та ескалації, ролі й відповідальність працівників, алгоритми реагування, порядок відновлення процесів і правила комунікації з керівництвом та зовнішніми органами.

Важливим елементом процесу є організація управління кризовими ситуаціями, що включає створення кризової команди або груп швидкого реагування. Визначається порядок прийняття рішень, координації дій та взаємодії між структурними підрозділами лабораторії під час надзвичайних подій.

Завершальними етапами є навчання персоналу, тестування та актуалізація плану. Працівники лабораторії проходять регулярні навчання й тренування за сценаріями можливих інцидентів, що дозволяє перевірити практичну придатність плану та підвищити рівень готовності. За результатами навчань і реальних інцидентів план переглядається та вдосконалюється.

Таким чином, процес розробки плану безперервності бізнесу для лабораторії є безперервним циклом, що поєднує аналіз ризиків, планування, практичну реалізацію та постійне вдосконалення. Реалізація такого підходу забезпечує стійкість лабораторії, збереження якості досліджень і безперервне виконання державних регуляторних функцій навіть в умовах криз і надзвичайних ситуацій.

Крім загального плану безперервності бізнесу розробляються інструкції з реагування на кожен інцидент, який було визначено як критичний для діяльності Лабораторії під час оцінки ризиків.

У діяльності лабораторій з контролю якості лікарських засобів особливе значення має здатність оперативно реагувати на інциденти та надзвичайні ситуації. Такі події можуть призвести до порушення досліджень, втрати даних, пошкодження зразків, ризиків для персоналу або зупинки критичних процесів [25, 26, 38, 39, 40, 41].

Відповідно до стандарту ISO 22301:2019, організація повинна мати документований план швидкого реагування – управління інцидентами, який забезпечує чіткі дії персоналу у випадку кризових подій.

План є ключовим компонентом BCMS і базується на принципах кризового менеджменту та ефективної комунікації.

План створюється для того, щоб забезпечити своєчасне та скоординоване реагування на інциденти, мінімізувати вплив на критичні процеси лабораторії, захистити персонал, обладнання, дані та зберегти роботу лабораторії на прийнятному рівні відповідно вимогам стандартів.

План також формує основу для подальшого відновлення діяльності згідно з планами Business Continuity та Disaster Recovery.

Згідно з рекомендаціями ISO 22301 і міжнародною практикою, план складається з таких ключових компонентів (Додаток Б):

1. Ідентифікація інцидентів. Документ має містити класифікацію інцидентів, серед яких: технічні – відмова обладнання, збій у вентиляційних системах, аварії з реактивами; IT-інциденти – кібератаки, збій LIMS, втрата

доступу до мережі; природні – пожежі, повені, землетруси; загрози безпеці – несанкціонований доступ, порушення фізичного захисту; епідеміологічні інциденти – захворювання персоналу, карантин.

2. Ролі та відповідальність. План визначає:

- керівника кризового реагування;
- координатора інцидентів;
- команду оцінки ситуації;
- відповідальних за технічні, ІТ-та безпекові аспекти;
- контакти екстрених служб.

Функції кожної ролі ретельно документуються для уникнення плутанини в кризових умовах.

3. Порядок дій у разі інциденту описує сценарії реагування за основними типами інцидентів:

- Виявлення та підтвердження інциденту.
- Початкове оцінювання масштабів та ризиків.
- Оповіщення керівництва та персоналу.
- Активування плану реагування.
- Виконання дій з локалізації та мінімізації наслідків.
- Документування інциденту та збереження доказів [2].

4. Комунікація є критичною під час надзвичайних ситуацій. Комунікаційний план визначає канали внутрішнього сповіщення (телефон, месенджери, система внутрішніх оповіщень), способи комунікації з регуляторними органами, правила взаємодії зі сторонніми службами, порядок інформування партнерів та стейкхолдерів.

5. План містить перелік ресурсів, доступних під час інцидентів:

- аварійні комплекти;
- резервні джерела живлення;
- запасні ноутбуки або сервери;
- засоби індивідуального захисту;

- протипожежне обладнання;
- резервні приміщення для тимчасової роботи.

6. План евакуації та дії щодо безпеки персоналу визначає маршрути евакуації, безпечні пункти збору, порядок порятунку людей, поведінку персоналу під час пожежі або хімічної аварії.

7. ISO 22301 підкреслює необхідність створення журналу інцидентів, у якому фіксуються: дата та час; тип інциденту; залучений персонал; прийняті заходи; наслідки; рекомендації щодо запобігання повторенню.

8. Лабораторія зобов'язана:

- проводити регулярні тренування;
- здійснювати перевірку сценаріїв аварій;
- оновлювати план на основі отриманих уроків;
- здійснювати аналіз ефективності реагування.

Розробка плану управління інцидентами є ключовим елементом системи безперервності діяльності лабораторії. Завдяки правильно розробленому документу організація може швидко реагувати на кризові події, мінімізувати збитки, забезпечити безпеку персоналу та зберегти критичні процеси. Такий план підвищує загальну стійкість лабораторії, сприяє відповідності стандартам ISO та зміцнює довіру партнерів і споживачів.

Сучасні лабораторії характеризуються високою залежністю від технологічного обладнання, інформаційних систем, стабільних поставок і кваліфікованого персоналу. Порухення будь-якого з цих елементів може призвести до зупинки роботи лабораторії та серйозних наслідків для якості, безпеки й регуляторної відповідності [25, 42, 43, 44].

Відповідно до стандарту ISO 22301:2019, організації повинні мати План відновлення критично важливих процесів (Recovery Plan), який забезпечує повернення діяльності до прийняттого рівня у визначені строки після інцидентів.

Цей план базується на результатах аналізу впливу на діяльність та оцінки ризиків, і є одним із ключових компонентів системи управління неперервністю діяльності лабораторії.

План відновлення виконує такі функції:

- забезпечує контрольований та швидкий перехід до післяінцидентного режиму роботи;
- мінімізує ризики втрати результатів досліджень, даних і зразків;
- гарантує безпеку персоналу та стабільність функціонування технічної інфраструктури;
- забезпечує відповідність нормативам та стандартам.

Цей документ також формує основу для забезпечення стійкості лабораторії та її здатності працювати у надзвичайних умовах.

Основні етапи побудови плану відновлення:

1. Визначення критичних процесів. На основі ВІА лабораторія визначає процеси, зупинка яких матиме найбільший вплив на:

- якість лабораторних випробувань;
- дотримання регуляторних вимог;
- безпеку персоналу;
- функціональність обладнання;
- здатність надавати результати клієнтам у встановлені строки.

2. Встановлення RTO та RPO. У плані визначаються: RTO (Recovery Time Objective) – максимальний дозволений час відновлення процесу; RPO (Recovery Point Objective) – допустима втрата даних у часі. Ці параметри дозволяють визначити, у які строки процеси повинні бути відновлені, щоб уникнути критичних наслідків.

3. Розробка стратегій відновлення. План містить перелік заходів і засобів, які дозволяють відновити діяльність лабораторії, зокрема:

- Резервування обладнання: дублювання критичних приладів (аналітичні ваги, мікроскопи, хроматографи); альтернативні робочі станції; ручні або спрощені методики як тимчасова заміна технологічним системам.

- Резервування приміщень: використання альтернативної кімнати або майданчика; обладнання зон тимчасового переміщення критичних процесів.

- IT-відновлення: використання хмарних сервісів; резервні сервери;
- відновлення LIMS із резервних копій; перевірка цілісності даних після аварій.

- Забезпечення безперебійного постачання реактивів: створення аварійного запасу; альтернативні постачальники; стандартизовані замінники.

4. Ролі та відповідальність. План визначає, хто відповідає за: активацію плану; прийняття рішень; відновлення обладнання; відновлення IT-систем; комунікацію; документування процесу; координацію дій між відділами.

5. Документ містить детальний опис дій, наприклад:

- Оцінка масштабу пошкоджень.
- Визначення доступних ресурсів.
- Перехід до резервних процесів.
- Перевірка працездатності обладнання.
- Підключення резервних IT-систем.
- Верифікація збережених даних.
- Поступове повернення до нормальної роботи.

6. Перевірка та тестування плану необхідне для: перевірки реалізованості плану; уточнення часових параметрів RTO/RPO; виявлення слабких місць; підготовки персоналу до дій у реальних умовах.

Використовуються наступні методи тестування: навчальні тренування, симульовані аварії, часткове або повне переключення на резервні системи.

План відновлення повинен відповідати політиці безперервності діяльності та узгоджуватись з планом реагування на інциденти й

ґрунтуватись на ВІА і ризик-менеджменті і є частиною системи СУЯ лабораторії [41, 45, 46].

Побудова плану відновлення критично важливих процесів є стратегічно важливою для забезпечення стійкості лабораторії та її здатності працювати в умовах надзвичайних ситуацій. Такий план дозволяє мінімізувати простої, забезпечити безперервність роботи, відновити збереження даних та підтримувати високу якість аналітичних досліджень.

Виконання вимог ISO 22301 гарантує, що лабораторія буде підготовлена до різних сценаріїв та зможе швидко повернутися до стабільної роботи після будь-яких інцидентів.

Висновки до розділу 3

У розділі обґрунтовано підходи до формування системи управління безперервністю діяльності Лабораторії контролю якості лікарських засобів та медичної продукції Держлікслужби України відповідно до вимог стандарту ISO 22301. Доведено, що забезпечення стійкості лабораторії в умовах надзвичайних ситуацій потребує комплексного поєднання системи оповіщення, визначених часових параметрів реагування та документованих планів безперервності й відновлення діяльності.

Встановлено, що ефективна система оповіщення є ключовим інструментом оперативного реагування, який забезпечує своєчасне інформування персоналу, активацію планів реагування та мінімізацію часу простою критичних процесів. Запропонована шкала оцінки рівня загроз дозволяє кількісно оцінювати ризики й обґрунтовано приймати управлінські рішення.

Обґрунтування часових параметрів MTPD, RTO та RPO дало змогу визначити допустимі межі переривання діяльності для критичних лабораторних процесів та сформувавши пріоритети їх відновлення з урахуванням регуляторних вимог і безпеки персоналу.

Розробка планів безперервності бізнесу, управління інцидентами та відновлення діяльності розглядається як безперервний процес, що включає аналіз ризиків, ВІА, розподіл ролей, навчання персоналу та регулярне тестування. Реалізація запропонованих заходів підвищує стійкість лабораторії, забезпечує збереження результатів досліджень і безперервне виконання державних функцій навіть у кризових умовах.

ЗАГАЛЬНІ ВИСНОВКИ

У результаті проведеного дослідження обґрунтовано, що лабораторії контролю якості лікарських засобів є ключовим елементом державної системи забезпечення безпеки, ефективності та відповідності фармацевтичної продукції національним і міжнародним вимогам. Їх діяльність базується на принципах наукової обґрунтованості, стандартизації, об'єктивності та ризик-орієнтованого підходу, що визначає їх стратегічну роль у захисті здоров'я населення та підтриманні стабільності фармацевтичного ринку.

Дослідження підтвердило, що в сучасних умовах зростання воєнних, техногенних, інформаційних і логістичних загроз традиційних механізмів управління якістю недостатньо для гарантування стійкості діяльності лабораторій. У цьому контексті впровадження системи управління безперервністю бізнесу відповідно до вимог міжнародного стандарту ISO 22301 є об'єктивною необхідністю.

Такий підхід дозволяє системно ідентифікувати критичні процеси, оцінювати ризики та наслідки їх порушення, визначати пріоритети відновлення і забезпечувати готовність організації до кризових ситуацій.

У розділі 2 здійснено комплексний аналіз діяльності Лабораторії контролю якості лікарських засобів та медичної продукції Держлікслужби України, який засвідчив наявність ефективної системи управління якістю, що відповідає стандартам, водночас виявив потребу в її доповненні інструментами управління безперервністю діяльності.

У межах розділу 3 обґрунтовано та системно розкрито підходи до забезпечення безперервності діяльності. Запропоновані рішення щодо впровадження BCMS, системи оповіщення, визначення часових параметрів реагування та розробки планів безперервності й відновлення створюють комплексну модель організаційної стійкості.

Таким чином, інтеграція систем управління якістю, ризиками та безперервністю діяльності відповідно до ISO 22301 забезпечує підвищення

стійкості лабораторії, мінімізацію наслідків надзвичайних ситуацій та безперервне виконання державних регуляторних функцій.

Таким чином, реалізація запропонованих заходів забезпечує підвищення стійкості лабораторії до технічних, інформаційних, кадрових і безпекових загроз, мінімізацію часу простою критичних процесів та збереження виконання державних регуляторних функцій навіть в умовах криз і надзвичайних ситуацій. Впровадження системи управління безперервністю діяльності відповідно до ISO 22301 є необхідною умовою надійного функціонування лабораторії та гарантією стабільності державного контролю якості лікарських засобів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Hiles A. The Definitive Handbook of Business Continuity Management. 4th ed. Wiley, 2016.
2. Herbane B. Business Continuity Management: A Crisis Management Approach. Routledge, 2022.
3. ДСТУ EN ISO 22300:2022. Безпека та стійкість. Словниковий запас (EN ISO 22300:2021, IDT; ISO 22300:2021, IDT). Офіц. вид. На заміну ДСТУ EN ISO 22300:2017 (EN ISO 22300:2014, IDT; ISO 22300:2012, IDT) ; чинний від 31.12.2023. URL: https://online.budstandart.com/ua/catalog/doc-page.html?id_doc=116907 (дата звернення: 27.11.2025).
4. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT). Офіц. вид. ; чинний від 01.09.2022. Київ : УкрНДНЦ, 2022. 18 с.
5. Лікарські засоби. Належна виробнича практика. Спеціальні правила належної виробничої практики лікарських засобів передової терапії : Настанова СТ-Н МОЗУ 42-4.9:2020. Вид. офіц. Київ : МОЗ України, 2020. 94 с.
6. Good Manufacturing Practice (GMP) guidelines / European Commission. 2020. Vol. 4. URL: https://health.ec.europa.eu/medicinal-products/eudralex/eudralex-volume-4_en (Date of access: 16.12.2025).
7. ICH Q9. Quality Risk Management / International Council for Harmonisation. 2005. 37 p.
8. Про лікарські засоби : Закон України від 04 квіт.1996 р. № 123/96-ВР. URL: <https://zakon.rada.gov.ua/laws/show/123/96-вр> (дата звернення: 16.12.2025).
9. ISO/IEC 17025:2017. General requirements for the competence of testing and calibration laboratories. Geneva, 2017. URL: <https://www.iso.org/standard/66912.html> (Date of access: 16.12/2025).

10. Elliott D., Swartz E., Herbane B. *Business Continuity Management: A Practical Guide*. 3rd ed. Routledge, 2020.
11. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та настанови (ISO 31000:2018, IDT). Офіц. вид. На заміну ДСТУ ISO 31000:2014. Київ : УкрНДНЦ, 2019. 24 с.
12. Engemann K. J. *The Routledge Companion to Risk, Crisis and Security in Business*. Routledge, 2018.
13. Rouco J. C., Figueiredo P. C. *Business Continuity Management and Resilience*. IGI Global, 2024.
14. Brown T., Warner J. Implementing Business Continuity Planning in Pharmaceutical Companies. *Journal of Business Continuity and Emergency Planning*. 2022. Vol. 16(1). P. 11–19.
15. ISO 22301. Управління безперервністю бізнесу. URL: <https://tms.ua/risk-menedzhment/iso-22301/> (дата звернення: 15.10.2025).
16. Engemann K. J., Douglas M. Henderson *Business Continuity Risk Management: Essentials of Organizational Resilience*. Rothstein Publishing, 2014. 354 p. URL: <https://surli.cc/jppgkq> (Date of access: 16.12.2025).
17. ISO/TR 22330:2018. Security and resilience – Business continuity management – Guidelines for people aspects. Geneva, 2018. 38 p.
18. Ліле К. В. Інтеграція управління ризиками в існуючі фармацевтичні системи управління якістю. *Управління якістю в фармації* : зб. матеріалів XII наук.-практ. конф., м. Харків, 18 трав. 2018 р. Харків : НФаУ, 2018. С. 123–124.
19. Новіков В., Никитюк О. Основи управління ризиками: рекомендації ILAS, ЕА. *Лабораторна справа*. 2020. № 2. С. 10–19.
20. Kambarov J., Ismailov N. Issues of the Impact of Production Risk Management on Industry Development. *Social Science Journal*. 2022. Vol. 13(1). P. 619–626.
21. Інтеграція процесів управління ризиками. Стратегічні ризики. URL: <https://tms.ua/instrumenty-menedzhmenta/sistema-sbalansirovannyh->

pokazatelej-bsc/integraciya-processov-upravleniya-riskami-i-realizacii-strategii/
(дата звернення: 03.11.2025).

22. Risk ranking and filtering risk assessment / Product Quality Research Institute. 2015. URL: https://pqri.org/wp-content/uploads/2015/08/pdf/Risk_Rank_Filter_Training_Guide.pdf (Date of access: 03.12.2025).

23. Massoud M. R., Mensah-Abrampah N. A. Guide to Quality Improvement Methods. WHO Press, 2018. URL: <https://apps.who.int/iris/handle/10665/272357> (Date of access: 16.12.2025).

24. ISO 9001:2015. Quality management systems – Requirements. Geneva, 2015. URL: <https://www.iso.org/standard/62085.html> (Date of access: 16.12/2025).

25. Про затвердження Положення про Державну службу України з лікарських засобів та контролю за наркотиками : Постанова Кабінету Міністрів України від 12 серп. 2015 р. № 647. URL: <https://zakon.rada.gov.ua/laws/show/647-2015-%D0%BF#Text> (дата звернення: 16.12.2025).

26. 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.

27. Москаль Н. В. Комплексний підхід до оцінки безперервності діяльності підприємства. *Економіка та суспільство*. 2024. № 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4409> (дата звернення: 16.12.2025).

28. Guidance for Business Continuity Planning / WHO. 2018. URL: <https://iris.who.int/handle/10665/324850> (Date of access: 16.12.2025).

29. Contingency Planning Guide for Federal Information Systems / M. Swanson et al. 2010. URL: <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf>

(Date of access: 16.12.2025).

30. Державна служба України з лікарських засобів та контролю за наркотиками : офіційний сайт. URL: <https://www.dec.gov.ua> (дата звернення: 16.12.2025).

31. До уваги лабораторій! URL: <https://www.dec.gov.ua/announcement/do-uvagy-laboratorij-4/> (дата звернення: 15.10.2025).

32. Приклад плану забезпечення безперервності бізнесу. URL: <https://tms.ua/blog/pryklad-planu-zabezpechennia-bezperervnosti-biznesu-velykuj-posibnyk/> (дата звернення: 15.10.2025).

33. Українська система громадського здоров'я задає нові регіональні стандарти кризового менеджменту. URL: <https://aph.org.ua/uk/page/3/> (дата звернення: 15.10.2025).

34. Engemann K. J. *The Routledge Companion to Risk, Crisis and Security in Business*. New York : Routledge, 2018. 222 p.

35. Sahebjamnia N., Torabi S. A., Mansouri S. A. Integrated business continuity and disaster recovery planning: Towards organizational resilience. *European Journal of Operational Research*. 2015. Vol. 242(1). P. 261–273. DOI: 10.1016/j.ejor.2014.09.055.

36. Портянко Т. М., Кучеренко В. С. Роль плану забезпечення безперервності бізнесу під час впровадження комп'ютеризованих систем на фармацевтичних підприємствах. *Вчені записки ТНУ ім. В. І. Вернадського. Серія : Технічні науки*. 2020. Т. 31(70), ч. 1, № 2. С. 152–156.

37. Мороз В. М., Мороз С. А. Ризик-менеджмент : навч. посіб. для студентів спец. 281 «Публічне управління та адміністрування». Харків : НТУ «ХП», 2018. 140 с.

38. Кібік О., Слободянюк О., Кузнецова Л. Ризик-менеджмент : навч.-метод. посіб. Одеса : Фенікс, 2024. 84 с.

39. Disaster Recovery and Business Continuity Plan. Exclusive research 2018 from IDC. URL: <https://www.business->

solutions.telefonica.com/media/2207/drp_bcp-white-paper-may18-web.pdf (Date of access: 15.11.2025).

40. Косюга А. В. Класифікація ризиків у підприємницькій діяльності. 2017. URL: <http://repository.hneu.edu.ua/bitstream/123456789/16350/14/518.pdf> (дата звернення: 03.11.2025).

41. Данченко О. Б., Занора В. О. Проектний менеджмент: управління ризиками та змінами в процесах прийняття управлінських рішень : монографія. Черкаси, 2019. 278 с.

42. Bandyopadhyay P. K. Risk Based Approach for Change Management. *Samvad*. 2019. Vol. 18. P. 1–5.

43. Курепін В. М. Оцінка ризиків на підприємстві: планування, практичні дії щодо профілактики виробничого травматизму. *Актуальні проблеми та перспективи розвитку охорони праці, безпеки життєдіяльності та цивільного захисту* : матеріали VI Міжнар. наук.-практ. конф., м. Одеса, 2-3 трав. 2024 р. Одеса : ОДАБА, 2024. С. 64–69.

44. Business Continuity Planning for Life Sciences and Laboratories / Deloitte Insights. 2020.

45. FMEA (Failure Modes and Effects Analysis). URL: <https://www.ifm.eng.cam.ac.uk/research/dmg/tools-and-techniques/fmea-failure-modes-and-effects-analysis/> (Date of access: 03.12.2025).

46. Деренська Я. М. Аналіз світових тенденцій в управлінні ризиками фармацевтичної галузі. *Mechanism of an Economic Regulation*. 2022. Vol. 3-4(97-98). P. 83–89.

ДОДАТКИ



МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

ГРАМОТА

нагороджується

ПАВЛЮК Ольга, ТКАЧУК Інна

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



(Signature)
Олександр КУХТЕНКО

10-11 грудня 2025 р. м. Харків





Міністерство
охорони здоров'я
України

Національний
фармацевтичний
університет



СЕРТИФІКАТ

Цим засвідчується, що

**Павлюк О.В., Ткачук І.В.,
Зборовська Т.В.**

**Науковий керівник:
Крутських 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

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

Всеукраїнська науково-практична конференція з міжнародною участю
«YOUTH PHARMACY SCIENCE»

Орлов Д.І.; Н. к.: Літвінова О.В.	519
Павлюк О.В., Ткачук І.В., Зборовська Т.В.; Н. к.: Крутських Т.В.	521
Паламарчук М.О.; Н. к.: Крутських Т.В.	523
Проняєва К.В., Крутських Т.В.; Н. к.: Зборовська Т.В.	525
Пузирьов Д.А.; Н. к.: Літвінова О.В.	528
Рачковська А.М.; Н. к.: Зборовська Т.В.	529
Сіфоров А.О.; Н. к.: Крутських Т.В.	532
Солодкий В.В., Крутських Т.В.; Н. к.: Зборовська Т.В.	533
Стецюк М.А.; Н. к.: Літвінова О.В.	534
Сулімовська А.А.; Н. к.: Лісна А.Г.	536
Суркова І.П.; Н. к.: Посилкіна О.В.	538
Сьомова Х.О.; Н. к.: Посилкіна О.В.	540
Таможанська Д.О.; Н. к.: Лісна А.Г.	541
Цветаєва К.Є.; Н. к.: Крутських Т.В.	543
Чекалін В.В.; Н. к.: Малініна Н.Г.	545

СЕКЦІЯ 14. СУСПІЛЬСТВОЗНАВСТВО
SOCIAL SCIENCE

Антюхова В.В.; Н. к.: Хіріна Г.О.	548
Губанова А.О.; Н. к.: Хіріна Г.О.	549
Гуренко Д.М.; Н. к.: Садовніков О.К.	550
Забіяка П.О.; Н. к.: Хіріна Г.О.	552
Зражевська К.А.; Н. к.: Хіріна Г.О.	554
Кравцова А.А.; Н. к.: Хіріна Г.О.	555
Матіюк К.І.; Н. к.: Назарко О.І.	556
Миргородська Є.О.; Н. к.: Хіріна Г.О.	557
Немченко Д.С.; Н. к.: Хіріна Г.О.	558
Нікітенко В.Д.; Н. к.: Садовніков О.К.	560
Подовжня С.М.; Н. к.: Хіріна Г.О.	562
Ребріна Г.Ю.; Н. к.: Хіріна Г.О.	563
Сіренко Д.С.; Н. к.: Болдарь Г.Є.	565
Ступак А.О.; Н. к.: Хіріна Г.О.	567
Сухомлин Д.В.; Н. к.: Хіріна Г.О.	569
Сухомлин К.В.; Н. к.: Хіріна Г.О.	571
Федорова С.Д.; Н. к.: Хіріна Г.О.	572
Чичова А.В.; Н. к.: Назарко О.І.	573
Ярошенко О.Я.; Н. к.: Савченко Л.П.	575

готовності медичних установ, формувати стратегічні орієнтири їх розвитку та підвищувати результативність управлінських рішень. Це сприятиме зміцненню конкурентоспроможності закладів охорони здоров'я, підвищенню ефективності використання ресурсів і забезпеченню більш високої якості медичних послуг для населення.

ПІДХОДИ ДО ОРГАНІЗАЦІЇ ДІЯЛЬНОСТІ ЛАБОРАТОРІЇ З КОНТРОЛЮ ЯКОСТІ ВІДПОВІДНО ДО ВИМОГ СТАНДАРТУ ISO 22301

Павлюк О.В., Ткачук І.В., Зборовська Т.В.

Науковий керівник: Крутських Т.В.

Національний фармацевтичний університет, Харків, Україна

Inna059210@gmail.com

Вступ. У сучасних умовах підвищеної нестабільності, ризиків техногенного, природного, військово-політичного та соціального характеру, забезпечення безперервності функціонування лабораторій контролю якості лікарських засобів в Україні набуває стратегічного значення. Перебої в роботі таких лабораторій можуть призвести до затримок у виробництві, втрати даних, невчасного виявлення дефектів фармацевтичної продукції, порушення вимог регуляторних органів та процесів підтвердження відповідності. Міжнародний стандарт ISO 22301 визначає вимоги до системи управління безперервністю бізнесу (СУББ), що дає можливість лабораторіям мінімізувати наслідки кризових ситуацій і гарантувати стабільність контролю якості продукції. Тому реалізація вимог ISO 22301 у діяльності лабораторій є надзвичайно актуальним для сьогодення функціонування лабораторій в Україні.

Мета дослідження. За мету нашого дослідження ми вибрали аналіз ключових вимог ДСТУ EN ISO 22301:2021 та визначення практичних підходів до організації роботи лабораторії з контролю якості лікарських засобів з метою забезпечення її стійкості, безперервності та здатності функціонувати в умовах надзвичайних ситуацій.

Матеріали та методи. У дослідженні нами застосовано: аналіз нормативної бази, зокрема положень ДСТУ EN ISO 22301:2021 «Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги»; метод системного підходу для визначення критичних процесів лабораторії; оцінку ризиків та аналіз впливу на бізнес (BIA) для ідентифікації вразливих місць та потенційних наслідків порушення роботи; експертний аналіз для формування рекомендацій з організації діяльності лабораторії відповідно до вимог стандарту.

Результати дослідження. У ході аналізу встановлено, що впровадження вимог ДСТУ EN ISO 22301:2021 у діяльність лабораторії передбачає комплекс організаційних та технічних заходів, таких як:

- ідентифікація ключових процесів лабораторії (випробування, калібрування, збереження зразків, передання результатів) та аналіз їх впливу на бізнес;
- визначення та оцінка потенційних та наявних загроз за рахунок реалізації ризикорієнтованого підходу;
- створення та підтримка плану безперервності діяльності (BCP), що включає алгоритми дій у разі відключення електропостачання, збою обладнання, порушення логістики матеріалів та інформаційних систем тощо;

Секція 13

«УПРАВЛІННЯ ЕКОНОМІКИ ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ У ФАРМАЦІЇ»

- забезпечення системи запасів, формування фонду резервного обладнання, дублювання інформаційних ресурсів та хмарного збереження даних, фізичного простору збереження зразків та архівів;
- встановлення чіткої системи комунікації під час надзвичайних ситуацій та узгодженої системи оповіщення щодо їх настання;
- організація регулярного навчання персоналу й проведення тестувань аварійних сценаріїв;
- постійний моніторинг ефективності розроблених шляхів реагування на інциденти за рахунок здійснення процесу внутрішнього аудиту.

Застосування цих принципів сприяє підвищенню стійкості лабораторних процесів, скороченню часу простою, покращенню управління ризиками та підвищенню довіри з боку зацікавлених сторін.

Результати проведеного дослідження дозволили сформувати комплексний перелік практичних підходів до організації роботи лабораторії відповідно до вимог стандарту, які стосуються управління безперервністю діяльності.

Ключовим чинником стійкості лабораторії є чітка ідентифікація критично важливих процесів, без яких неможливе виконання базових функцій контролю якості. До таких процесів належать: приймання та реєстрація зразків, проведення випробувань і калібрувань, оброблення та верифікація результатів, їх передавання замовнику, а також зберігання даних і доказових матеріалів. Для кожного процесу визначено рівень допустимого простою та потенційні наслідки його порушення у разі настання надзвичайної ситуації.

Також для забезпечення працездатності лабораторії необхідно здійснювати системну оцінку ризиків та аналіз впливу на діяльність. Нами запропоновано ранжувати ризики за групами:

- технічні (вихід з ладу обладнання, збій у роботі програмного забезпечення);
- інфраструктурні (відключення електроенергії, проблеми з водопостачанням або вентиляцією);
- логістичні (перебої у постачанні реактивів або витратних матеріалів), кадрові (відсутність ключових співробітників);
- ризики фізичної безпеки персоналу та розташування;
- ризики інформаційної безпеки (кіберзагрози, несанкціоновані зміни результатів випробування, тощо).

Результати аналізу продемонстрували, що найбільш критичними для лабораторій є технічні та інфраструктурні ризики, які здатні повністю зупинити процеси випробувань.

Нами сформовано рекомендації щодо створення Плану безперервності діяльності лабораторії. На основі вимог стандарту та специфіки лабораторних процесів запропоновано включити до плану такі обов'язкові елементи:

- опис сценаріїв інцидентів (технічна аварія, пожежа, кібератака, порушення логістики, загроза безпеки персоналу(включаючи реагування на провітрені загрози та терористичні атаки));
- чіткі процедури переходу до аварійного режиму роботи, включно з поділом процесів на критичні та ті, що можуть бути тимчасово призупинені;
- алгоритми резервування обладнання (наприклад, наявність дубльованих спектрометрів, холодильників, джерел безперебійного живлення);
- використання альтернативних шляхів постачання матеріалів та можливість аутсорсингу окремих випробувань до партнерських лабораторій;

- заходи з інформаційної стійкості: хмарні резервні копії даних, дублювання серверів, інструкції щодо відновлення інформаційних систем.

Запропоновано також визначити відповідальних осіб за комунікацію, створити перелік контактних груп (керівництво лабораторії, замовники, акредитуючі органи, аварійні служби) та затвердити шаблони інформаційних повідомлень, що дозволить мінімізувати непродуктивні затримки у прийнятті оперативних рішень.

Реалізація вимог стандарту неможлива без регулярного навчання та тестування персоналу. Необхідно проводити тренування з моделювання аварійних сценаріїв не рідше одного разу на рік, а також організувати інструктаж для нових співробітників з правил реагування на інциденти. Лабораторії, які виконують такі навчання, мають значно вищий рівень готовності до кризових умов та скорочують час простою на 30–40%.

Впровадження системи безперервності діяльності сприяє зменшенню технологічних втрат, підвищенню точності й відтворюваності результатів випробувань, а також стабільної репутації відповідальної лабораторії. Особливо важливо це для лабораторій, що здійснюють обов'язковий державний контроль.

Висновки. Впровадження підходів, визначених стандартом ДСТУ EN ISO 22301:2021, є ефективним засобом забезпечення безперервності роботи лабораторії контролю якості лікарських засобів в умовах непередбачуваних зовнішніх і внутрішніх загроз. Реалізація системи управління безперервністю діяльності дозволяє мінімізувати наслідки інцидентів, забезпечити стабільність критичних процесів та підвищити загальний рівень операційної надійності лабораторії на всіх рівнях виконання нею функцій з контролю якості.

ФОРМУВАННЯ СИСТЕМИ КОНТРОЛЮ ЗА ДОТРИМАННЯМ ВИМОГ НАЛЕЖНОЇ ПРАКТИКИ КУЛЬТИВУВАННЯ У ПРОЦЕСІ ВИРОЩУВАННЯ МЕДИЧНОГО КАНАБІСУ

Паламарчук М.О.

Науковий керівник: Крутських Т.В.

Національний фармацевтичний університет, Харків, Україна

mashap44@gmail.com

Вступ. Становлення сучасної фармацевтичної галузі України супроводжується активним розвитком нормативної, регуляторної та технологічної інфраструктури, необхідної для формування упорядкованої системи культивування рослин роду *Cannabis* для медичного використання та регулювання діяльності суб'єктів господарювання. Ухвалення Закону України № 3528-IX, що набрав чинності 16 серпня 2024 року, започаткувало етап інтеграції медичного канабісу в національну систему виробництва лікарських засобів, що, у свою чергу, зумовлює потребу у впровадженні стандартизованих підходів до забезпечення якості та практик відповідального культивування. Значної актуальності у даному контексті набуває впровадження принципів належної практики культивування та збору вихідної сировини рослинного походження (Good Agriculture and Collection Practice, GACP), що передбачають застосування регламентованих підходів до організації технологічних процесів, спрямованих на отримання високоякісної, безпечної та стандартизованої рослинної сировини для подальшого виробництва лікарських засобів.

Формування ефективної системи контролю за дотриманням GACP у процесі вирощування медичного канабісу – це ключова умова забезпечення стабільності якісних та

ПРОЄКТ (загальний)

ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ
Лабораторія контролю якості лікарських засобів та медичної продукції
Державної служби України з лікарських засобів та контролю за
наркотиками

Підготовлений:

Посада, ПП: _____

Дата: _____

Підпис: _____

Узгоджений:

Посада, ПП: _____

Дата: _____

Підпис: _____

Затверджений:

Посада, ПП: _____

Дата: _____

Підпис: _____

ЗМІСТ

1. Загальні положення
2. Основні терміни та визначення
3. Цілі та область дії Плану
4. Критичні процеси лабораторії
5. Стратегії безперервності бізнесу
6. Управління кризовими ситуаціями
7. Комунікації в умовах НС
8. Захист персоналу та майна
9. Документування та завершення дії Плану
10. Перевірка, оновлення та перегляд Плану

СПИСОК ЗМІН

Версія №	Дата внесення змін	Опис змін	Діє з	Підпис
1.0	_____	Початкова редакція	_____	_____

ЗМІСТ ПОНЯТЬ

ВІА-аналіз – системний процес визначення критичних лабораторних процесів та оцінювання наслідків їх порушення для виконання регуляторних функцій.

Аналіз ризику – процес ідентифікації, оцінювання та пріоритизації загроз, що можуть призвести до зупинки або деградації лабораторної діяльності.

Час відновлення (RTO) – максимально допустимий період часу для відновлення критичного процесу після інциденту.

Інцидент – будь-яка подія, що порушує або може порушити нормальну діяльність лабораторії.

Максимально допустимий період перериву (MTRP) – граничний час, після якого зупинка процесу стає неприйнятною.

Мінімально прийнятна конфігурація (МПК) – мінімальний набір ресурсів, необхідний для виконання критичних функцій лабораторії.

План відновлення бізнесу – сукупність процедур і заходів для відновлення діяльності лабораторії після інциденту.

Критичний процес – процес, зупинка якого призводить до невиконання регуляторних повноважень та загроз безпеці пацієнтів.

ПЛАН ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

План визначає порядок реагування на інциденти та кризові ситуації з метою забезпечення безперервного виконання лабораторією функцій державного контролю якості лікарських засобів і медичної продукції, недопущення неприйнятних репутаційних, соціальних і регуляторних втрат.

1. Способи розповсюдження Плану

План доводиться до:

- керівництва лабораторії;
- відповідальних за критичні процеси;
- членів кризової групи;
- керівників структурних підрозділів.

План зберігається в електронному та паперовому вигляді.

2. Цілі Плану

- забезпечення безперервності критичних лабораторних процесів;
- мінімізація часу простою;
- збереження достовірності результатів досліджень;
- захист життя та здоров'я персоналу;
- виконання вимог законодавства та ISO 22301.

Область дії Плану

План поширюється на всі структурні підрозділи лабораторії, включаючи аналітичні, адміністративні та допоміжні функції.

Список критичних процесів

- приймання, реєстрація та зберігання зразків;
- проведення лабораторних досліджень;
- управління лабораторними даними;
- формування та передача результатів;
- зберігання реактивів і стандартних зразків.

Припущення Плану

- персонал доступний у мінімально необхідній кількості;
- наявні альтернативні джерела енергопостачання;
- резервні копії даних збережені.

Сценарії, для яких розроблений План

- відключення електропостачання;
- кібератака або відмова ІТ-систем;
- пошкодження обладнання;
- обмежений доступ до приміщень;
- дефіцит персоналу.

Тривалість надзвичайного режиму

До повного відновлення функціонування критичних процесів або переходу до альтернативного режиму роботи визначено за відповідним сценарієм.

Стратегія безперервності бізнесу (СББ)

- резервування обладнання та даних;
- пріоритетне відновлення критичних аналізів;
- альтернативні робочі зони;
- гнучкий розподіл персоналу.

Структура управління кризовими ситуаціями (СУНС)

- керівник лабораторії – керівник кризової групи;
- відповідальні за процеси – координатори;
- ІТ та інженерні служби – технічна підтримка.

Введення в дію Плану

План активується рішенням керівника лабораторії або уповноваженої особи.

Правила передачі інформації

Інформація передається за затвердженими каналами зв'язку з фіксацією часу та відповідальних осіб – інструкція з інформування про надзвичайні події.

Відповідальність за управління у надзвичайному режимі
Несе керівник лабораторії або особа, що його заміщує.

Правила зовнішнього та внутрішнього зв'язку

Зовнішні комунікації здійснюються виключно уповноваженими особами Держлікслужби.

Правила співробітництва

Взаємодія з іншими лабораторіями, постачальниками та органами влади здійснюється відповідно до чинних угод та за затвердженням керівника Держлікслужби.

Керівні принципи щодо захисту здоров'я та життя

Пріоритет надається евакуації персоналу, дотриманню вимог охорони праці та санітарної безпеки.

Керівні принципи щодо збереження майна

Забезпечується захист обладнання, зразків, документації та даних (інструкції на відповідний аспект захисту відносно місці їх дислокації).

Методи запису ходу екстрених дій

Усі дії фіксуються у журналі інцидентів та звітах (за затвердженими формами).

Припинення дії Плану

План припиняє дію після відновлення штатного режиму роботи відповідно до інструкції за інцидентом/надзвичайною подією.

Перевірка Плану

План тестується не рідше одного разу на рік за затвердженою програмою навчання.

Оновлення Плану

План переглядається у разі змін у процесах, структурі або ризиках відповідно кількісному та якісному показнику виникнення інцидентів.

Огляд Плану

Огляд здійснюється керівництвом лабораторії з оформленням протоколу.

Алгоритм реагування на відключення електропостачання в лабораторії**1. Виявлення та первинна оцінка (0–5 хв)**

- Фіксація факту відключення електропостачання (візуально або через системи моніторингу).
- Черговий відповідальний повідомляє:
 - керівника лабораторії / координатора BCMS;
 - відповідального за інфраструктуру та ІТ.
- Первинна оцінка:
 - тривалість відключення (короткочасне / невизначене / довготривале);
 - час доби та наявність персоналу;
 - поточні критичні дослідження (аналізи «в процесі»).

2. Забезпечення безпеки персоналу (5–10 хв)

- Перевірка освітлення аварійними джерелами.
- Заборона проведення лабораторних робіт, пов'язаних з:
 - нагріванням;
 - тиском;
 - леткими або токсичними речовинами.
- Забезпечення безпечного стану робочих місць:
 - закриття реактивів;
 - зупинка небезпечних процедур;
 - фіксація стану обладнання.

3. Активація резервного електроживлення (10–20 хв)

- Увімкнення UPS для:
 - критичного лабораторного обладнання;
 - серверів LIMS;
 - холодильників і морозильників зі зразками.
- За тривалого відключення – запуск дизель-генератора (за наявності).
- Перевірка коректності роботи обладнання після переходу на резервне живлення.

4. Захист зразків, реактивів і даних (20–40 хв)

- Контроль температури холодильного обладнання.
- За необхідності:
 - переміщення зразків у резервні камери;
 - використання холодоелементів.
- Перевірка:
 - збереження даних у LIMS;
 - коректності автоматичного збереження результатів.

- Заборона запуску нових аналізів.

5. Управління процесами та комунікація (30–60 хв)

- Рішення керівництва:
 - продовження обмеженої роботи;
 - часткове або повне припинення діяльності.
- Інформування:
 - персоналу;
 - територіального органу Держлікслужби (за потреби).
- Реєстрація інциденту в журналі інцидентів.

6. Відновлення електропостачання

- Поступове підключення обладнання відповідно до інструкцій виробника.
- Перевірка калібрування та стабільності роботи приладів.
- Оцінка придатності результатів досліджень, виконаних до інциденту.
- Відновлення стандартного режиму роботи.

7. Післяінцидентний аналіз (до 24 годин)

- Аналіз причин відключення.
- Оцінка:
 - відповідності фактичного RTO;
 - впливу на критичні процеси.
- Формування звіту про інцидент.
- Визначення коригувальних і запобіжних заходів:
 - збільшення автономного часу UPS;
 - оптимізація пріоритетів живлення;
 - додаткове навчання персоналу.

Очікувані часові параметри

- Максимально допустимий час зупинки (MTPD): **2–4 години**
- Цільовий час відновлення (RTO): **до 1 години**
- Допустима втрата даних (RPO): **0–15 хв**

Результат реалізації алгоритму

- збереження безпеки персоналу;
- мінімізація втрат зразків і результатів;
- дотримання вимог ISO 22301 та ISO/IEC 17025;
- забезпечення безперервності критичних лабораторних процесів.

ЗВІТ ПРО ІНЦИДЕНТ

1. Загальна інформація

- Номер інциденту: _____
- Дата та час виявлення: _____
- Дата та час виникнення (якщо відрізняється): _____
- Підрозділ / локація: _____
- Тип інциденту: _____

2. Опис інциденту

(детальний опис події, умов виникнення, залучених процесів)

3. Критичні процеси, що постраждали

- приймання та реєстрація зразків
- лабораторні випробування
- зберігання зразків / реактивів
- LIMS / IT-системи
- безпека персоналу
- інше: _____

4. Оцінка рівня загрози

- Імовірність (P): _____
- Вплив (I): _____
- Рівень ризику ($R = P \times I$): _____
- Класифікація: низький помірний високий критичний

5. Вжиті дії реагування

- Дата і час початку реагування: _____
- Опис виконаних заходів:
- Активовано план безперервності (BCP): так ні

6. Часові параметри

- Фактичний час реагування: _____
- Фактичний час відновлення (RTO): _____
- Фактична втрата даних (RPO): _____

7. Наслідки інциденту

- втрати зразків
- втрата / пошкодження даних
- затримка досліджень
- порушення вимог стандартів

- загроза персоналу
- відсутні

8. Аналіз причин (Root Cause Analysis)

- Безпосередня причина: _____
- Системна причина: _____

9. Коригувальні та запобіжні дії

- Запропоновані заходи:
- _____
- Відповідальні особи: _____
- Термін виконання: _____

10. Висновки та рекомендації

(оцінка ефективності реагування, пропозиції щодо вдосконалення BCMS)

11. Затвердження

- Відповідальний за BCMS: _____ /підпис/
- Дата: _____
- Керівник лабораторії: _____ /підпис/

Примітка щодо використання

- Звіт формується для кожного значущого інциденту;
- Дані використовуються для аналізу з боку керівництва, перегляду ВІА, ВСР та навчання персоналу;
- Звіти зберігаються відповідно до вимог СУЯ та ISO 22301.