

**МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ
Факультет фармацевтичних технологій та менеджменту
Кафедра менеджменту, маркетингу та забезпечення якості у
фармації**

КВАЛІФІКАЦІЙНА РОБОТА

**на тему: ВПРОВАДЖЕННЯ ВИМОГ СИСТЕМИ МЕНЕДЖМЕНТУ
БЕЗПЕРЕРВНОСТІ БІЗНЕСУ В ДІЯЛЬНІСТЬ
ДИСТРИБ'ЮТОРСЬКОЇ КОМПАНІЇ**

Виконав:
здобувач вищої освіти
2 курсу, групи 1
спеціальності 073 Менеджмент
освітньої програми
Якість, стандартизація та
сертифікація
Дмитро ХАРЧЕНКО

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

Рецензент:
завідувачка кафедри соціальної
фармації НФаУ,
к. фармац. наук, доцент
Аліна ВОЛКОВА

АНОТАЦІЯ

Основні етапи розробки та впровадження системи безперервності бізнесу включають: аналіз бізнес-процесів, ідентифікацію ризиків, розробку політики та планів відновлення, навчання персоналу та постійний моніторинг ефективності.

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 36 найменувань, 4 додатки, і містить 8 рисунків, 2 таблиці. Повний обсяг кваліфікаційної роботи складає 101 сторінку.

Ключові слова: фармацевтичне підприємство, система забезпечення безперервності бізнесу.

ABSTRACT

The main stages of developing and implementing a business continuity system include: business process analysis, risk identification, development of recovery policies and plans, staff training, and ongoing performance monitoring.

Structure and scope of the qualification work: the qualification work consists of an introduction, three sections, general conclusions, a list of references of 36 items, 4 appendices, and contains 8 figures, 2 tables. The full scope of the qualification work is 101 pages.

Keywords: pharmaceutical enterprise, business continuity system.

ЗМІСТ

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ	4
ВСТУП.....	5
РОЗДІЛ 1 ОСОБЛИВОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ	
БЕЗПЕРЕРВНОСТІ БІЗНЕСУ	9
1.1 Актуальність побудови системи управління на принципах стабільної діяльності.....	9
1.2 Положення стандартів системи менеджменту безперервності бізнесу	11
1.3 Інтеграція безперервності бізнесу та управління ризиками в організації. 19	
Висновки до розділу 1	22
РОЗДІЛ 2 АНАЛІЗ ДІЯЛЬНОСТІ СУБ'ЄКТУ ФАРМАЦЕВТИЧНОГО	
РИНКУ	24
2.1 Сучасні загрози безперервності бізнесу бізнес-процесів в діяльності дистриб'юторської компанії в Україні	24
2.2 Діяльність компанії на фармацевтичному ринку	28
Висновки до розділу 2.....	35
РОЗДІЛ 3 ПРАКТИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ДІЯЛЬНОСТІ	
КОМПАНІЇ НА ОСНОВІ СИСТЕМИ БЕЗПЕРЕРВНОСТІ.....	36
3.1 Організація заходів з розробки системи менеджменту	36
3.2 Етапи впровадження системи забезпечення безперервності бізнесу	41
3.3 Розробка проекту плану безперервності та відновлення бізнесу	47
Висновки до розділу 3.....	52
ЗАГАЛЬНІ ВИСНОВКИ	53
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	54
ДОДАТКИ.....	58

ПЕРЕЛІК УМОВНИХ СКОРОЧЕНЬ

BCM – (Business Continuity Management) – управління безперервністю бізнесу.

BCP – (Business Continuity Planning) – планування безперервності бізнесу.

BIA – Business impact analysis

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

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

KRI – Key Risk Indicators (Ключові індикатори ризику)

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

НП – надзвичайна подія

НС – надзвичайна ситуація

ПЗББ – План забезпечення безперервності бізнесу

СЗББ – Система менеджменту безперервності бізнесу

СОП – стандартна операційна процедура

СУЯ – система управління якістю

УЕО – Уповноважений економічний оператор

ФСЯ – фармацевтична система якості

ВСТУП

У кожній компанії є критичні бізнес-процеси, від яких залежить її функціонування. Якщо ці процеси порушуються через надзвичайні ситуації (НС), це може серйозно загрожувати існуванню компанії.

Основною метою управління безперервністю бізнесу (BCM – business continuity management) є забезпечення безперервної роботи критичних процесів і підтримка операцій під час або після екстремальних, надзвичайних (НП) подій у будь якій компанії.

Надзвичайний стан є серйозним викликом. Аутсорсинг, диверсифікація постачальницьких ланцюгів, перебої в постачанні енергії, повні збої в ІТ-системах або пандемії, як Covid-19, та військові дії – це лише кілька прикладів подій, які можуть мати серйозні наслідки як для окремої компанії, так і для всієї галузі чи країни. Надзвичайні ситуації часто виникають несподівано, і всі вони мають одну спільну рису: вони становлять загрозу для існування організації. Важливим є не тільки саме подія, а й її вплив на компанію. Тому управління кризовими ситуаціями та попередження НП є важливими для належної підготовки до створення умов сталого функціонування та захисту компанії.

Управління безперервністю бізнесу є комплексним підходом до організації управління. Компанії повинні розуміти, які їхні критичні процеси і цінності, а також як їх захист від шкідливих впливів може забезпечити їх максимальну надійність. Завдяки систематичному плануванню, комунікації в потрібний час, практичним заходам і здатності ефективно реагувати під час НС, компанії можуть забезпечити довіру важливих клієнтів та партнерів.

Міжнародно визнаний стандарт ISO 22301 створює основу для впровадження системи BCM в організації. Цей стандарт має загальні вимоги, що підходять для будь-яких типів і розмірів організації. Комплексний підхід дозволяє ефективно реагувати на серйозні інциденти та мінімізувати їхні наслідки шляхом визначення критичних процесів і ресурсів, а також

встановлення належного рівня захисту. Окрема увага приділяється ранньому виявленню ризиків, визначенню потенційної шкоди та розробці відповідних заходів для підтримки бізнес-операцій навіть у складних ситуаціях, що допомагає прискорити відновлення роботи компанії [1].

Кожна компанія має на меті надавати високий рівень обслуговування своїм клієнтам та підтримувати надійні стосунки з працівниками, акціонерами та постачальниками. Для забезпечення безперервності доступу до своїх товарів і послуг, компанія повинна розробити політику безперервності бізнесу та аварійного відновлення. З практики відомо, що реагування на кризові ситуації за попередньо розробленим планом є менш витратним, ніж вирішення проблем по мірі їх виникнення.

Впровадження системи менеджменту безперервності бізнесу (СЗББ) відповідно до міжнародного стандарту ISO 22301 є важливим для сучасної діяльності логістичних компаній в Україні. Особливо це стало актуально у країні з військовими діями, а й виправдано для міжнародних партнерів. Наявність такої функціонуючої системи надає організаціям значні переваги в конкурентному середовищі.

Процес управління безперервністю бізнесу включає ідентифікацію потенційних загроз для діяльності компанії, оцінку їхнього впливу на бізнес-процеси в разі виникнення, а також розробку плану відновлення та реагування на інциденти. Це дозволяє скоротити час відновлення і забезпечити захист репутації підприємства [2].

Мета роботи. Виходячи з актуальності питання ми визначили метою досліджень розробку заходів з впровадження вимог системи менеджменту безперервності бізнесу в діяльність дистриб'юторської компанії.

Об'єкт та предмет дослідження. Об'єкт дослідження є діяльність дистриб'юторської компанії, а предметом дослідження є підходи до розробки системи менеджменту безперервності бізнесу в компанії.

Основні завдання роботи:

- Дослідити теоретичну складову впровадження системи

менеджменту безперервності бізнесу.

- Визначити ризики, які можуть вплинути на діяльність фармацевтичного підприємства.
- Окреслити етапи впровадження системи управління безперервністю бізнесу в діючу фармацевтичну компанію.
- Розробити проект плану забезпечення безперервності та відновлення бізнесу.

Методи дослідження:

- Метод аналізу наукових джерел: вивчення статей, книг, дисертацій та інших наукових джерел для узагальнення наявних знань по темі.
- Метод контент-аналізу: систематичний аналіз текстових матеріалів для виявлення тенденцій, шаблонів або основних ідей.
- Експеримент: створення контрольованих умов для вивчення причинно-наслідкових зв'язків між змінними.
- Статистичний аналіз: використання статистичних методів для аналізу великих обсягів даних, виявлення залежностей, трендів або прогнозування.
- Математичне моделювання: побудова моделей, що описують процеси чи явища, для їх подальшого аналізу та прогнозування результатів.
- Порівняльний аналіз: порівняння різних теорій, підходів, моделей чи практик для виявлення їхніх особливостей, переваг та недоліків.
- Аналіз трендів: визначення майбутніх тенденцій на основі аналізу історичних даних та поточних тенденцій.
- Метод вивчення конкретних ситуацій: застосовується для аналізу реальних випадків, що допомагає виявити проблеми і потенційні рішення в конкретних ситуаціях.

Практичне значення отриманих результатів. Результати дослідження будуть використані компанією для створення умов безперервності діяльності

у вигляді плану.

Дослідження і публікації. «Актуальність впровадження безперервності бізнесу в роботу фармацевтичних дистриб'юторських компаній в Україні» Збірник матеріалів I міжнарод. наук.-практ. internet-конференції з міжнар. участю «Актуальні проблеми якості, менеджменту і економіки у фармації і охороні здоров'я», 19 травня 2023 р. (Додаток А) «Огляд ризиків бізнес-процесів дистриб'юторської компанії в розрізі безперервної діяльності» Збірник матеріалів Youth Pharmacy Science: матеріали V Всеукраїнської науково-практичної конференції з міжнародною участю, 10-11 грудня 2024 р. (Додаток Б).

Структура і обсяг кваліфікаційної роботи: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, переліку посилань 36 найменувань, 4 додатки, і містить 8 рисунків, 2 таблиці. Повний обсяг кваліфікаційної роботи складає 101 сторінку, з яких перелік посилань займає 4 сторінки, додатки – 42 сторінки.

РОЗДІЛ 1

ОСОБЛИВОСТІ СИСТЕМИ МЕНЕДЖМЕНТУ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

1.1 Актуальність побудови системи управління на принципах стабільної діяльності

Система менеджменту безперервності бізнесу є критично важливою для забезпечення стабільної та безперебійної діяльності організації, особливо в умовах сучасних викликів та ризиків.

Сучасне бізнес-середовище характеризується підвищеною ймовірністю виникнення різноманітних кризових ситуацій, таких як природні катастрофи, техногенні аварії, кіберзагрози, пандемії та інші непередбачувані події. Відсутність підготовленості до таких ситуацій може призвести до значних втрат та навіть до припинення діяльності компанії.

Забезпечення безперервності критичних бізнес-процесів: СЗББ дозволяє ідентифікувати та захистити ключові процеси та ресурси організації, що є основою для її стабільної роботи. Це включає розробку планів реагування на НС, відновлення після катастроф та забезпечення безперебійної роботи навіть у складних умовах [1, 3].

Організації, які впроваджують ефективні системи безперервності бізнесу, демонструють проактивний підхід до управління ризиками, що підвищує довіру клієнтів, партнерів та акціонерів. Це може стати конкурентною перевагою та сприяти зростанню бізнесу.

В багатьох галузях існують законодавчі та регулюючі вимоги щодо забезпечення безперервності бізнесу. Впровадження СЗББ допомагає організаціям відповідати цим вимогам, уникати штрафів та зберігати ліцензії на діяльність.

Системний підхід до управління безперервністю бізнесу дозволяє організаціям швидко адаптуватися до змін, ефективно реагувати на КС та забезпечувати стійкість у довгостроковій перспективі.

Таким чином, впровадження та підтримка СЗББ є необхідною умовою для забезпечення стабільної та ефективної діяльності організації в умовах сучасних викликів та ризиків [2, 4].

Історичні аспекти виникнення потреби у СЗББ пов'язані з еволюцією економіки, технологій та соціальних структур. Виникнення СЗББ як окремої концепції зумовлене низкою подій, які демонстрували важливість готовності бізнесу до кризових ситуацій.

У XIX столітті, під час промислової революції, підприємства зіткнулися з необхідністю зменшення ризиків виробничих аварій і фінансових криз.

Перша світова війна і Велика депресія 1929 року показали важливість планування для забезпечення стійкості організацій.

У 1960-х роках із розвитком комп'ютерних технологій компанії почали залежати від автоматизованих систем.

Збої в роботі ІТ-інфраструктури стали серйозними загрозами. Наприклад, пожежі в дата-центрах та технічні збої змусили компанії впроваджувати плани відновлення після катастроф [5, 6].

Теракти і стихійні лиха. Наприклад, вибух на заводі Union Carbide у Бхопалі (1984 р.) і аварія на Чорнобильській АЕС (1986 р.) продемонстрували глобальний вплив катастроф. У цей період компанії почали розробляти не лише плани аварійного відновлення, а й комплексні стратегії забезпечення безперервності бізнесу.

Теракти 11 вересня 2001 року стали важливою віхою в розвитку СЗББ. Ця подія продемонструвала, що не лише технічні, а й фізичні загрози можуть паралізувати роботу великих корпорацій та фінансових установ. Компанії почали активно впроваджувати системи управління ризиками, зосереджуючись на відновленні ланцюгів поставок, комунікації з клієнтами та співробітниками, їх безпеці та захисту.

Збільшення кількості регуляторних вимог призвело до створення міжнародних стандартів. У 2012 році був прийнятий стандарт ISO 22301, який встановив чіткі вимоги до побудови СЗББ. Він став основою для

впровадження СЗББ у компаніях різних галузей.

Пандемія COVID-19 та військові дії в Україні і збройні конфлікти в інших країнах яскраво продемонструвала необхідність мати системи, які дозволяють організаціям швидко адаптуватися до змін і продовжувати роботу навіть в умовах глобальних криз., а зростання кіберзагроз також стало однією з ключових причин для посилення уваги до безперервності бізнесу [7, 8].

Історичний розвиток концепції СЗББ показує, що потреба в таких системах виникла через сукупність технологічних, економічних і соціальних змін. Еволюція підходів до безперервності бізнесу є відповіддю на виклики часу, спрямованою на забезпечення стійкості організацій перед непередбачуваними загрозами [9, 10, 11, 12].

1.2 Положення стандартів системи менеджменту безперервності бізнесу

Передовий досвід побудови ефективних СЗББ організації акумульовано у стандартах, нормативних документах, прийнятих у різних країнах: практиках британського інституту безперервності бізнесу (Business Continuity Institute, BCI), міжнародного інституту аварійного відновлення (Disaster Recovery Institute International, DRII) і американського інституту SANS (SysAdmin, Audit, Network, Security Institute), стандартах і специфікаціях Британського інституту стандартів (British Standard Institute, BSI), керівництвах Австралійського національного агентства аудиту (Australian National Audit Office, ANAO); у національних стандартах: Німеччини (BSI 100-4), США і Канади (NFPA 1600, NIST SP 800-34); у відповідному розділі міжнародного стандарту з інформаційної безпеки ISO/IEC 27001; а також у міжнародних стандартах ISO 22301, ISO 22313, ISO/IEC 27031; стандартах і бібліотеках COBIT, ITIL, MOF в частині безперервності діяльності, галузевих стандартах [11].

Система управління безперервністю бізнесу (BCMS) – це структура управління, яка готує організацію, розробляючи стратегії безперервності

бізнесу, щоб виконати свої бізнес-зобов'язання та статутні зобов'язання під час інциденту. Йдеться про оптимізацію доступності послуг і збереження ефективності бізнесу для забезпечення майбутнього зростання ринку. Система управління безперервністю бізнесу покликана виступати в якості каталізатора для прискорення прогресу на шляху від управління безперервністю бізнесу та управління ризиками до створення та впровадження системи управління безперервністю бізнесу відповідно ISO 22301 в організаціях.

Вимоги ISO 22301, які наведені в пунктах 4-10 чітко описують дії з боку організації щодо питання критичності процесів, відповідальності керівництва, визначення різного роду впливів та розробки відносно них заходів захисту для відповідних процесів. Особливістю цього стандарту є створення, на постійній основі, культури безперервності як захисного механізму та принципів і правил роботи кожного співробітника.

Пункт 4 – Контекст: організації повинні розуміти, хто вони, що вони роблять, і які процеси та результати вони повинні підтримувати. Вони також повинні визначити, хто зацікавлений у безперервності операцій – зацікавлені сторони – і які їхні очікування. Також необхідно визначити та задокументувати законодавчі та нормативні вимоги. Маючи цю інформацію, організація встановлює та документує сферу застосування ISO 22301. При визначенні масштабу необхідно враховувати місцезнаходження, місії, цілі, продукти та послуги організації.

Пункт 5 – Лідерство. Для успішного впровадження ISO 22301 організаціям потрібна постійна підтримка та лідерство вищого керівництва. Щоб продемонструвати свою прихильність, вище керівництво організації має розробити, задокументувати та довести до відома політику всередині організації та зацікавлених сторін, надаючи ресурси, спрямовуючи та ведучи працівників, щоб зробити внесок у ефективність ISO 22301. З цією метою організаційні ролі мають бути чітко визначені з обов'язками, повноваженнями та компетенціями для кожної ролі.

Пункт 6 – Планування. Для планування безперервності бізнесу організації повинні розуміти, які збої потенційно можуть виникнути та як ці інциденти впливають на бізнес. Організації повинні враховувати наслідки ризиків, їхній вплив і переваги можливостей щодо їх контексту та планувати дії для їх усунення. Стандарт також зобов'язує організації встановлювати вимірювані цілі BCMS, щоб гарантувати мінімально життєздатні продукти чи послуги, а також дотримання будь-яких законодавчих або нормативних вимог. Ці цілі мають бути задокументовані та повідомлені. Щоб їх досягти, організації повинні мати плани дій у визначені часові рамки з розподілом обов'язків.

Пункт 7 – Підтримка: жодна організація не може просуватися без ресурсів і підтримки. Організації повинні враховувати потреби в ресурсах і надавати їх для досягнення своїх цілей BCMS. Ці ресурси можуть включати інфраструктуру, технології, зв'язок, компетентність, обізнаність та задокументовану інформацію. Стандарт вимагає задокументованих доказів компетентності для визначених ролей, таких як записи про навчання, освіта та професійна підготовка.

Пункт 8 – Експлуатація: цей розділ стандарту описує дії, які слід виконувати для досягнення цілей BCMS і повернення до нормального способу функціонування організації. Основні види діяльності включають:

Проведення та документування аналізу впливу на бізнес (BIA) та оцінки ризиків. BIA має визначити операційні, правові та фінансові наслідки збою. Під час проведення BIA тривалість збою є важливою вхідною інформацією для визначення впливу та, пізніше, часу відновлення. Оцінка ризику дозволяє організації проаналізувати ймовірність порушення її діяльності та ресурсів.

Розробка стратегії безперервності бізнесу Компанії повинні розробити стратегію безперервності, використовуючи інформацію, зібрану в результаті оцінки ризиків та аналізу впливу на бізнес. Стратегія безперервності бізнесу по суті означає розробку варіантів і вибір найбільш відповідних дій,

включаючи пом'якшення, реагування та відновлення.

Створення та впровадження процедур безперервності бізнесу. Від організацій вимагається документувати плани та процедури безперервності бізнесу на основі результатів їхньої стратегії. Плани та процедури повинні містити чіткі та конкретні кроки для вирішення проблем, чітко визначені ролі та потреби в ресурсах, а також організоване спілкування.

Відпрацювання та тестування процедур безперервності бізнесу . ISO 22301 вимагає періодичного тестування планів і процедур, щоб перевірити, чи вони відповідні та ефективні. Результати тестування необхідно переглянути та повідомити для отримання рекомендацій та покращень.

Пункт 9 – Оцінка ефективності: Організації повинні враховувати показники ефективності та метрики; контролювати, вимірювати, аналізувати та оцінювати їх; а потім задокументуйте результати. Заплановані внутрішні аудити слід проводити для вимірювання рівня відповідності стандарту та власним вимогам організації. Програма та результати аудиту повинні бути задокументовані. Нарешті, вище керівництво має переглядати ефективність BCMS через заплановані проміжки часу та документувати результати цих перевірок.

Пункт 10 – Покращення: Організації повинні мати методологію для усунення невідповідностей із зазначенням основних причин і коригувальних дій, а також стратегії для постійного вдосконалення. Стандарт передбачає задокументовану інформацію для оцінки коригувальних дій. Організація повинна розглянути результати аналізу та оцінки, а також результати аналізу керівництва, щоб визначити, чи є потреби чи можливості [12].

Кінцевою реалізацією побудови СЗББ є отримання сертифікату ISO 22301, що є доказом відповідності компанії вимогам стандарту, а також підтвердженням зобов'язань компанії щодо безперервності бізнесу.

Як і всі стандарти ISO, сертифікація ISO 22301 є добровільною діяльністю та залишається вибором організації. Однак у багатьох країнах для деяких галузей бізнесу існують правила сертифікації ISO 22301. Приклади

можна знайти в таких галузях, як енергетика, фінанси, громадський транспорт і логістика. Крім того, як згадувалося раніше, компанії мають багато переваг від впровадження та отримання сертифікації третьою стороною після оцінки.

Кожна організація – велика чи мала – яка впровадила ISO 22301, може звернутися до органу сертифікації для оцінки. Для цього необхідно вибрати орган сертифікації. Вибір акредитованого органу сертифікації є важливим, оскільки органи акредитації мають правила для незалежних органів сертифікації, і це визнано на міжнародному рівні. Органи сертифікації попросять вас надіслати інформацію про організацію, наприклад кількість співробітників і основні процеси, щоб вони могли подати пропозицію на основі тривалості аудиту в людино-днях. Щойно ви приймаєте пропозицію та підписуєте договір з органом сертифікації, програма аудиту починається.

Перед офіційною програмою аудиту проводиться необов'язковий попередній аудит, який називається аналізом прогалин, під час якого орган сертифікації уважніше вивчає існуючу систему управління безперервністю бізнесу та порівнює її з вимогами ISO 22301. Це економить час і гроші, визначаючи ті сфери, які потребують більше зусиль, перш ніж розпочати офіційне оцінювання.

Сертифікаційний аудит проводиться в два етапи. На першому етапі аудиторська група перевіряє, чи відповідаєте ви вимогам ISO 22301, таким як обов'язкові документи та записи, і переглядає впровадження в цілому. Він переглядає поточне управління безперервністю бізнесу в контексті контрольного списку ISO 22301. Якщо аудиторська група виявить розбіжності, це дозволить їх усунути. Якщо ви відповідаєте всім вимогам, аудитори проведуть офіційний аудит готовності до сертифікації.

Після проходження сертифікаційного аудиту ви отримаєте сертифікат ISO 22301, дійсний протягом трьох років. Протягом наступних двох років ви будете проходити контрольні перевірки. Нагляди займають менше часу, як правило, половину тривалості сертифікаційного аудиту. А наприкінці

третього року ви повинні пройти повторний сертифікаційний аудит до закінчення терміну дії сертифікації. Майте на увазі, що перед кожним аудитом, будь то сертифікація, нагляд або повторна сертифікація, провідний аудитор надсилає план аудиту, який включає, які елементи стандарту будуть перевірені та коли. Наприкінці кожного аудиту подається звіт про аудит. Він повинен принаймні містити заяву про відповідність для перевірених областей. Якщо є виявлені факти, які призвели до невідповідності, організації повинні вжити коригувальні дії, щоб зберегти свій сертифікат.

Залежно від масштабу та складності організації та бізнесу тривалість ефективного впровадження різна. Це також залежить від ресурсів і зусиль організації. Загалом для малих і середніх компаній із меншими вимогами відповідності це може зайняти від трьох до шести місяців. Для великих організацій із багатьма територіями або компаній, які мають відповідати багатьом нормам, ця тривалість може становити рік або навіть більше (у таких випадках, як транснаціональні енергетичні компанії чи державні заклади охорони здоров'я). Але яким би не був тип компанії, дуже важливо мати хороший і чіткий план проекту для впровадження ISO 22301. У межах цього терміну також потрібно буде розраховувати на період сертифікаційного аудиту, перш ніж сертифікат буде виданий органом сертифікації [12, 13, 14].

Окрім ISO 22301 (стандарту для управління безперервністю бізнесу), існують й інші стандарти, що сприяють забезпеченню стійкості організацій у разі кризових ситуацій:

1. ISO 27001 – стандарт управління інформаційною безпекою. Допомогає захищати конфіденційність, цілісність і доступність інформації, що є важливим під час кризових ситуацій.

2. ISO 31000 – стандарт управління ризиками. Забезпечує методологію для ідентифікації, оцінки та управління ризиками, що можуть впливати на бізнес-процеси.

3. ISO 22320 – стандарт управління надзвичайними ситуаціями. Визначає принципи реагування на кризові події та координації дій між

різними організаціями.

4. COBIT (Control Objectives for Information and Related Technologies) – фреймворк для управління ІТ-сервісами, який підтримує безперервність критичних інформаційних систем.

5. ITIL (Information Technology Infrastructure Library) – набір практик для управління ІТ-сервісами, які забезпечують стійкість і відновлення бізнесу після аварій чи збоїв.

Кожен із цих стандартів забезпечує специфічні аспекти, що разом створюють комплексний підхід до захисту й підтримки безперервності бізнесу (табл. 1.1.) [15, 16, 17]:

Таблиця 1.1.

Зв'язок ISO 22301 з іншими стандартами

Аспект	Деталі
Пов'язані стандарти	ISO/IEC 27031 (Інформаційні технології. Методи забезпечення безпеки. Керівництво зі створення готовності інформаційно-комунікаційних технологій до забезпечення безперервності бізнесу).
Замінений стандарт	BS 25999-2 був скасований Британським інститутом стандартів і замінений на ISO 22301.
Вимоги до переходу	Компанії, які впровадили BS 25999-2, мали перейти на ISO 22301 до травня 2014 року.
Основні відмінності ISO 22301 від BS 25999-2	1. Більший акцент на визначенні цілей, моніторингу та вимірюванні діяльності. 2. Чіткі вимоги до дій вищого керівництва. 3. Розширені та структуровані вимоги до планування і підготовки ресурсів.
Додаткові стандарти ISO 223	ISO 22300 Соціальна безпека. Термінологія. ISO 22313 Керівництво по застосуванню. ISO 22311 Відеоспостереження. Сумісність вихідних даних. ISO/TR 22312 Технологічні можливості. ISO 22320 Менеджмент надзвичайних ситуацій. Вимоги до реагування на інциденти. ISO 22398 Керівництво з підготовки.

Продовження таблиці 1.1.

Додаткові стандарти ISO 223	ISO 22300 Соціальна безпека. Термінологія. ISO 22313 Керівництво по застосуванню. ISO 22311 Відеоспостереження. Сумісність вихідних даних. ISO/TR 22312 Технологічні можливості. ISO 22320 Менеджмент надзвичайних ситуацій. Вимоги до реагування на інциденти. ISO 22398 Керівництво з підготовки.
Стандарти в процесі розробки	ISO/DIS 22315: Масова евакуація. ISO/NP 22316: Організаційна стійкість. ISO/DIS 22322: Громадське попередження. ISO/DIS 22324: Попереджувальне кольорове маркування. ISO/CD 22325: Оцінка здатності управління в надзвичайних ситуаціях. ISO/DTR 22351: Структура повідомлення для обміну інформацією. ISO/DIS 22397: Рекомендації для встановлення партнерських угод.
Інші міжнародні стандарти управління безперервністю бізнесу	BS 25999, частини 1 і 2 (Британський інститут стандартів). NFPA 1600:2010 (Національна асоціація захисту від пожеж). ASIS SPC.1-2009 (ASIS International). AS/NZS 5050 (Австралія/Нова Зеландія). SS540 (Сінгапурський стандарт). CSA Z1600 (Канадський стандарт). BCP Керівництва (Уряд Японії). NASD 3510/3520 (Національна асоціація фондових дилерів). NIST SP 800-34 (Національний інститут стандартів і технологій). NYSE Правило 446 (Нью-Йоркська фондова біржа).
Зв'язок з ISO 27001	ISO 22301 корисний для сертифікації за ISO/IEC 27001, особливо у частині A.14 (Управління безперервністю бізнесу). Для оцінки ризиків можна використовувати ISO/IEC 27005, ISO 31000 або ISO 31010.

1.3 Інтеграція безперервності бізнесу та управління ризиками в організації

Інтеграція безперервності бізнесу та управління корпоративними ризиками набуває вирішального значення для організацій, що прагнуть ефективно управляти ризиками. Узгодження цих двох стратегічних процесів зміцнює здатність компаній протистояти потенційним загрозам.

Ефективне управління ризиками підприємства (ERM) у поєднанні з надійним планом безперервності бізнесу сприяє зменшенню ризиків. Інтеграція ERM із загальним плануванням безперервності бізнесу надає суттєві переваги, зокрема покращує прийняття рішень, оптимізує розподіл ресурсів і створює прозору систему управління. Це досягається шляхом чіткого розподілу ролей і обов'язків у сфері управління ризиками, що забезпечує підзвітність на всіх рівнях організації. Успішна реалізація ERM потребує стандартизованої інфраструктури для управління ризиками.

Ключовим завданням компаній є розробка уніфікованих стратегій управління різними типами ризиків, таких як активація планів аварійного відновлення або впровадження інтелектуальних маршрутних планів для надзвичайних ситуацій на основі бізнес-правил. Важливо також створити ефективні механізми моніторингу та регулярного звітування для забезпечення постійного вдосконалення.

Поєднання планування безперервності бізнесу з управлінням ризиками підприємства дозволяє компаніям ефективніше виявляти потенційні загрози та приймати обґрунтовані рішення для їх подолання. Такий підхід допомагає уникнути дублювання зусиль і оптимізувати процеси виявлення, оцінки, моніторингу та контролю ризиків. Інтегрована стратегія сприяє визначенню пріоритетів у реагуванні на ризики, враховуючи їхню серйозність та потенційний вплив на бізнес.

З кожним роком інтегрована стратегія стає особливо важливою, адже в сучасну цифрову епоху кіберзагрози та зовнішні масштабні впливи

виникають дедалі частіше. Згідно зі звітом IBM «Вартість витоку даних у 2023 році», у середньому компаніям потрібно 280 днів, щоб виявити порушення безпеки. Це підкреслює критичну необхідність наявності надійних BCP та ефективних практик ERM.

Для успішної інтеграції безперервності бізнесу з управлінням ризиками необхідний детально продуманий, як швейцарський годинник, план. Важливо визначити чіткі ролі та обов'язки, а також забезпечити, щоб кожен у команді мав структуроване розуміння природи ризиків і методів їх мінімізації.

У добре функціонуючій організації кожен співробітник чітко усвідомлює свою роль у процесі управління ризиками — від топ-менеджменту до рядових працівників. Інтеграція цих процесів зазвичай починається з вищого керівництва: саме рада директорів або виконавча команда визначає прийнятний рівень ризику та формулює стратегію його управління.

Ключові індикатори ризику (KRI) є ефективним інструментом раннього попередження, який сигналізує про можливі загрози. Вони дають змогу організаціям діяти на випередження, мінімізуючи потребу в реагуванні на вже виниклі проблеми.

Після розробки KRI важливо донести їх значення до всіх рівнів організації. Кожен співробітник має розуміти, як їхні щоденні обов'язки впливають на загальний стан ризиків і безперервність бізнесу.

Ключову роль у цьому процесі відіграє директор з управління ризиками, який трансформує стратегічні цілі в конкретні операційні завдання. Менеджер з безперервності бізнесу відповідає за наявність і ефективність планів дій у випадку непередбачуваних обставин.

Фахівці з інформаційної безпеки зосереджуються на захисті конфіденційних даних і забезпеченні відповідності нормативним вимогам, що є критично важливим у сучасних умовах зростаючих кіберзагроз.

Профільні фахівці забезпечують роботу всіх систем і фізичного здійснення основних процесів організації.

Першим кроком є визначення наявних та потенційних ризиків, з якими стикається організація – від стихійних лих до кібератак. Після того, як ідентифікували, потрібно проаналізувати ймовірність їх настання та потенційні наслідки впливу на бізнес. Це допоможе визначити, які частини найбільше страждають під час НС.

Оцінка ризиків – це не одноразова дія, а безперервний процес, постійно з'являються нові загрози, а старі стають неактуальними. Після того, як ідентифікували та оцінили ризики, складають план. Описують кроки, які забезпечують безперебійну діяльність та взаємодію з зацікавленими сторонами під час збоїв. Після цього потрібно регулярно тестувати план та тренувати персонал і оновлювати його за потреби. Бути готовим до НС – це не просто швидко діяти при настанні кризи але й бути на крок попереду передбачаючи потенційні проблеми [18, 19, 20, 21, 22].

Таким чином, така компіляція заходів з планування безперервності бізнесу та управлінням ризиками дає організаціям загальний профіль впливів та можливість приймати обґрунтовані рішення і бути більш стійкими при НС.

Після ідентифікації ризиків, настає час впроваджувати заходи з аналізу впливу на бізнес (BIA), які допомагають зрозуміти, як НС можуть вплинути на діяльність, і де потрібно зосередити зусилля та ресурси. Потрібно керувати кожним ризиком: розробити захист, заходи зменшення впливу, прийняти в роботу і далі циклічно з ними працювати та мати звітність щодо зміни обставин виникнення та тяжкості наслідків.

Крім цього потрібно зробити запас ресурсів для реалізації та підтримки планів. Це означає, що має бути кваліфікований (навчений) персонал, який готовий до реагування, коли станеться НС та відповідні інструкції з реагування за кожною окремою подією.

Відстеження ризиків є критично важливим у безперервності бізнесу організації, саме тому моніторинг та звітність є такими важливими. Для цього потрібно розробити методичні підходи до надійної системи відстеження ризиків, оцінки засобів контролю та вимірювання їх

ефективності з плином часу. Кроки відстеження ризиків:

- відстеження всіх ризиків,
- оцінка засобів контролю, чи виконують вони свою роботу,
- стратегії пом'якшення наслідків.

Прозора звітність – це шлях до успішної роботи, щоб усі були в курсі – від топ-менеджерів до стажерів. Ділячись інформацією про поточні ризики та кроки, які робляться для їх зменшення всі тримаються в курсі подій.

Для цього потрібно розробити та технічно оснастити інформаційну панель, яка актуально (в режимі реального часу) демонструє дані про всі НС, з якими стикається організація.

Управління ризиками підприємства та управління безперервністю бізнесу – це дві окремі, але взаємодоповнюючі складові, які сприяють загальній стратегії організації з управління невизначеністю, зниження ризиків і забезпечення стійкості.

ERM зосереджується на виявленні, оцінці та підготовці до потенційних небезпек чи невизначеностей, які можуть негативно вплинути на діяльність організації або її стратегічні цілі. Воно забезпечує всеосяжне уявлення про ризики на всіх рівнях підприємства, допомагаючи приймати обґрунтовані рішення.

У свою чергу, BCM фокусується на підтриманні безперервності критично важливих функцій під час і після деструктивних подій. Це включає планування сценаріїв, що дозволяє мінімізувати наслідки інцидентів і забезпечити оперативне відновлення бізнес-процесів [23, 24].

Висновки до розділу 1

В розділі автор зробив огляд джерел літератури та встановив актуальність СЗББ та її критично важливу функцію для захисту ключових процесів і ресурсів організації в умовах сучасних ризиків (природні катастрофи, техногенні аварії, кіберзагрози, пандемії тощо). Система забезпечує безперебійність операцій навіть у кризових ситуаціях. Компанії з

впровадженими СЗББ отримують підвищену довіру клієнтів і партнерів, що сприяє зростанню бізнесу. У багатьох галузях впровадження СЗББ допомагає відповідати законодавчим і регулюючим нормам, що запобігає штрафам і втраті ліцензій.

Еволюція СЗББ пов'язана з важливими подіями (промислова революція, економічні кризи, техногенні катастрофи, терористичні атаки). Зростання кіберзагроз і пандемія COVID-19 також підкреслили необхідність таких систем. Міжнародні та національні стандарти (ISO 22301, BSI 100-4, NIST SP 800-34 тощо) визначають вимоги до побудови СЗББ. Сертифікація за вимогами ISO 22301 підтверджує відповідність системи стандарту та забезпечує репутаційні й операційні переваги. Процес сертифікації включає попередній аудит, два етапи офіційного аудиту, а також регулярні перевірки протягом трьох років.

СЗББ є невід'ємною складовою успішного функціонування сучасної організації. Її впровадження забезпечує стабільність бізнесу, відповідність регуляторним вимогам і довготривалу конкурентоспроможність. Стандарти ISO 22301 виступають основою для системного впровадження, управління ризиками та забезпечення готовності до будь-яких кризових ситуацій.

РОЗДІЛ 2

АНАЛІЗ ДІЯЛЬНОСТІ СУБ'ЄКТУ ФАРМАЦЕВТИЧНОГО РИНКУ

2.1 Сучасні загрози безперервності бізнесу бізнес-процесів в діяльності дистриб'юторської компанії в Україні

Стандарт BCM є комплексним процесом, що визначає потенційні загрози та їхній вплив на критично важливі бізнес-операції. Його основна мета – забезпечити стійкість компанії, спочатку відновивши її життєздатність, а потім якнайшвидше повернути до нормального функціонування після інциденту, який порушив роботу. Таким чином, система управління безперервністю бізнесу відрізняється від традиційного управління ризиками.

Незважаючи на всі прогнози та плани, надзвичайні ситуації або кризи зазвичай виникають раптово та несподівано, і будь-яка компанія може постраждати. Тому стабільно успішні організації активно дбають про збереження своєї працездатності. Вони передбачають можливі кризи та готуються до конкретних сценаріїв, впроваджуючи організаційні заходи та приймаючи рішення на основі фактів.

У надзвичайних ситуаціях співробітники повинні бути готові діяти зосереджено та структуровано, незважаючи на значний емоційний стрес. Залежно від характеру кризи, може виникнути потреба враховувати вплив зовнішнього середовища на власну компанію під час процесу відновлення. BCM, як складова ризик-менеджменту, також допомагає виконувати превентивні та корпоративні зобов'язання щодо можливих матеріальних і нематеріальних збитків.

Варто зазначити, що управління безперервністю бізнесу є реактивним підходом, який фокусується на швидкому реагуванні на фактичні збої в роботі організації в режимі реального часу. Натомість стійкість бізнесу полягає в проактивній здатності суб'єкта господарювання протистояти, відновлюватися та адаптуватися до широкого кола проблем, збоїв і змін.

Таким чином, управління безперервністю бізнесу полягає у реагуванні на фактичні перерви, тоді як стійкість бізнесу вимагає послідовного планування сценаріїв і регулярного навчання для підготовки до ймовірних типів порушень [25, 26, 27, 28, 29, 30, 31, 32, 33, 34, 35, 36].

У 2020 році Allianz Group опублікувала дослідження "Барометр ризиків", яке базується на опитуванні понад 2 700 експертів із більш ніж 100 країн (рис. 2.1.).



Рис. 2.1 Барометр ризиків Allianz 2020

Вперше кіберінциденти були визнані найважливішим бізнес-ризиком у світі, отримавши 39% відповідей.

Ризик переривання бізнесу (включаючи порушення ланцюга постачання) посів друге місце з 37% відповідей, залишаючись провідним викликом для компаній, особливо в Німеччині.

Ризики, пов'язані зі зміною клімату, піднялися на сьоме місце з 17% відповідей.

Компанії висловлюють занепокоєння щодо загроз та пошкодження майна внаслідок екстремальних погодних явищ.

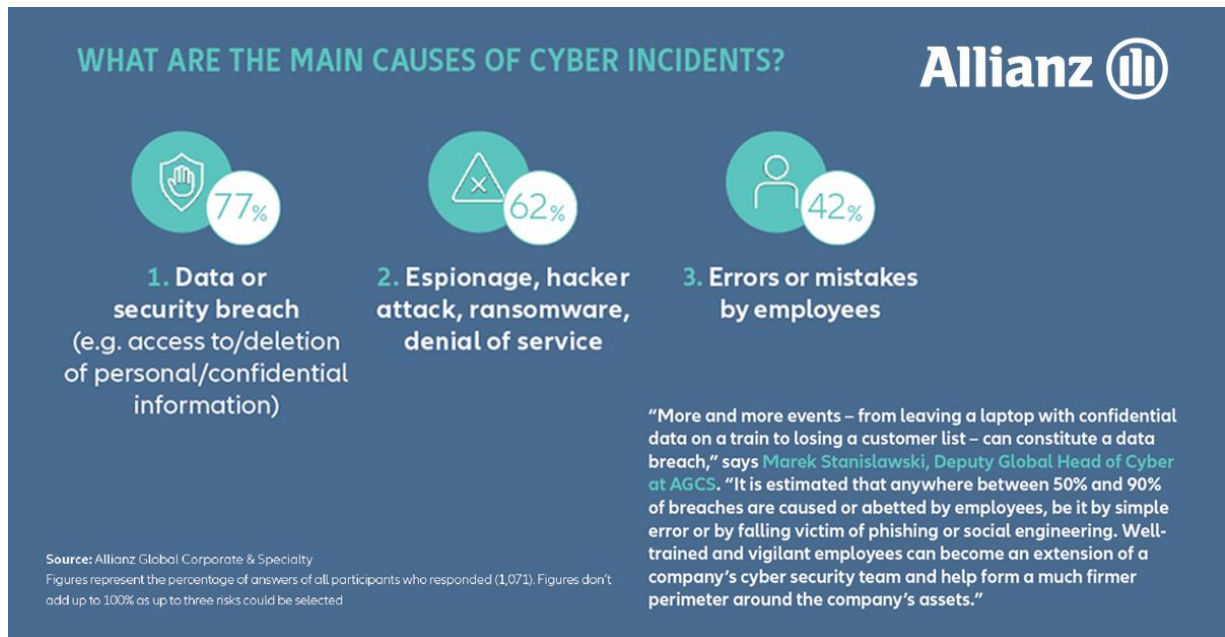


Рис. 2.2 Основні причини кіберінцидентів

Які основні причини кіберінцидентів: порушення даних або безпеки (наприклад, доступ до/видалення особистої або конфіденційної інформації) – 77%, шпигунство, хакерські атаки, програми-вимагачі, відмова у наданні послуг – 62%, помилки або недоліки співробітників – 42%

За оцінками, від 50-90% порушень викликані або їм сприяють співробітники, чи то через прості помилки, чи через те, що вони стають жертвами фішингу або соціальної інженерії. Добре підготовлені та уважні співробітники можуть стати продовженням команди кібербезпеки компанії та створити значно сильніший захисний периметр навколо активів компанії [25, 26, 27, 28, 29].

Загрози безперервності бізнесу в Україні та інструменти їх мінімізації можуть бути наступними:

1. Втрата персоналу: інвентаризація навичок персоналу, перехресне навчання, документування процесів, планування кадрового резерву, залучення аутсорсингових послуг для роботи персоналу.
2. Втрата основних засобів чи доступу до них:

- внутрішнє переміщення персоналу (переміщення персоналу в інше приміщення, що належить організації),
- віддалена робота (забезпечення можливості роботи персоналу з дому або інших місць (коворкінги, антикризові центри),
- релокація бізнесу (переміщення суб'єкта господарювання (повне або часткове) в більш сприятливе географічне середовище з метою продовження його функціонування).

3. Перебої енергопостачання: забезпечення резервного електропостачання.

4. Збої та втручання в інформаційно-технологічні системи:

- підтримка тієї самої технології в різних місцях (використання однакових технологічних рішень, таких як програмне забезпечення, обладнання та інфраструктура, в декількох локаціях),
- зберігання старого обладнання (створення резерву старого обладнання для екстреної заміни або запасних частин),
- кібербезпека (заходи, спрямовані на захист комп'ютерних систем, мереж та даних від несанкціонованого доступу, використання, порушення їх роботи або знищення (хмарне резервне копіювання, шифрування, контроль доступу тощо).

5. Порушення цілісності ланцюгів постачання:

- диверсифікація постачальників (співпраця з декількома постачальниками для отримання товарів або послуг),
- визначення резервних маршрутів (пошук альтернативних логістичних сполучень та способів доставки),
- створення резервних запасів (зберігання запасів ключових товарів або компонентів),
- вимога підтвердження здатності безперервності (заохочення або вимога до постачальників мати підтверджену здатність безперервності бізнесу) [18, 19, 20, 25, 26, 27, 28, 29, 30].

Наявність плану безперервності бізнесу стає все більш важливою через

зростання ризиків, таких як пандемії, проблеми з ланцюгами поставок, витоки даних та екстремальні погодні умови, політичні та військові дії. Однак, згідно з опитуванням 2020 року, 51% компаній не мали такого плану під час пандемії.

Малі та середні підприємства часто не мають плану через обмеження в часі, бюджеті та ресурсах. Відсутність пов'язана з високим ризиком: 25% підприємств не відновлюються після катастрофи, а 90% з них закриваються протягом року, якщо переривання діяльності триває понад п'ять днів.

2.2 Діяльність компанії на фармацевтичному ринку

Компанія є глобальним лідером у біофармацевтичній сфері, з основною метою об'єднання науки, технологій і таланту для боротьби з хворобами.

Її стратегічна мета полягає в тому, щоб до 2031 року позитивно вплинути на здоров'я 2,5 мільярда людей, активно розвиваючи інноваційні підходи до лікування та профілактики хвороб.

Серед основних напрямків діяльності — розробка вакцин, спеціалізованих і загальних препаратів, а також фокус на науці про імунну систему та новітніх технологіях.

Компанія інвестує в чотири терапевтичні області: інфекційні захворювання, ВІЛ, респіраторні/імунологічні проблеми та онкологію.

У 2023 році компанія зафіксувала £30,3 млрд від продажу ліків і вакцин, має 71 препарат у розробці та просуванні. Крім того, вона має широку низку вакцин для боротьби з інфекційними захворюваннями, зокрема від менінгіту, оперізувального лишая, грипу, поліомієліту та інших.

Спеціалізовані лікарські засоби охоплюють боротьбу з інфекціями, респіраторними захворюваннями і ВІЛ, а також нові розробки в онкології.

Загальні препарати включають понад 150 продуктів, що охоплюють антибіотики та інгалятори для лікування астми та ХОЗЛ, які значно покращують якість життя мільйонів людей у світі.

Основні пріоритети компанії включають інновації, продуктивність та

довіру. Вона зосереджена на новітніх технологіях для ефективного і швидкого наукового прогресу, а також ставить завдання щодо зростання і підвищення ефективності до 2026 року, за рахунок сприяння стабільного розвитку бізнесу.

Важливим аспектом є відповідальність перед зацікавленими сторонами, де компанія підтримує принципи прозорості та довіри, дотримуючись етичних стандартів. Вона активно підтримує глобальні ініціативи, такі як дослідження антибіотикорезистентності, і приділяє велику увагу програмам вакцинації, особливо в країнах з низьким рівнем щеплення.

Компанія також реалізує кілька важливих дослідницьких проєктів у галузі респіраторної медицини, онкології та епідеміології, зокрема співпрацюючи з міжнародними науковими організаціями. Вона активно підтримує освітні програми щодо вакцинації та сприяє розвитку медичного діалогу, щоб покращити доступ до сучасних медичних знань.

Компанія надає різноманітні послуги та продукти, серед яких: посередництво при укладанні угод з виробниками, транспортування фармацевтичного обладнання, а також послуги з реєстрації та регуляторної підтримки. Організаційна структура наведена в Додатку В Компанія здійснює постачання активних фармацевтичних інгредієнтів, допоміжних речовин та готових лікарських форм від провідних європейських виробників. Це створює особливе навантаження на постійність логістичної діяльності та приводить до залучення інших суб'єктів господарювання при транспортуванні продукції, і відповідно, маємо додаткові ризики взаємодії.

Політика та цілі якості охоплюють наступні ключові пункти:

1. Усі зусилля співробітників компанії орієнтовані на забезпечення високої якості та своєчасного виконання робіт відповідно до встановлених процедур.

2. Компанія активно займається відбором кадрів і підтримує підвищення їх професійної кваліфікації через планові навчальні програми. Керівництво компанії очікує, що співробітники поділяють її політику і

застосовують її в повсякденній практиці. Всі працівники несуть відповідальність за забезпечення якості у своїх функціональних областях, прагнучи постійно вдосконалювати свою роботу та сприяти організаційному розвитку.

3. Компанія активно працює над поліпшенням захисту навколишнього середовища та природних ресурсів, зосереджуючи зусилля на запобіганні забрудненням. Вона сприяє використанню екологічно чистих методів та вимагає від своїх контрагентів дотримання екологічно безпечних практик.

4. Компанія зобов'язується підвищувати безпеку робочих місць, забезпечуючи відповідність юридичним вимогам, що стосуються екологічних аспектів та професійних ризиків.

5. Компанія прагне постійно вдосконалювати програми митної безпеки, зберігаючи статус уповноваженого економічного оператора (УЕО) відповідно до європейських регламентів, зокрема Регламенту Європейського парламенту і Ради № 648/2005 та змін до Митного кодексу Спільноти.

6. Компанія активно підтримує відповідність вимогам SÚKL (Чеський державний інститут контролю лікарських засобів) та ÚSKVBL (Чеський інститут державного ветеринарного контролю біопродуктів та фармацевтичних засобів) щодо зберігання та продажу фармацевтичних препаратів.

Документообіг компанії представлений в 5-ти рівневій ієрархії, яка наведена на рисунку 2.3.



Рис. 2.3. Ієрархія документів компанії

Вивчивши підходи фахівців Інституту безперервності бізнесу (BCI), Міжнародного інституту відновлення після катастроф (DRII) та інших наукових джерел і нормативних актів, можна виділити два ключові напрями розвитку концепції СЗББ:

- Планування безперервності бізнесу (ПББ).
- Відновлення бізнес-процесів після аварій та катастроф.

План забезпечення безперервності бізнесу (ПЗББ) – це задокументований набір процедур і механізмів, розроблений і підтримуваний для забезпечення можливості організації продовжувати виконання критично важливих функцій під час інциденту [35, 36]. Головна мета ПЗББ – забезпечення актуального стану структур, операцій та ресурсів, необхідних для стабільного функціонування організації у надзвичайних ситуаціях.

Сучасний підхід до СЗББ спрямований на всю організацію, акцентуючи увагу на критично важливих бізнес-процесах, і виходить за межі виключно інформаційних систем [34, 35, 36].

Існує декілька моделей життєвого циклу СЗББ. За однією з них він складається з двох основних етапів (рис. 2.4):



Рис. 2.4 Життєвий цикл систем ЗББ

Планування: аналіз загроз, оцінка ризиків, ідентифікація критичних

ресурсів, розробка документації, навчання персоналу.

Реалізація: впровадження превентивних заходів, організація засобів для відновлення критичних процесів.

Деякі дослідники пропонують чотирьохетапну модель, яка включає: планування, впровадження, тестування та підтримку. Інші моделі виділяють стадії аналізу, проектування, тестування й підтримки [31, 32].

Компанія вже має систему управління якістю, яка структурує діяльність на організаційні, виробничі та дослідницькі процеси основної діяльності

Процесний підхід у СУЯ дозволяє визначити інформаційні та управлінські зв'язки, відповідальність, повноваження та ресурси, вдосконалюючи існуючу систему управління.

Процеси поділяються на:

Управлінські: забезпечення конкурентоспроможності, стратегічне планування, управління фінансами, якістю, маркетингом, аудитом.

Основні: задоволення клієнтів (консультації, лабораторні дослідження, виробництво, реалізація).

Допоміжні: забезпечення ресурсів, інфраструктури, юридична підтримка, закупівлі.

Усі процеси контролюються шляхом оцінювання результативності, корегувальних дій та визначення повноважень і відповідальності.

Підприємницька діяльність у ринкових умовах завжди супроводжується ризиками, тобто можливістю отримання негативних результатів. Ризик розглядається як сукупність імовірних економічних, політичних і соціальних наслідків, пов'язаних із реалізацією певних рішень.

Компанія постійно перебуває у ситуації ризику. Оцінка й аналіз ризиків є важливими інструментами для керівників, зокрема у фармацевтичній діяльності, де управління ризиками для якості лікарських засобів (ЛЗ) є пріоритетом.

Quality Risk Management (QRM) – це систематичний процес оцінювання, ідентифікації, контролю та аналізу ризиків для якості ЛЗ

протягом усього життєвого циклу лікарського засобу.

Вибір методу оцінювання залежить від характеру ризику, доступності інформації та необхідної точності оцінки ймовірності подій. Аналіз існуючих методів виявив, що вони здебільшого підходять для окремих видів ризиків, що суперечить системному підходу. У зв'язку з цим була розроблена трирівнева система оцінки, яка враховує внутрішні ризики елементів організації, її підсистем і загальні ризики підприємства.

Нормативно-правова база фармацевтичної діяльності передбачає обов'язкову оцінку ризиків критичних процесів, що впроваджено в системі якості. Доцільно проводити ідентифікацію та ранжування ризиків, які не охоплюються діючою системою, критично впливають на безперервність виконання господарської діяльності.

СЗББ є складовою ризик-менеджменту. Ризики поділяють на залежні й незалежні від діяльності компанії. Незалежні ризики, такі як коливання валютного курсу чи погашення заборгованостей, тісно пов'язані з бізнес-процесами.

Організацію доцільно розглядати як систему, що складається з виробничо-технічної, кадрово-інтелектуальної, фінансової, комерційної, інноваційно-інвестиційної та інформаційної підсистем:

Виробничо-технічна підсистема. Ризики: вихід із ладу обладнання, порушення технологій, низька якість продукції.

Фінансова підсистема. Ризики: втрата фінансових ресурсів, зниження стійкості, невиконання зобов'язань.

Комерційна підсистема. Ризики: недопостачання сировини, зміна умов постачання, збої в дистрибуції.

Кадрово-інтелектуальна підсистема. Ризики: некомпетентність персоналу, втрата ключових співробітників, розголошення інформації.

Інформаційна підсистема. Ризики: недостовірність даних, невідповідність нормативним вимогам.

Політична підсистема. Нормативно-правова база та політичні рішення

та взаємодії між країнами [25].

Таблиця 2.1.

Елементи системи та їхні ризики

Елемент системи (організації)	Об'єкт ризику	Ризики
Ресурси праці	- Будинки та споруди - Обладнання та устаткування - Засоби пересування - Електронно-обчислювальна техніка	- Поломка обладнання - Аварії, вибухи, пожежі - Крадіжки чи навмисне пошкодження - Простої обладнання - Неефективне використання об'єктів - Випуск неякісної продукції в реалізацію
Предмети праці	- Сировина, матеріали	- Втрата чи пошкодження продукції - Несвоєчасність виплат - Несвоєчасні поставки - Протиправні дії осіб - Зростання цін на сировину, матеріали
Персонал	- Відносини в колективі - Організаційний клімат	- Страйки - Звільнення працівників - Втрата працівників через хворобу чи смерть - Зниження продуктивності праці - Неефективне управління - Розголошення комерційної таємниці
Інформація	- Матеріали архіву - Документи - Електронні бази даних - Інформація на електронних носіях	- Втрата інформації - Порушення цілісності інформації - Несвоєчасне надходження інформації - Витік і розголошення інформації - Надходження та використання недостовірної інформації

Продовження таблиці 2.1.

Фінанси	- Дохід і прибуток підприємства - Власний капітал - Довгострокові та поточні зобов'язання - Грошові засоби - Дебіторська заборгованість - Цінні папери	- Неефективне використання фінансових ресурсів - Неплатоспроможність - Зниження фінансової стійкості - Ліквідність - Валютні коливання - Інфляція - Неповорнення зобов'язань
---------	---	--

Для оцінки ступеня ризиків підсистем організації рекомендується використовувати: метод аналогій; експертний аналіз; аналітичний підхід; «Дерево рішень»; аналіз фінансового стану підприємства. Рівень ризиків слід визначати на основі розробленої системи індикаторів, яка враховує специфіку діяльності організації.

Висновки до розділу 2

СЗББ є ключовим інструментом для забезпечення стійкості компанії в умовах непередбачуваних криз. Основними загрозами, що впливають на безперервність бізнес-процесів дистриб'юторських компаній в Україні, є втрата персоналу, перебої енергопостачання, збої в інформаційних системах, порушення ланцюгів постачання, а також кіберінциденти. Аналіз сучасних досліджень і статистики свідчить про значний вплив кіберінцидентів на діяльність компаній. Крім того, ризики переривання бізнесу, включаючи порушення логістичних ланцюгів, займають провідні позиції серед загроз.

Інструменти мінімізації ризиків включають планування кадрового резерву, запровадження віддаленої роботи, впровадження резервного електропостачання, використання кібербезпеки та диверсифікацію постачальників. Також важливими є сценарне планування, навчання персоналу та розробка чітких планів реагування на кризи. Стабільна діяльність компаній залежить від здатності впроваджувати активні заходи з підготовки до НС і швидко адаптуватися до змін.

РОЗДІЛ 3

ПРАКТИЧНІ ПІДХОДИ ДО ФОРМУВАННЯ ДІЯЛЬНОСТІ КОМПАНІЇ НА ОСНОВІ СИСТЕМИ БЕЗПЕРЕРВНОСТІ

3.1 Організація заходів з розробки системи менеджменту

Планування безперервності бізнесу охоплює всю організацію. Кожен відділ відповідає за підготовку як поточних, так і комплексних планів безперервності для своїх бізнес-операцій. Кожен такий план повинен містити відповідні процедури, що визначають процес забезпечення наявності та доставки необхідних товарів, а також відповідальних осіб і інструменти для виконання вимог щодо відповідності.

Ефективність впровадження СЗББ на підприємстві можна підтвердити через здатність організації продовжувати роботу в разі збоїв у роботі своїх систем. Це також можна оцінити за результатами аудиту та відповідності нормативним вимогам відносно функціонування. Особливо така діяльність актуальна для організацій, які співпрацюють або є частиною міжнародної діяльності в певній сфері.

Звичайно, створення та ефективна реалізація такої системи неможлива без значних фінансових, людських і тимчасових ресурсів, що доступні не кожній компанії.

Переваги планування безперервності бізнесу:

- Покращення сприйняття та репутації компанії: ВСП демонструє проактивний підхід і готовність до непередбачених ситуацій, що формує у клієнтів та громадськості позитивне враження і довіру до компанії, перетворюючи їх на лояльних клієнтів.
- Підвищення морального духу працівників: ВСП дає співробітникам впевненість і гордість за свою компанію, мотивуючи їх до підвищення продуктивності та лояльності.
- Зміцнення відносин з акціонерами та зацікавленими сторонами: Наявність ВСП підвищує довіру акціонерів і партнерів до компанії, що спри-

яє їхньому подальшому інвестуванню та співпраці.

- Підвищення загальної ефективності організації: У разі кризи або порушення бізнес-процесів наявність ВСР дозволяє швидко і ефективно реагувати, мінімізуючи втрати та витрати.

Оскільки компанія працює відповідно до вимог Належної практики дистрибуції, впровадження СЗББ у функціонуючу систему якості та поєднання вимог двох стандартів буде доцільним кроком.

До зацікавлених сторін у впровадженні СЗББ можна віднести головне керівництво компанії, заводи-виробники, які є постачальниками, а також найманий персонал.

СЗББ, як і будь-яка система управління, базується на стратегічному плануванні. Її основою є розробка плану безперервності бізнесу (BCP) та плану аварійного відновлення (DRP) для екстрених ситуацій. Стратегія створюється з урахуванням методів управління ризиками (RM). Упровадження СЗББ в організації передбачає комплексний, багаторівневий підхід, що включає впровадження технічних і програмних рішень, регулювання дій, розподіл обов'язків, а також навчання персоналу.

Чотири основні етапи розробки плану безперервності бізнесу:

1. Аналіз бізнес-впливу для визначення критично важливих функцій і процесів, а також ресурсів, які їх підтримують.
2. Визначення, документування та реалізація заходів для відновлення критичних функцій і процесів.
3. Формування команди з безперервності бізнесу та створення відповідного плану для керування бізнесом.
4. Проведення тренінгів, тестування та навчання, щоб перевірити стратегії відновлення та вдосконалити план.

Для максимальної ефективності план безперервності бізнесу потрібно інтегрувати в щоденні операції. Це живий документ, який потребує регулярного перегляду та оновлення. Для виявлення недоліків і підвищення кваліфікації персоналу слід проводити регулярні тестування, навчання та

аудити.

Стандарт ISO 22301 ґрунтується на принципі TQM («запобігати краще, ніж виправляти») і використовує модель PDCA (plan – do – check – act: «плануй – виконуй – перевіряй – дій»). Планування СЗББ охоплює розробку політики безперервності бізнесу, визначення цілей, засобів управління, процесів і процедур для запобігання збоїв або їх швидкого усунення, забезпечуючи безперебійну роботу організації.

Розробка та впровадження фармацевтичної системи якості включає інтеграцію Системи менеджменту безперервності бізнесу (СЗББ) у чинну систему якості. Нижче наведена послідовність розробки Плану безперервності бізнесу (BCP):

Plan – визначення сфери дії плану, розробка політики та цілей СЗББ.

Першим кроком є визначення сфери і цілей плану, а також припущень, які будуть враховані під час його реалізації. На цьому етапі також здійснюється бюджетування програми, враховуючи витрати на дослідження, тренінги та інші послуги.

При формуванні комісії з безперервності бізнесу створюється структура управління, до якої входять співробітники з чітко визначеними ролями, обов'язками та кваліфікацією. Розробляються посадові інструкції для членів комісії.

Аналіз бізнес-впливу (BIA) проводиться на основі зібраних даних створюється карта ключових бізнес-процесів, що відображає можливі збої та їх вплив на бізнес. Результатом є модель причинно-наслідкових зв'язків між бізнес-процесами, інформаційними потоками та рівнем збитків.

Аналіз ризиків починається з ідентифікації потенційних загроз безперервності, оцінюється ймовірність їх виникнення, і визначаються заходи для їх мінімізації.

При визначенні стратегії та плануванні заходів розробляються дії спрямовані на відновлення критичних функцій у надзвичайних ситуаціях, визначаються часові межі та ресурси, необхідні для відновлення.

До – розробка та документація.

Створюється проєкт плану безперервності, який підлягає тестуванню та доопрацюванню до остаточної версії. План регулярно оновлюється відповідно до змін у бізнесі.

Check – впровадження та тестування.

План впроваджується шляхом навчання персоналу та інформування зацікавлених сторін. Тестування здійснюється через сценарії та вправи для перевірки ефективності плану і внесення необхідних коректив.

Act – коригування та вдосконалення.

Програма коригується на основі результатів тестування, змін у бізнес-процесах, введення нових технологій або змін у складі команди. План оновлюється для відображення цих змін.

На початковому етапі впровадження СЗББ передбачається формування комісії, до складу якої увійдуть представники ключових структурних підрозділів, що відповідають за основні бізнес-процеси. Пропонуються посади:

1. Генерального директора
2. Заступника генерального директора з питань якості
3. Менеджера відділу збуту
4. Менеджера з реєстрації лікарських засобів
5. Представника IT-відділу

Для реалізації цього етапу підприємство має видати наказ про створення комісії з безперервності бізнесу та запровадити процедуру щорічної ротації її складу та навчання.

Типова структура команди ВСР компанії та її обов'язки:

Голова комісії з безперервності бізнесу (Генеральний директор)

Відповідає за загальне керівництво СЗББ, розробку політики ВСР, бюджетування, моніторинг і координацію всіх заходів, пов'язаних із впровадженням ВСР (проведення ВІА, забезпечення якості, організація навчання тощо). Також визначає пріоритетні напрями розвитку СЗББ.

Представник керівництва з якості (Заступник генерального директора з питань якості) забезпечує стабільність і надійність потоку даних для ВСР. Його основні обов'язки:

- Керівництво процесом впровадження та управління СЗББ;
- Контроль дотримання вимог СЗББ усіма співробітниками.
- Представники підрозділів (Менеджер відділу збуту, Менеджер з реєстрації ЛЗ, Представник ІТ-відділу).

Вони є основними джерелами інформації про роботу своїх бізнес-процесів і сприяють аналізу даних для ВСР. Їхні обов'язки включають:

- Підтримку процесу впровадження та розвитку СЗББ;
- Забезпечення ресурсами для функціонування СЗББ;
- Перегляд і оновлення цілей СЗББ відповідно до бізнес-цілей;
- Підтримку інформаційної безпеки як ключового аспекту роботи підприємства.

Кожен співробітник зобов'язаний підтримувати належний рівень СЗББ у межах своїх функціональних обов'язків і повноважень. Вони повинні виконувати вимоги політики, законодавчих і внутрішніх норм, а також несуть відповідальність за їх порушення згідно з чинним законодавством України та внутрішніми регламентами підприємства.

Загальна схема виконання діяльності за посадами може виглядати так:

1. Розробка політики та цілей СЗББ – Голова комісії СЗББ
2. Внесення змін до Настанови з якості (визначення управління СЗББ), навчання персоналу – Представник керівництва з якості
3. Проведення аналізу ризиків для критичних процесів – Комісія на чолі з Головою
4. Розробка стандартних операційних процедур ББ, навчання персоналу – Комісія на чолі з Головою
5. Внесення коригувань в діючі СОП відповідно до сфери охоплення СЗББ – Представник керівництва з якості
6. Розробка «План дій в разі екстрених ситуацій», навчання

персоналу – Представник керівництва з якості

- 7. Розробка Плану ББ – Комісія на чолі з Головою
- 8. Аудит СЗББ – Новостворена комісія

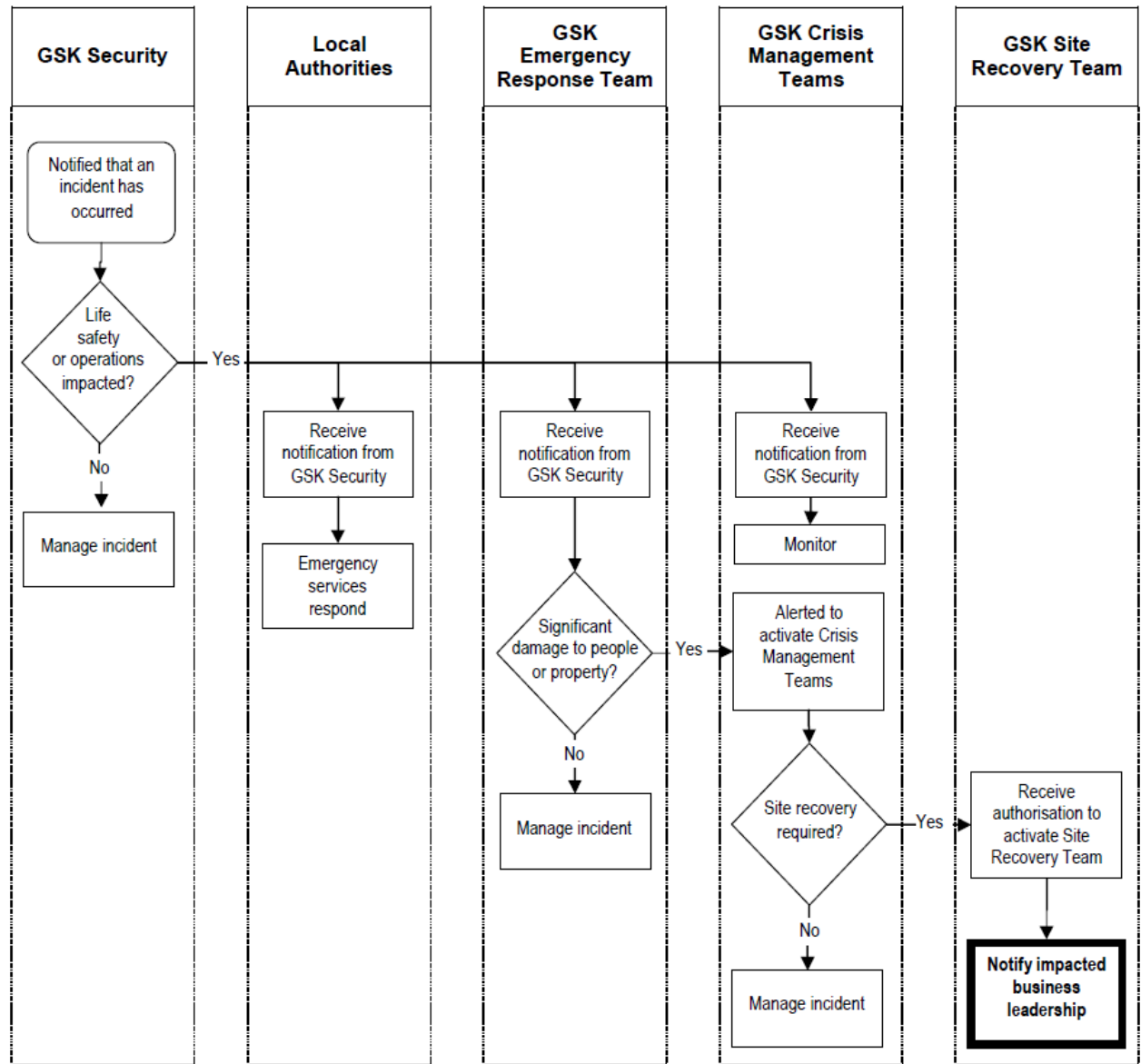


Рис. 3.1 Структура управління за розподіленими командами

3.2 Етапи впровадження системи забезпечення безперервності бізнесу

Важливо зазначити, що впровадження СЗББ повинно бути адаптоване до специфіки фармацевтичної галузі, де особливу увагу приділяють безпеці пацієнтів, якості продукції та цілісності даних. Забезпечення безперервності бізнесу є одним із найважливіших стратегічних напрямів розвитку будь-якої

компанії.

Етапи впровадження СЗББ в діючу фармацевтичну компанію:

1.1 Оцінка поточного стану компанії: На цьому етапі потрібно здійснити аналіз поточних бізнес-процесів і ресурсів компанії, щоб зрозуміти, які з них є критичними для безперервності бізнесу. Також варто оцінити поточний рівень ризику для цих процесів.

1.2 Ідентифікація та аналіз ризиків: Визначити потенційні загрози, що можуть перервати діяльність підприємства, та оцінити їхній вплив на ключові бізнес-процеси.

1.3 Розробка політики безперервності бізнесу (BCM): Розробка офіційної політики управління безперервністю бізнесу, яка має визначати стратегічні цілі, принципи та підходи до забезпечення безперервності в організації.

1.4 Розробка стратегії відновлення бізнесу: Вибір відповідних стратегій для мінімізації впливу кризових ситуацій на бізнес-процеси, зокрема планування альтернативних шляхів постачання, планування відновлення ІТ-систем та ін.

1.5 Розробка та впровадження плану відновлення після інцидентів (DRP): План відновлення після інцидентів включає чіткі інструкції, як відновити роботу в разі надзвичайної ситуації. Це може включати перезапуск ІТ-систем, забезпечення альтернативних джерел енергії, відновлення постачань.

1.6 Навчання та тренування персоналу: Проведення тренінгів та навчальних програм для працівників з реагування на кризові ситуації, використання інструментів для забезпечення безперервності бізнесу.

1.7 Моніторинг та оцінка ефективності системи: Постійний моніторинг і оцінка результатів впровадження системи, а також коригування процесів та стратегій у разі необхідності.

Для розробки політики СЗББ важливо визначити основні зацікавлені сторони, які впливають на її впровадження. Внутрішні сторони: інвестори,

власники, персонал, члени сімей персоналу та зовнішні: покупці, суспільство, держава, фінансові установи, аутсорсингові компанії, екстрені служби, ЗМІ, постачальники продукції, конкуренти.

Комісія з безперервності бізнесу розробить проект політики системи безперервності, яка буде інтегрована з діючою політикою з якості. Основна мета організації полягає в забезпеченні фармацевтичного ринку якісними, безпечними лікарськими засобами, що відповідають сучасним ринковим потребам, а також у запровадженні системи заходів для забезпечення безперервної діяльності. Організація також прагне до забезпечення належного контролю та безпеки на всіх етапах життєвого циклу лікарських засобів.

Ключові цілі організації в сфері безперервності бізнесу включають:

- Поліпшення результативності фармацевтичної системи якості.
- Збереження якості лікарських засобів на всіх етапах їхнього життєвого циклу.
- Забезпечення задоволеності споживачів.
- Постійне поліпшення системи безперервності бізнесу.
- Швидке реагування на зміни в нормативно-правовому законодавстві.

У результаті досягнення цих цілей, підприємство фокусується на створенні ефективної взаємодії з клієнтами, формуванні партнерських відносин із постачальниками, регулярному підвищенні кваліфікації персоналу та запобіганні потрапляння на ринок неякісних лікарських засобів.

Керівництво компанії гарантує дотримання політики якості та безперервності бізнесу, вживаючи необхідних заходів для належного виконання поставлених завдань і надаючи відповідні ресурси для підвищення кваліфікації персоналу.

Аналіз впливу на бізнес (BIA) є критичним етапом для визначення та оцінки потенційних наслідків переривання критичних бізнес-процесів через надзвичайні ситуації. Це дозволяє пріоритизувати важливі процеси, що

потребують більше ресурсів для відновлення в разі надзвичайних ситуацій.

До основних завдань, що виникають під час аналізу ВІА, відносяться:

- Визначення ключових бізнес-функцій, персоналу та технологічних ресурсів, необхідних для відновлення роботи компанії.
- Встановлення часу відновлення бізнес-процесів (RTO) та точок відновлення для даних (RPO).

Критичні бізнес-процеси організації включають такі функції, як реалізація, зберігання, управління персоналом, фінансами, документообігом, постачанням, реєстрацією активних фармацевтичних інгредієнтів (АФІ) та управлінням ІТ-технологіями.

Крім того, до критичних ресурсів відносяться: економічні, технічні, людські, інфраструктурні ресурси.

Співробітники, відповідальні за підтримку системи безперервності бізнесу, повинні розробити та вести документацію, що забезпечує її функціонування. До такої документації можуть входити:

- Стратегія та політика безперервності бізнесу.
- Аналіз впливу на бізнес та оцінка ризиків та загроз.
- Програми ознайомлення та навчання.
- План забезпечення безперервності бізнесу з плани управління інцидентами та відновлення бізнесу.
- Графіки та звіти з тестування.
- Угоди та договори про зовнішнє обслуговування.

Ідентифікація ризиків відбувається за наступними категоріями:

1 Ризики, пов'язані з постачанням сировини: Перерви в постачанні активних фармацевтичних інгредієнтів або упаковки можуть призвести до зупинки виробництва.

2 Технічні та ІТ-ризики: Збої в роботі ІТ-систем або кіберзагрози можуть призвести до втрати доступу до важливих даних або зупинки виробничих процесів.

3 Регуляторні та правові ризики: Зміни в законодавстві або

невідповідність вимогам може призвести до втрати ліцензій або санкцій.

4 Надзвичайні події (катастрофи, пандемії, військові дії): Природні катастрофи або епідемії можуть вплинути на здатність підприємства здійснювати свою діяльність.

5 Ризики, пов'язані з людським фактором: Втрата ключових кадрів, нещасні випадки, відсутність персоналу через хворобу чи інші причини можуть спричинити перебої в роботі.

6 Фінансові ризики: Погіршення фінансового стану компанії може призвести до зменшення інвестицій у забезпечення безперервності бізнесу.

Наступним є оцінка потенційних та наявних загроз для стабільної діяльності організації відповідно до існуючої процесної моделі системи управління якістю. Ця робота проводиться згідно зі стандартом ISO 31000. Проводити роботи з ризиками можемо за запропонованим алгоритмом на рисунку 3.2.

Сучасне розуміння ризик-менеджменту базується на концепції "прийнятного ризику", за якою основною метою управління ризиками є забезпечення максимальної стійкості діяльності компанії шляхом підтримання сукупного ризику (очікуваного рівня втрат) в межах, визначених стратегією розвитку підприємства. Але в СЗББ максимальне навантаження розуміння прийняття залежить від руйнівного впливу ризику, в незалежності від можливості його виявлення чи настання.

В результаті цієї роботи потрібно формувати звіт щодо ризиків відповідно до критичних процесів організації.

Група експертів визначить усі ризики в кожному стратегічному процесі, який впливає на діяльність компанії, і проведе їх ранжування.

Організація повинна розробити структуру системи реагування на інциденти, яка забезпечить ефективну реакцію та відновлення в разі нештатних ситуацій. Кожен інцидент потребує простої та швидко активованої системи реагування, яка дасть змогу організації:

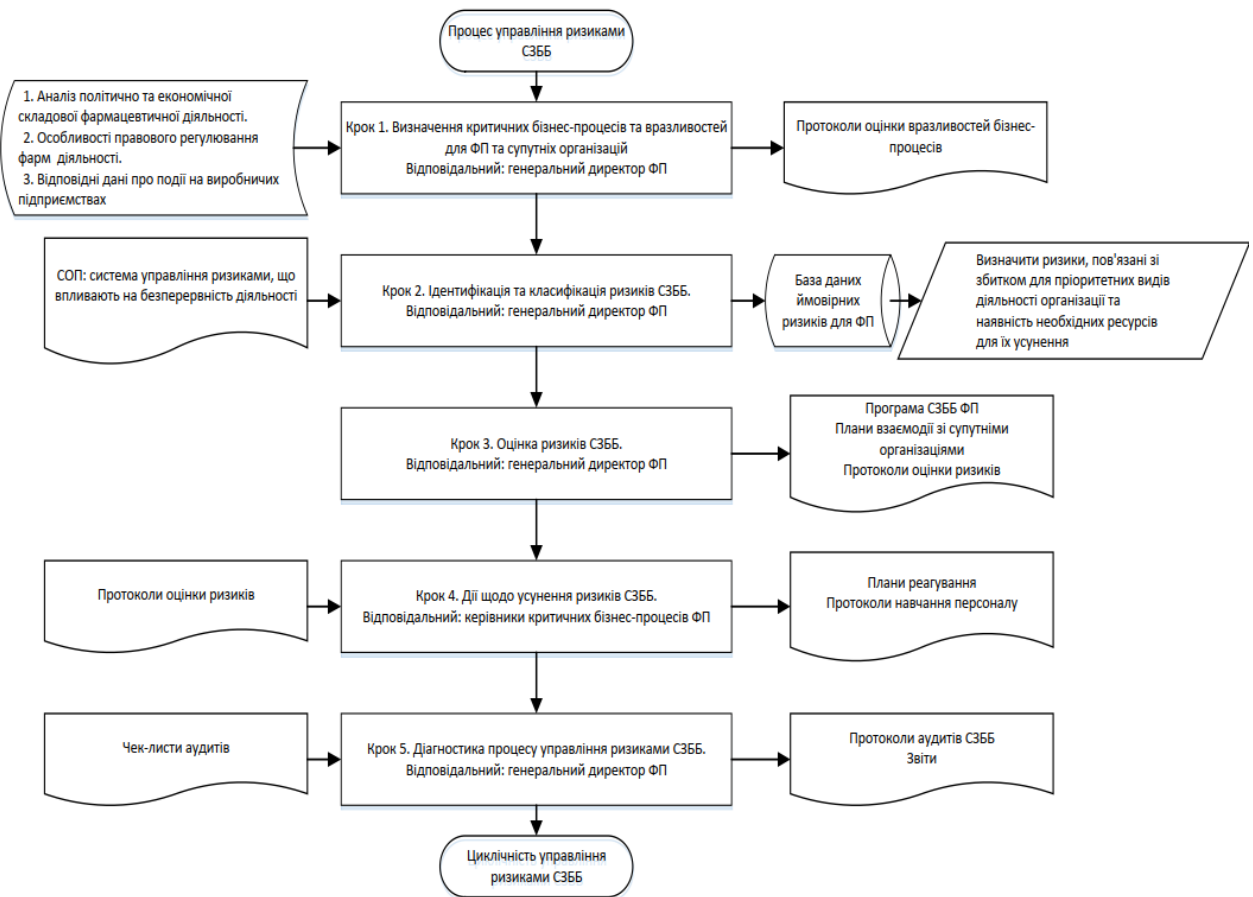


Рис. 3.2. Алгоритм побудови системи управління ризиками СЗББ.

- Підтвердити тип та масштаби інциденту.
- Взяти ситуацію під контроль.
- Забезпечити мінімізацію наслідків інциденту.
- Інформувати зацікавлені сторони.

Ця структура має також ініціювати відповідну процедуру для забезпечення безперервності бізнесу. Вона може бути сформована як група з управління інцидентами або група з управління кризовими ситуаціями.

Група повинна мати наявні плани, процеси та процедури для управління інцидентами, які інтегровані з механізмами безперервності бізнесу, що дозволить забезпечити стійкість та відновлення критичних бізнес-процесів.

Група повинна бути готова до активізації, координації та інформування під час реагування на інцидент. На рис. 3.3 показані три основні стадії обробки інциденту та їх взаємозв'язок з процесами забезпечення

безперервності бізнесу [15, 16, 17, 25, 36].

В окремих випадках організація може одночасно або з меншою затримкою активувати плани реагування на інциденти, відновлення бізнесу та забезпечення безперервності.

Крім того, організація може розробити плани для відновлення операцій до звичного стану, проте іноді неможливо визначити цей «нормальний» стан без певного часу після інциденту. В таких ситуаціях реалізація планів відновлення може бути відкладена. Тому організаціям можуть бути необхідні плани забезпечення безперервності бізнесу, які забезпечують достатній час для підготовки до відновлення ("повернення до нормального стану").

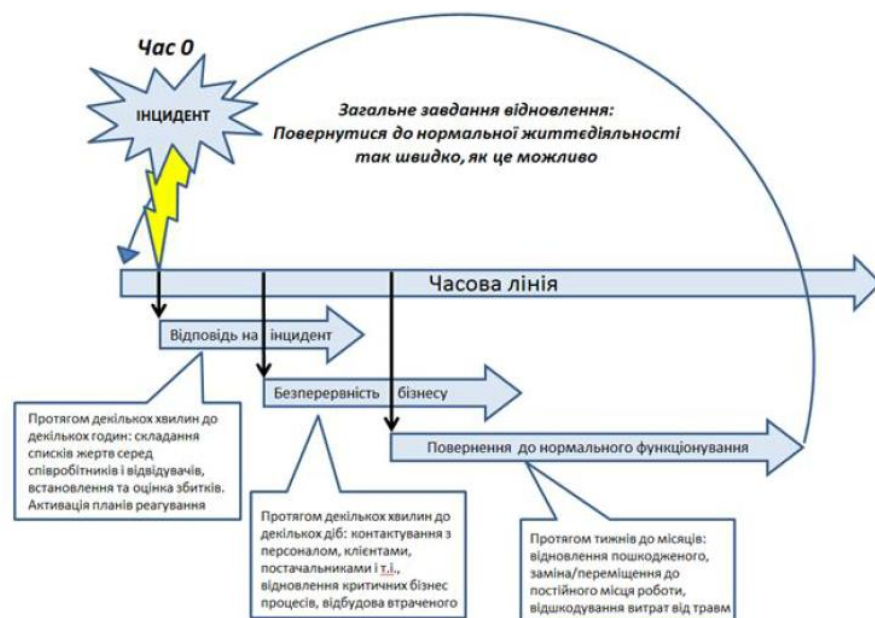


Рис. 3.3 Часові рамки інциденту

3.3 Розробка проекту плану безперервності та відновлення бізнесу

Усі плани, і управління інцидентами, забезпечення безперервності бізнесу та відновлення бізнесу є чітко визначеними та доступними для осіб, чий обов'язок описаний в цих планах. Мета та область застосування кожного плану повинні бути чітко сформульовані, узгоджені з вищим керівництвом і зрозумілі тим, хто буде реалізовувати цей план. Усі зв'язки з іншими відповідними планами або документами повинні бути точно вказані, а також зазначено, як отримати доступ до цих планів (Додаток Г).

Кожен план управління інцидентами, безперервності бізнесу та відновлення бізнесу має визначати пріоритетні завдання в контексті:

- критичних для бізнесу виробничих процесів, які потребують відновлення;
- тимчасових рамок для відновлення цих процесів;
- рівнів відновлення, необхідних для кожного критичного виробничого процесу;
- ситуацій, коли кожен план буде застосовуватися.

Плани можуть також включати процедури та рекомендації, що підтримують процес аналізу після інциденту, коли це доречно.

Ролі та обов'язки уповноважених співробітників (як щодо прийняття рішень, так і щодо витрат) і груп під час інциденту та після нього повинні бути чітко задокументовані. Необхідно визначити конкретних осіб і групи, чії дії охоплюються цими планами.

Час, витрачений на реагування, неможливо відновити. У більшості випадків краще мобілізувати групу реагування та скасувати її мобілізацію, ніж упустити можливість стримати інцидент на ранніх етапах і не допустити його ескалації.

Організація може орієнтуватися на міжнародно узгоджені стадії ескалації, враховуючи чіткі рекомендації авторитетних джерел, таких як рекомендації Всесвітньої організації охорони здоров'я щодо пандемії.

Метод активації плану управління інцидентами, забезпечення безперервності або відновлення бізнесу повинен бути чітко задокументований. Цей процес має забезпечити швидку активацію необхідних планів або їх частин після виникнення нештатної ситуації.

Компанія повинна розробити та задокументувати чіткі рекомендації і критерії, які визначатимуть, хто має повноваження активувати план(и) і за яких умов.

Процес активації може вимагати термінової мобілізації ресурсів організації. План повинен містити точний опис того, як буде здійснюватися

мобілізація груп:

- місце проведення первинної зустрічі;
- місця для наступних зібрань груп та інформацію про альтернативні місця (центри управління інцидентами або кризові центри).

Організація повинна мати чітко прописаний процес скасування мобілізації груп після завершення інциденту, а також процес повернення до звичайного функціонування.

Один основний власник плану повинен бути призначений, а також визначено, хто відповідатиме за регулярний аналіз, удосконалення та коригування плану. Контроль версій має бути забезпечений, із формальним інформуванням усіх зацікавлених сторін про зміни в планах. Також повинні вестись записи розсилки плану з регулярними оновленнями.

Контактні дані можуть включати інформацію для зв'язку поза робочим часом, при цьому якщо план містить конфіденційну інформацію, потрібно особливу увагу приділити її захисту. Кожен план має включати необхідні контактні дані для всіх ключових зацікавлених осіб або містити посилання на них.

Розробка кожного плану безперервності та відновлення бізнесу (рис. 3.4):

3.1 Мета і завдання плану: Визначити основні цілі плану безперервності бізнесу, зокрема забезпечення безперервного виробництва, постачання та обслуговування клієнтів під час надзвичайних ситуацій.

3.2 Ідентифікація критичних бізнес-процесів: Визначити бізнес-процеси, без яких діяльність компанії неможлива, та оцінити їхню важливість для підтримки основних операцій.

3.3 Оцінка потенційних загроз і сценаріїв: Для кожного критичного процесу визначити можливі загрози та сценарії їхнього впливу на бізнес.

3.4 Розробка заходів для зниження ризиків: Створити заходи для запобігання виникненню негативних ситуацій або мінімізації їхнього впливу на бізнес.

3.5 Розробка плану відновлення після інцидентів: Для кожного критичного процесу розробити алгоритм дій після виникнення надзвичайної ситуації, включаючи відновлення ІТ-систем, логістики, постачання сировини тощо.

3.6 Розподіл відповідальностей і ролей: У плані потрібно чітко визначити, хто відповідальний за виконання кожного етапу відновлення і хто приймає рішення в разі кризи.

3.7 Тестування і тренування плану: Проведення регулярних тренувань та симуляцій для перевірки ефективності плану відновлення бізнесу та підготовленості персоналу.

3.8 Оцінка результатів і постійне вдосконалення: Аналіз результатів відновлення бізнесу після кризових ситуацій та внесення коректив у план для покращення реакції на майбутні інциденти.

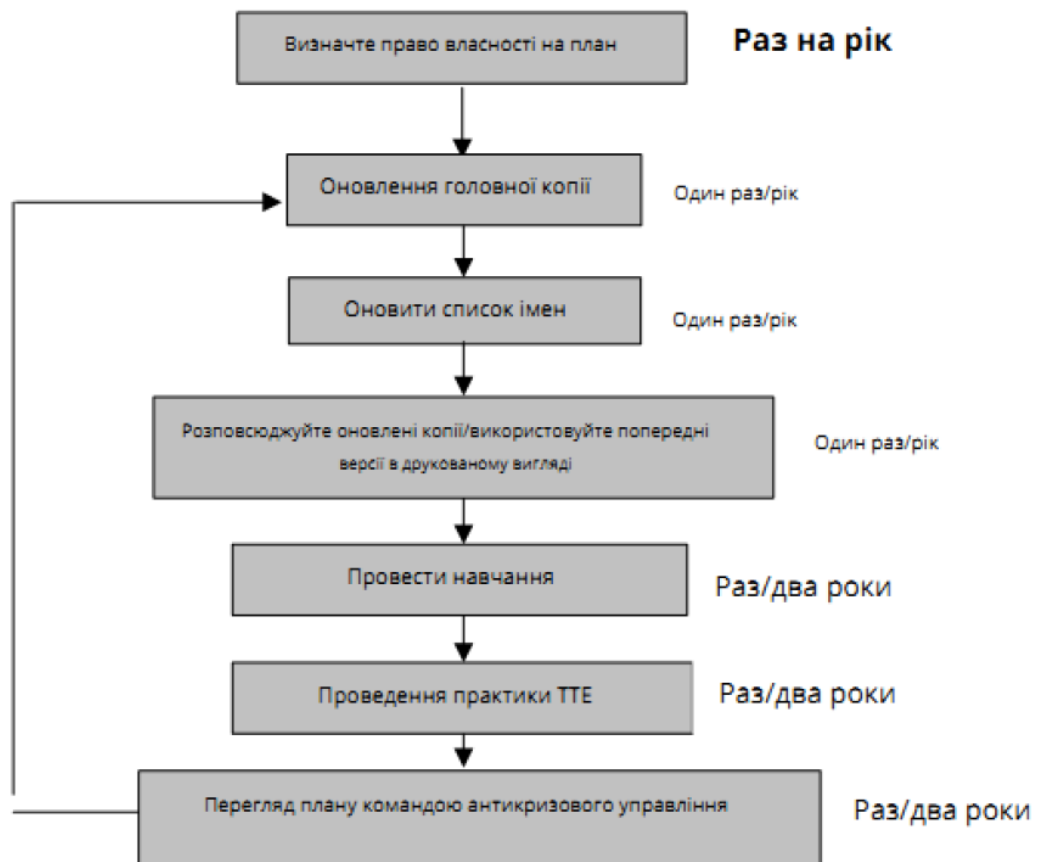


Рис. 3.4 Алгоритм складання плану безперервності бізнесу

Плани забезпечення безперервності бізнесу та управління інцидентами не можна вважати надійними без проведення регулярних тестувань і

оновлень. Тестування є важливим для покращення взаємодії, компетентності, впевненості та знань, необхідних під час кризових ситуацій.

Плани повинні проходити перевірку за допомогою тестування, аудиту та самооцінки, щоб оцінити їх відповідність встановленим вимогам.

Процеси тестування забезпечують підтвердження наявності необхідних навичок і ресурсів для підтримки безперервності бізнесу та ефективного управління інцидентами. Інвестиції часу та ресурсів у перевірку стратегій і планів допомагають переконатися, що вони відповідають своїм цілям. Навіть найкраще розроблені плани можуть потребувати коригувань, що стає очевидним після реалістичних тестувань.

Програма тестування повинна бути узгоджена з цілями та областями застосування плану забезпечення безперервності, а також відповідати всім нормативним вимогам. Тестування може включати:

- заздалегідь визначений результат, наприклад, з попередньо встановленим планом та обсягом;
- можливість розробки новаторських рішень для організації.

Програма тестування має бути спроектована так, щоб забезпечити впевненість у тому, що план забезпечення безперервності бізнесу спрацює, коли це буде потрібно. Вона повинна:

- перевіряти всі аспекти плану забезпечення безперервності, включаючи технічні, логістичні, адміністративні та інші складові;
- тестувати структуру і інфраструктуру управління безперервністю бізнесу, зокрема ролі, обов'язки, приміщення для управління інцидентами, робочі місця;
- перевіряти відновлення технологій та телекомунікацій, а також забезпечення наявності персоналу для їх перебазування.

Програма тестування також повинна сприяти вдосконаленню управління безперервністю бізнесу шляхом:

- практичного тренування здатності організації відновлювати діяльність під час інциденту;

- перевірки, чи всі критичні виробничі процеси враховані в плані забезпечення безперервності, а також їх пріоритети та залежності;
- вивчення припущень, що потребують додаткового аналізу;
- зміцнення впевненості учасників тестування;
- підвищення поінформованості всієї організації щодо забезпечення безперервності бізнесу шляхом поширення результатів тестування;
- перевірки ефективності і своєчасності відновлення критичних для бізнесу виробничих процесів;
- наочного демонстрування кваліфікації ключових груп реагування та їх дублерів.

Висновки до розділу 3

Впровадження СЗББ є стратегічно важливим кроком для забезпечення стабільності роботи підприємства в умовах НС. СЗББ підвищує репутацію компанії, ефективність процесів та довіру зацікавлених сторін. Її розробка потребує ресурсів і чіткого планування: аналіз бізнес-впливу, управління ризиками, створення плану, навчання персоналу та регулярного тестування, формування комісії з ключових підрозділів. Основні етапи включають аналіз бізнес-процесів, ідентифікацію ризиків, розробку політики та планів відновлення, навчання персоналу та постійний моніторинг ефективності.

Врахування специфіки галузі та використання стандартів, таких як ISO 31000, допоможуть мінімізувати ризики, забезпечити гнучкість і стійкість компанії в умовах кризових ситуацій.

Ефективне управління інцидентами є критично важливими для підтримки стабільності організації в умовах НС. Ключовими аспектами цих процесів є чітке визначення ролей і відповідальності, регулярне тестування планів, а також адаптація до змін через постійний аналіз і вдосконалення. Інвестиції у підготовку персоналу, належну документацію та перевірку планів забезпечують впевненість у здатності організації реагувати на кризові ситуації та підтримувати основні бізнес-процеси.

ЗАГАЛЬНІ ВИСНОВКИ

У роботі розглянуто актуальність СЗББ як ключового елемента захисту критично важливих процесів і ресурсів організації в умовах сучасних загроз (природні катастрофи, техногенні аварії, кіберзагрози, пандемії). Система забезпечує безперебійність операцій навіть у КС, сприяючи довірі клієнтів і партнерів, зростанню бізнесу та відповідності регуляторним вимогам.

Міжнародні стандарти (ISO 22301, BSI 100-4, NIST SP 800-34) визначають принципи побудови системи, а сертифікація за ISO 22301 забезпечує репутаційні та операційні переваги.

СЗББ є основним механізмом забезпечення стійкості компаній в умовах криз. Для дистриб'юторських компаній України найбільшими загрозами є втрата персоналу, перебої енергопостачання, збої в інформаційних системах, порушення ланцюгів постачання та кіберінциденти. Для мінімізації ризиків важливо звернути увагу на кадровий резерв, резервне електропостачання, засоби кібербезпеки, диверсифікувати постачальників, а також застосовувати сценарне планування та проводити навчання персоналу. Ефективна підготовка до надзвичайних ситуацій і здатність швидко адаптуватися є запорукою стабільної роботи компанії.

Впровадження СЗББ є стратегічним кроком для забезпечення стабільної роботи підприємства в умовах надзвичайних ситуацій. Ця система підвищує репутацію компанії, оптимізує бізнес-процеси та зміцнює довіру зацікавлених сторін. Її розробка вимагає ретельного планування, включаючи аналіз впливу на бізнес, управління ризиками, створення планів реагування, навчання персоналу та регулярне тестування. Формування команди з представників ключових підрозділів забезпечує комплексний підхід до впровадження.

Інвестиції в підготовку персоналу, якісну документацію та перевірку планів гарантують готовність організації до КС і забезпечують безперебійність основних бізнес-процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Управління безперервністю бізнесу – система менеджменту стійкістю. URL: <http://surl.li/rkfaru> (дата звернення: 30.10.2024).
2. Hiles A. The Definitive Handbook of Business Continuity Management. Chichester : John Wiley Sons, 2011. 832 p.
3. Rittinghouse J., Ransome J. Business Continuity and Disaster Recovery for InfoSec Managers. Oxford : Elsevier, 2005. 220 p.
4. Akhtar S., Afsar S. Business Continuity Planning Methodology. Mississauga : Sentryx, 2004. 304 p.
5. Business Continuity Preparedness Handbook. AT&T Believes. 2016. URL: https://www.attbelieves.com/ecms/dam/pages/disaster_relief/AT&T%20BCH.pdf (Date of access: 30.10.2024).
6. Engemann K. J. The Routledge Companion to Risk, Crisis and Security in Business. New York : Routledge, 2018. 405 p.
7. The One Essential Guide to Disaster Recovery: How to Insure IT and Business Continuity. URL: <https://www.pax8.com/resource/display/1499> (Date of access: 30.10.2024).
8. DRP & BCP. Disaster Recovery and Business Continuity Plan. Exclusive research 2018 from IDC. URL: https://www.business-solutions.telefonica.com/media/2207/drп_bcp-white-paper-may18-web.pdf (Date of access: 20.11.2024).
9. ДСТУ ISO 22300:2020. Безпека і стійкість. Словник (ISO 22300:2018, IDT). Київ : УкрНДНЦ, 2021. 34 с.
10. ДСТУ EN ISO 22301:2021. Безпека та стабільність. Системи управління неперервністю бізнесу. Вимоги (EN ISO 22301:2019, IDT; ISO 22301:2019, IDT) ; чинний від 01.09.2022. Вид. офіц. Київ : УкрНДНЦ, 2022. 18 с.
11. ДСТУ ISO 31000:2018. Менеджмент ризиків. Принципи та наста-

нови (ISO 31000:2018, IDT). Київ : УкрНДНЦ, 2019. 24 с.

12. ДСТУ ISO/IEC 27001:2015. Інформаційні технології. Методи захисту. Системи управління інформаційною безпекою. Вимоги (ISO/IEC 27001:2013, IDT). Київ : УкрНДНЦ, 2015. 34 с.

13. Enhancing business continuity management to address changing business realities. New York : IBM Corporation, 2017. URL: <https://www.ibm.com/downloads/cas/ZGLEMLRR> (Date of access: 30.10.2024).

14. Якубовський В. В. Сучасні підходи та моделі в менеджменті безперервності бізнесу. *Актуальні проблеми міжнародних відносин*. 2015. Вип. 126, ч. 2. С. 91–100.

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

16. Зборовська Т. В., Губін Ю. І. Статистичний огляд впровадження системи забезпечення безперервності бізнесу. *Актуальні проблеми розвитку галузевої економіки та логістики* : матеріали VI наук.–практ. конф. з міжнар. участю, м. Харків, 25–26 жовт. 2018 р. Харків : НФаУ, 2018. С. 126–128.

17. 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.

18. Кухарська Н., Полотай О. Аспекти інформаційної безпеки в управлінні безперервністю діяльності організації. *Information Technology and Security*. 2019. Vol. 7, № 2(13). Р. 97–102.

19. Інтеграція безперервності бізнесу та управління ризиками підприємства. URL: https://tic-ua.com/uk/statti/integracziya-bezperervnosti-biznesu-ta-upravlinnya-ryzykamy-pidpryyemstva/?utm_source=chatgpt.com (дата звернення: 30.10.2024).

20. Ситайло У. В. Безперервність бізнесу в Україні: виклики та можливості в умовах війни. *Економіка та суспільство*. 2024. № 62. URL:

<https://economyandsociety.in.ua/index.php/journal/article/view/3887> (дата звернення: 15.10.2024).

21. Шнюков А. В., Проскурня О. М. Актуальність забезпечення безперервності бізнесу на логістичному фармацевтичному підприємстві. *Управління якістю в фармації* : матеріали IX наук.–практ. конф., м. Харків, 22 трав. 2015 р. Харків : НФаУ, 2011. С. 144–145.

22. Калужінська А. Імплементація вимог стандарту ISO 22301 в роботу організації ТОВ «Джонсон і Джонсон Україна» : кваліфікаційна робота. Харків, 2023. 61 с.

23. Барський М. В. Безперервність бізнесу в контексті ланцюгів постачання. *Сталий розвиток економіки*. 2024. № 1(48). С. 302–308.

24. Проскурня О. М. Удосконалення системи організації виробництва енергетичних підприємств через впровадження менеджменту безперервності бізнесу. *Вісник НТУ «ХПІ»*. 2018. № 20(1296). С. 102–106.

25. Панченко В., Резнікова Н. Від вразливості ланцюгів поставок до їх гнучкості та стійкості для МСП. URL: <https://www.industry4ukraine.net/publications/vid-vrazlyvosti-lanczyugiv-postavok-do-yih-gnuchkosti-ta-stijkosti-dlya-msp/> (дата звернення: 11.12.2023).

26. Мушинський Б. М. Безперервність ведення бізнесу як концепція управління фінансовою установою. *Економічна кібернетика: теорія, практика та напрямки розвитку* : матеріали наук.–практ. інтернет–конф. URL: https://economics.net.ua/files/science/ek_kiber/2018/112.pdf (дата звернення: 11.12.2023).

27. Шнюков А. В., Проскурня О. М. Актуальність забезпечення безперервності бізнесу на логістичному підприємстві. *Управління якістю в фармації* : матеріали IX наук.–практ. конф. URL: <http://surl.li/qgfbl> (дата звернення: 14.12.2024).

28. Дослідження KPMG 2023 CEO Outlook. URL: <https://kpmg.com/ua/uk/home/insights/2023/10/kpmg-global-ceo-outlook-survey.html> (дата звернення: 18.12.2024).

29. Москаль Н. В. Комплексний підхід до оцінки безперервності діяльності підприємства: обліково–аналітичні аспекти. *Економіка та суспільство*.

2024. № 65. URL: <https://economyandsociety.in.ua/index.php/journal/article/view/4409> (дата звернення: 15.10.2024).

30. Назаренко І. М. Особливості оцінки принципу безперервності в практичній діяльності підприємств. *Європейський вектор модернізації економіки: креативність, прозорість та сталий розвиток* : матеріали XII Міжнар. наук.–практ. конф. Харків : ХНУБА, 2020. С. 118–119. URL: <https://repo.snau.edu.ua/bitstream/123456789/7733/1/Назаренко%20І.М.%20Особливості%20оцінки%20принципу.pdf>. (дата звернення: 15.10.2024).

31. Топоркова О., Коваленко М. Індикатори аудиторської оцінки безперервності діяльності. *Перспективи розвитку обліку, аналізу та аудиту в контексті євроінтеграції* : матеріали XI Міжнар. наук.–практ. конф. Одеса : ОНЕУ, 2023. С. 244–246. URL: https://lib.lntu.edu.ua/sites/default/files/2023-09/Збірник%20конферен-ції_18.05.2023.pdf#page=245 (дата звернення: 30.10.2024).

32. Rouco J. C., Figueiredo P. C. Business Continuity Management and Resilience : Theories, Models, and Processes. 2024. 360 p.

33. Чому актуальність стандарту ISO 22301 вкрай висока? URL: <http://surl.li/uatsml> (дата звернення: 15.10.2024).

34. Якубовський В. В. Сучасні підходи та моделі в менеджменті безперервності бізнесу. *Актуальні проблеми міжнародних відносин*. 2015. Вип. 126, ч. 2. С. 91–100.

35. 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.

36. GSK : офіційний сайт. URL: <https://www.gsk.com/en-gb/> (дата звернення: 02.12.2024).

ДОДАТКИ

МАТЕРІАЛИ

**І науково-практичної
internet-конференції з
міжнародною участю
«АКТУАЛЬНІ ПРОБЛЕМИ
ЯКОСТІ, МЕНЕДЖМЕНТУ І
ЕКОНОМІКИ У ФАРМАЦІЇ І
ОХОРОНІ ЗДОРОВ'Я»**

(19 травня 2023 р.)

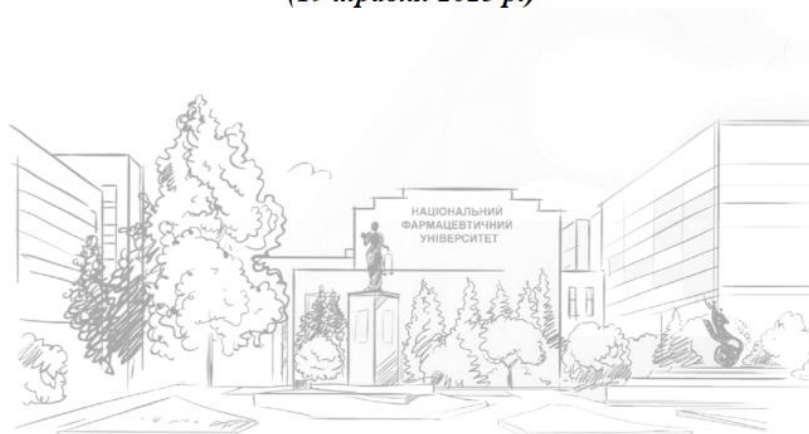


*Міністерство охорони здоров'я України
Міністерство освіти і науки України
Національний фармацевтичний університет
Кафедра управління та забезпечення якості у
фармації*



МАТЕРІАЛИ

**І науково-практичної internet-конференції з міжнародною участю
«АКТУАЛЬНІ ПРОБЛЕМИ ЯКОСТІ, МЕНЕДЖМЕНТУ І
ЕКОНОМІКИ У ФАРМАЦІЇ І ОХОРОНІ ЗДОРОВ'Я»
(19 травня 2023 р.)**



MATERIALS

**of I scientific and practical internet-conference
with international participation
«ACTUAL PROBLEMS OF QUALITY, MANAGEMENT,
AND ECONOMY IN PHARMACY AND HEALTH CARE»
(19 May 2023)**

Харків

2023

Савченко Л. П., Георгіяни В. А. <i>Національний фармацевтичний університет, м. Харків</i> Розробка підходів до вивчення стабільності мазей, виготовлених в аптеці	213
Самборський О.С., Слободянюк М.М. <i>Івано-Франківський національний медичний університет</i> <i>Національний фармацевтичний університет, м. Харків</i> Опрацювання методичного підходу до визначення потенційної ємності ринку антианемічних лікарських засобів	215
Соловійов С.О., Трохимчук В.В., Кабачна А.В <i>Національний університет охорони здоров'я України ім. П. Л. Шупика, м. Київ</i> Аналіз компетентностей професіоналів з фармаконагляду	218
Ткаченко Н.О.¹, Червоненко Н.М.², Демченко В.О.³, Маганова Т.В.⁴, Литвиненко О.В.⁵, Демченко В.О.⁶, Зарічна Т.П.⁷, <i>Запорізький державний медико-фармацевтичний університет, м. Запоріжжя</i> Роль дослідницької складової у формуванні професійних компетентностей майбутніх фармацевтичних фахівців	220
Ткаченко О.В. <i>Національний фармацевтичний університет, м. Харків</i> Підходи до ідентифікації та оцінки екологічних аспектів на хіміко-фармацевтичних і біотехнологічних підприємствах	223
Федюніна Н. С., Братішко Ю. С. <i>Національний фармацевтичний університет, м. Харків</i> Актуальні питання соціальної відповідальності фармацевтичного бізнесу	226
Фетісова О.Г., Андрюкова Л.М. <i>Інститут підвищення кваліфікації спеціалістів фармації НФаУ, м. Харків</i> Аналіз змін у переглянутому ІСН документі Q 9 «Управління ризиками для якості»	229
Харченко Д. С.¹, Зборовська Т.В.², Гончаров С.В. ¹<i>ТОВ «ГлаксоСмітКляйн Фармасьютікалс Україна», м. Київ</i> ²<i>Національний фармацевтичний університет, м. Харків</i> Актуальність впровадження безперервності бізнесу в роботу фармацевтичних дистриб'юторських компаній в Україні	231
Чегринець А. А., Бережна-Пилипчук Н. Ю. <i>Національний фармацевтичний університет, м. Харків</i> Аналіз асортименту відхаркувальних засобів, який представлений на вітчизняному фармацевтичному ринку	234
Чегринець А. А., Романенко А. А. <i>Національний фармацевтичний університет, м. Харків</i> Дослідження обізнаності населення щодо Корпорації “Артеріум”	236

Харченко Д. С.¹, Зборовська Т.В.², Гончаров С.В.

¹ТОВ «ГлаксоСмітКляйн Фармасьютікалс Україна», м. Київ

²Національний фармацевтичний університет, м. Харків

Актуальність впровадження безперервності бізнесу в роботу фармацевтичних дистриб'юторських компаній в Україні

4137299@gmail.com

Вступ. Важливість та актуальність системи управління безперервністю бізнесу ми можемо побачити на прикладі долі підприємств та організацій в Україні після початку повномасштабного вторгнення в 2022 році. Одні бізнеси закрились і не відновились, інші ж – навпаки, продемонстрували вражаючу стійкість і швидко відновили свою операційну діяльність та навіть побачили нові можливості для розвитку. Що ж відрізняє успішні приклади від сумних? Можна сказати з впевненістю, що такі дії, як: впровадження ефективної системи управління безперервністю бізнесу, виділення ключових процесів, оцінка можливих ризиків для кожного процесу та розробка способів їх попередження та/або реагування на них з мінімізацією їх негативного впливу, регулярний перегляд та оновлення політики управління безперервністю бізнесу є головними чинниками, які з високою долею імовірності дозволяють такому бізнесу успішно пережити більшість форс-мажорних обставин та непередбачуваних подій та своєчасно відновити функціонування.

Мета дослідження. Виходячи з цього ставимо за мету дослідити передумови впровадження системи управління безперервністю бізнесу на прикладі діяльності організації з дистрибуції лікарських засобів.

Матеріали та методи. В якості методів будемо використовувати дослідження джерел літератури та відкриті статистичні дані фармацевтичної галузі щодо форс-мажорних обставин.

Отримані результати. Сьогодні суб'єкти фармацевтичного ринку України орієнтуються на досвід провідних компаній, які вже впровадили у свою діяльність декілька систем управління та успішно розвивають їх як єдину

інтегровану систему. Однією з таких систем доцільно обрати систему забезпечення безперервності бізнесу (СЗББ), яка підвищить шанс виживання компанії та забезпечить стабільність функціонування.

Задля уніфікації підходів та підвищення ефективності створення такої системи був розроблений Стандарт ISO 22301:2019 Безпека і стійкість. Системи менеджменту безперервності бізнесу. Вимоги цього стандарту дозволяють побудувати ефективну систему управління при настанні будь-яких ситуацій.

Розглянемо загрози, які траплялися в нашій компанії протягом останніх трьох років та мали найбільший вплив і призвели до тимчасової зупинки діяльності, що порушило терміни виконання договорів.

Виходячи з проведеного аналізу можливостей компанії, ми пропонуємо впровадити відповідні запобіжні заходи та паралельно розробити дії щодо швидкого реагування при виникненні надзвичайної ситуації з відповідним встановленням критичних термінів щодо повного відновлення.

Таблиця

Тип загрози	Вплив на процеси (наслідки)	Можливі запобіжні заходи	Дії з реагування на інцидент	Критичний термін (час) повного відновлення
Зупинка поставок лікарських засобів (ЛЗ) через логістичні проблеми	Критичний, оскільки це ключовий процес організації	Наявність чіткого алгоритму використання альтернативних шляхів постачання (повітряний, автомобільний, залізничний), наявність контракту або попередня домовленість з альтернативним логістичним партнером	Оперативне коригування шляхів поставок та/або залучення основного або альтернативного логістичного партнера	Протягом 30 робочих днів
Неналежні умови зберігання ЛЗ на складі через збій в роботі електричних мереж	Суттєвий – реалізація ЛЗ є основним елементом господарської діяльності та ключовим процесом	Наявність обладнання, що дозволяє підтримувати необхідні вимоги протягом певного періоду часу, наявність одного чи декількох резервних джерел живлення	Налаштування автоматичного перемикання між різними джерелами живлення у разі, коли основне джерело відключається	Протягом 1 години

Збій роботи через неможливість співробітників критичних функцій виконувати свої посадові обов'язки	Помірний, залежить від тривалості такого збою	Визначення критичних функцій та мінімальної кількості співробітників для їх здійснення. Визначення back-up функцій та співробітників, які у разі відсутності основних будуть виконувати критично важливі функції. Навчання та підтримання актуальності знань та навичок таких співробітників	Запровадження регулярних звітів з метою ідентифікації збою у разі його виникнення. Залучення заздалегідь визначених співробітників на заміну тих, хто тимчасово не може виконувати свої обов'язки	Протягом 8 годин
Збій роботи мережевої інфраструктури (комп'ютери, мережа Інтернет і т.п.)	Помірний, залежить від тривалості збою	Забезпечення співробітників критичних функцій альтернативними засобами зв'язку та доступом до мережі Інтернет. Визначення місць із наявними альтернативними джерелами живлення та зв'язку (наприклад, «Пункт незламності»), куди такі співробітники можуть дістатись за потреби і де вони можуть виходити на зв'язок та підтримувати діяльність компанії	Кожен співробітник має діяти згідно заздалегідь розробленої інструкції, яка «активується» за чітко визначених умов настання збою	Протягом 8 годин

Висновки. Підводячи підсумки, можемо сказати, що на цьому прикладі ми бачимо, як важливо побудувати ефективну систему управління безперервністю бізнесу, що дозволить підприємству бути захищеним і продовжувати здійснювати операційну діяльність при будь-яких форс-мажорних ситуаціях. В побудові системи важливо звернути увагу не на безпосередньо подію, а на можливі негативні наслідки від неї, відповідні шляхи її попередження, кроки з реагування та відновлення.



Міністерство
охорони здоров'я
України

Національний
фармацевтичний
університет



Цим засвідчується, що

Харченко Д. С.

**Науковий керівник:
Крутських Т. В.**

брав(ла) участь у роботі IV Всеукраїнської
науково-практичної конференції
з міжнародною участю

**YOUTH
PHARMACY
SCIENCE**

СЕРТИФІКАТ

Ректор НФаУ,
д. фарм. н., проф.



Алла КОТВИЦЬКА

10-11 грудня 2024 р.
м. Харків,
Україна



Міністерство
охорони здоров'я
України

Національний
фармацевтичний
університет

ЗБІРНИК МАТЕРІАЛІВ

V Всеукраїнська науково-практична
конференція з міжнародною участю

YOUTH PHARMACY SCIENCE

10-11 грудня 2024 р.,
м.Харків, Україна



МІНІСТЕРСТВО ОХОРОНИ ЗДОРОВ'Я УКРАЇНИ
НАЦІОНАЛЬНИЙ ФАРМАЦЕВТИЧНИЙ УНІВЕРСИТЕТ

YOUTH PHARMACY SCIENCE

МАТЕРІАЛИ
V ВСЕУКРАЇНСЬКОЇ НАУКОВО-ПРАКТИЧНОЇ
КОНФЕРЕНЦІЇ З МІЖНАРОДНОЮ УЧАСТЮ

10-11 грудня 2024 року
м. Харків

Харків
НФаУ
2024

визначити місце логістичного управління серед інших напрямів дослідження та управління, таких як адміністрування, маркетинг і класичний менеджмент.

Відповідно до концепції логістичного управління, для розвитку ЛС у ЗОЗ слід дотримуватись встановлених принципів логістики. До ключових із них належать принципи раціональності, цілісності, системності, ієрархічності, інтеграції, формалізації та організації.

Принципи логістики доцільно використовувати в організації роботи реєстратури ЗОЗ, зокрема для запису пацієнтів і їх направлення до лікарів різного профілю. Оптимізація інформаційних потоків, контроль за впорядкуванням черговості прийому пацієнтів та організація цього процесу можуть розглядатися як ефективні складові комплексного логістичного аналізу внутрішніх потоків економічних структур.

Рекомендується також застосовувати логістичні підходи для оптимізації внутрішніх потоків медичного персоналу та пацієнтів, забезпечення їх необхідним обладнанням і належним обслуговуванням у ЗОЗ.

Одним із перспективних напрямків використання логістики у ЗОЗ є організація взаємодії закладів із службою швидкої допомоги в реальному часі. Це дозволить оптимізувати потік пацієнтів до лікарень, уникнути пікових навантажень, підготувати персонал та обладнання для прийняття тяжкохворих тощо.

Висновки. Запровадження управлінського підходу в діяльність ЗОЗ на підставі логістичного менеджменту зумовлене не лише збільшенням обсягів виробництва ЛЗ і надання МП, а передусім створенням ефективних БП, які сприяють успішній адаптації ЗОЗ до сучасних реформ.

Варто зазначити, що створення ЗОЗ в умовах необхідності раціонального використання ресурсів, задіяних у процесах обслуговування пацієнтів, набуває інноваційного значення. Такі інновації повинні бути спрямовані на підвищення ефективності використання ресурсів із врахуванням їх медичної, економічної та соціальної цінності.

Для використання прихованих резервів необхідно посилити економічний аспект управління, застосовуючи сучасні підходи до управління потоками ресурсів і вдосконалюючи механізми оплати праці персоналу ЗОЗ.

ОГЛЯД РИЗИКІВ БІЗНЕС-ПРОЦЕСІВ ДИСТРИБ'ЮТОРСЬКОЇ КОМПАНІЇ В РОЗРІЗІ БЕЗПЕРЕРВНОЇ ДІЯЛЬНОСТІ

Харченко Д. С.

Науковий керівник: Крутських Т. В.

Національний фармацевтичний університет, Харків, Україна

krutskikh.tetyana@gmail.com

Вступ. Організації, незалежно від галузі та розміру, мають критичні бізнес-процеси. Якщо ці процеси порушуються, перериваються або їм заважають виконуватися надзвичайні ситуації, їх виживання може бути під загрозою. Забезпечення стійкого функціонування критичних бізнес-процесів, підтримка повсякденних операцій під час або після настання загрози є метою та перевагою реалізації системи менеджменту безперервності бізнесу (СМББ).

Надзвичайний стан є величезним викликом. Аутсорсинг, диверсифіковані ланцюги поставок, перерви в енергопостачанні, збій ІТ-процесів і не в останню чергу пандемія та військовий стан – це тільки частина зовнішніх загроз, які можуть призвести до подій з глобальними негативними наслідками. Надзвичайні ситуації зазвичай виникають без

попередження. І вони мають одну спільну рису: загрозливий для існування характер. Вирішальним є не сама подія, а вплив, який він має на організацію. Це робить попередження надзвичайних ситуацій та управління кризовими ситуаціями ще більш важливими, щоб бути максимально підготовленим.

Мета дослідження. Тому мета нашого дослідження полягає в визначенні ризиків та огляді можливостей реалізації СМББ в дистрибуторській організації.

Матеріали та методи. Аналіз літературних джерел, стандарті ДСТУ EN ISO 22301:2021 та нормативно-правові вимоги дистрибуції.

Результати дослідження. Дистрибуторська діяльність досить поширена на міжнародних та внутрішніх ринках і продовжує досить стрімко розвиватися. В таких країнах як Німеччина, Великобританія, Швеція на частку торговельних посередників припадає близько половини обороту товарів і послуг.

В Україні торговельно-посередницька діяльність розвивається досить різнопланово. Розширення зовнішньоекономічних зв'язків, лібералізація торгівлі, відносна віддаленість постачальників і покупців, ускладнення комерційних операцій в умовах війни, з одного боку, об'єктивно потребують прискореного реформування дистрибуторської діяльності та посилення її у міжнародних відносинах включаючи нові умови взаємодії з партнерами.

Основним завданням успішного дистрибутора є забезпечення регулярних продажів обумовленого обсягу товару. При цьому ланцюжок руху товару від виробника до потенційних споживачів може бути різним і не мати проміжних етапів. Дистрибутор, як торговельно-посередницька структура, може працювати самостійно або представляти одночасно декілька компаній. Це ускладнює процес його діяльності, збільшує обсяги роботи, додає відповідальності та потребує взаємного налагодження та чіткого узгодження відносин з виробниками. Дистрибуторська діяльність має ряд характерних особливостей: представляючи зацікавлені сторони вони здійснюють як юридичні, так і фактичні дії; дистрибутори виконуючи угоди часто і фінансують їх, надають додаткові послуги, беруть на себе ризики тощо.

У сучасних умовах дистрибуторські компанії – це торговельно-посередницькі структури незалежного і специфічного виду діяльності, які здійснюють свій бізнес на основі таких принципів: рівноправність сторін; підприємливість; оперативність; обслуговування контрагентів; економічна зацікавленість; комерціалізація діяльності; договірні взаємовідносини.

Всі ці принципи в тій чи іншій мірі мають велику кількість настання непередбачуваних надзвичайних ситуацій, що приводить до порушення діяльності та ланцюга постачання продукції.

Управління безперервністю бізнесу, яке вибудовується в таких організаціях повинно бути закріпленим в організаційній культурі та базуватися на циклі PDCA. Ключовим аспектом є програма управління системою безперервності бізнесу із завданнями: розробкою стратегії, розподілом відповідальності, реалізацією безперервності бізнесу та постійною підтримкою за допомогою вдосконалення планів, тренувань груп управління та швидкого реагування і перевірок ефективності усіх попередньо розроблених методик та заходів.

Бізнес-процеси спочатку аналізуються на специфічній для організації основі щодо впливу на бізнес і відповідно обґрунтовуються пріоритети. Таким чином, операції можна відновити оптимальним чином після закінчення кризи. ISO/TS 22317 можна використовувати як керівництво та підтримку для проведення та документування аналізу впливу на бізнес, а ISO 31000 для визначення зовнішніх та внутрішніх ризиків.

Загрози безперервності бізнесу в Україні та інструменти їх мінімізації можуть бути наступними:

1. Втрата персоналу: інвентаризація навичок персоналу, перехресне навчання, документування процесів, планування кадрового резерву, залучення аутсорсингових послуг для роботи персоналу.
2. Втрата основних засобів чи доступу до них: внутрішнє переміщення персоналу, віддалена робота, переміщення організації (географічне).
3. Перебої енергопостачання: забезпечення резервного електропостачання.
4. Збої та втручання в інформаційно-технологічні системи: використання однакового програмного забезпечення, обладнання, інфраструктури тощо, створення резерву обладнання для екстреної заміни або запасних частин, кібербезпека.
5. Порушення цілісності ланцюгів постачання: диверсифікація постачальників, визначення альтернативних логістичних сполучень та способів доставки, створення резервних запасів.

СЗББ – це цілісний процес визначення загроз та їх можливого впливу на критичні процеси з метою відновлення живучості, а потім якомога швидшого відновлення діяльності до нормального стану після інциденту. СЗББ чітко відрізняється від звичайного управління ризиками. Незважаючи на всі передбачення і планування збої можуть бути несподівано тому всі намагаються зберегти свою здатність до роботи використовуючи організаційні заходи та проводячи тренування. Рішення приймаються на підставі фактів. У надзвичайних ситуаціях співробітники готові діяти зосереджено і процедурно, незважаючи на стрес.

Наявність плану безперервності бізнесу та розроблених протоколів реагування на інциденти допоможе реалізувати в повній мірі можливості організації локалізувати небезпеку та мінімізувати, в першу чергу, негативний вплив на персонал в момент настання інциденту, а потім зосередити зусилля на ліквідації наслідків від нього. Опитування 2020 року показало, що 51% компаній зіткнулися з пандемією без плану безперервності бізнесу. За оцінками Федеральної асоціації управління надзвичайними ситуаціями (FEMA), 75% малих підприємств не мають плану подолання збоїв. Малі та середні компанії вказують на обмеження часу, бюджету та ресурсів як причини, чому їх немає.

Висновки. Кожне четверте підприємство не відкривається знову після катастрофи, а 90% зазнають краху протягом року, якщо їх діяльність припиняється більше ніж на п'ять днів. СЗББ для дистриб'юторських компаній створить умови виживання і структурує не тільки захист, але й вбудує його в повсякденну роботу організації. Тому визначення потенційних небезпек, розробка планів швидкого реагування та розрахунок часу відновлення є основним нашим завданням в подальших дослідженнях.

ВИКОРИСТАННЯ ІНСТРУМЕНТІВ АНТИКРИЗОВОГО УПРАВЛІННЯ У ДІЯЛЬНОСТІ АПТЕЧНОГО ЗАКЛАДУ

Ющенко Д. А., Посилкіна О. В.

Національний фармацевтичний університет, Харків, Україна
dasha19990403@gmail.com

Вступ. Сучасний розвиток фармацевтичного ринку України відбувається в умовах постійних економічних та політичних змін, що підвищує необхідність застосування антикризових інструментів управління в діяльності аптечних закладів. Зокрема, ТОВ «АПТЕКА911.ЮА» стикається з викликами, пов'язаними з нестабільністю економічного

ЗМІСТ

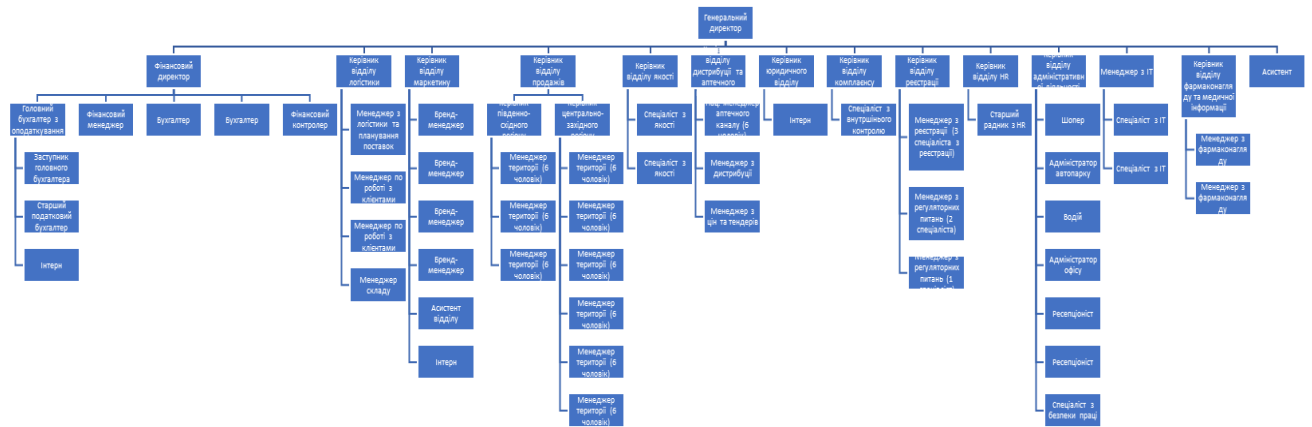
Скринник А. А., Германова Д. С.; Н. к.: Жадько С. В.	386
Таранушич М. С.; Н. к.: Рогуля О. Ю.	387
Федорович А. Ю.; Н. к.: Рогуля О. Ю.	388
Чемерис О. О.; Н. к.: Рогуля О. Ю.	390
Шарко А. О.; Н. к.: Шуванова О. В.	391
Щетницька В. С., Малініна Н. Г.; Н. к.: Рогуля О. Ю.	392

СЕКЦІЯ 14. УПРАВЛІННЯ, ЕКОНОМІКА ТА ЗАБЕЗПЕЧЕННЯ ЯКОСТІ У ФАРМАЦІЇ MANAGEMENT, ECONOMIC, AND QUALITY ASSURANCE IN PHARMACY

Боримський О. І.; Н. к.: Коваленко С. М.	395
Брага В. В.; Н. к.: Коваленко С. М.	395
Бризицький О. А.; Н. к.: Пестун І. В.	396
Великоіваненко К. І.; Н. к.: Деренська Я. М.	398
Вертейко Д. Ю.; Н. к.: Зборовська Т. В.	400
Виноградський В. В.; Н. к.: Коваленко С. М.	401
Гнатюк В. П.; Н. к.: Коваленко С. М.	402
Грачов О. О.; Н. к.: Бабічева Г. С.	403
Дерев'янка М. В.; Н. к.: Дядюн Т. В.	404
Дереза Є. О.; Н. к.: Крутських Т. В.	405
Жовтоніжко К. В.; Н. к.: Братішко Ю. С.	407
Захарова Я. М.; Н. к.: Деренська Я. М.	407
Кайзер Ю. М.; Н. к.: Малініна Н. Г.	409
Коляда Т. А., Калекіна Т. В., Микуленко В. К.	411
Краснопольська Т. Е.; Н. к.: Посилкіна О. В.	413
Кутова К. В.; Н. к.: Посилкіна О. В.	415
Кушнір Я. О.; Н. к.: Малініна Н. Г.	416
Лещенко В. В.; Н. к.: Лісна А. Г.	418
Маковецький А. С.; Н. к.: Коваленко С. М.	420
Масляний В. В.; Н. к.: Бондарєва І. В.	421
Машкіна О. В.; Н. к.: Ковальова В. І.	422
Ольховська О. В.; Н. к.: Шуванова О. В.	424
Орловський О. М.; Н. к.: Лісна А. Г.	425
Пілеко І. М.; Н. к.: Гладкова О. В.	427
Подгайний Д. Г.; Н. к.: Малініна Н. Г.	429
Ткаченко А. В.; Н. к.-и.: Рогуля О. Ю., Зборовська Т. В.	430
Трет'як В. С.; Н. к.: Літвінова О. В.	432
Філенко К. Б., Дядюн Т. В.	433
Фомченко С. П.; Н. к.: Літвінова О. В.	434
Хаврук М. Ю.; Н. к.: Лісна А. Г.	435
Харченко Д. С.; Н. к.: Крутських Т. В.	437
Ющенко Д. А., Посилкіна О. В.	439

ДОДАТОК В

Організаційна структура компанії

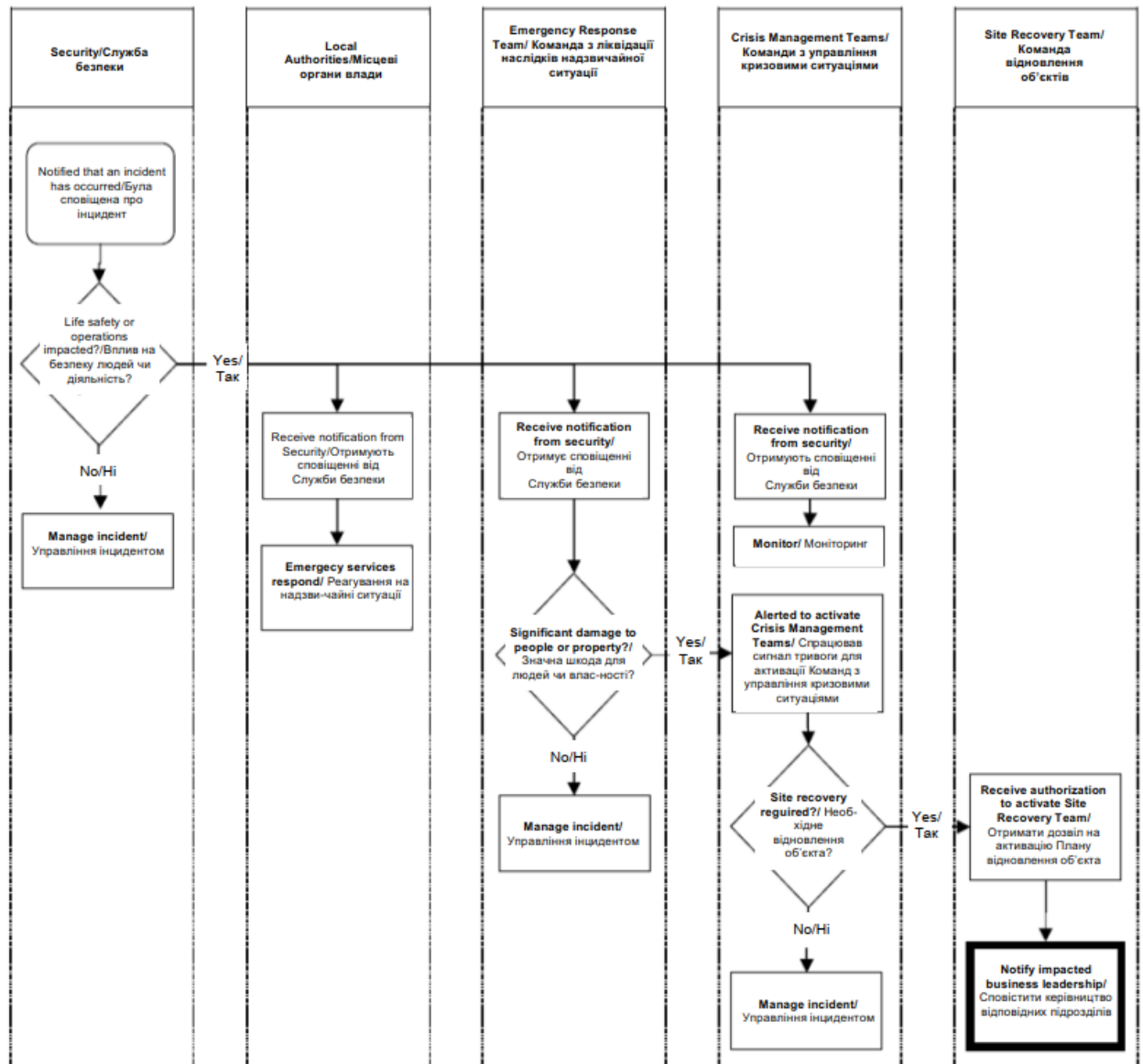


Distribution Business Continuity Plan	План безперервності бізнесу для діяльності з дистрибуції
Plan Sponsor: Head of Logistics and Distribution / Спонсор плану: Начальник відділу логістики та дистрибуції	Published Date/ Дата публікації: 19.08.2024 Last Team Review Date/ Дата останнього перегляду Командою: 16.08.2024
Plan Owner: Warehouse Manager/ Власник плану: Завідуючий аптечним складом	Last Exercise/Activation Date/ Дата останньої вправи/активації: 24.02.2022
ПІБ	
Distribution Business Continuity/ Безперервність бізнесу для діяльності з дистрибуції	
Recovery Timeframe Objective/ Цільовий часовий проміжок відновлення	
Tier 2: 1-3 days/ Рівень 2: 1-3 дні	
Critical Business Process/ Критичний бізнес-процес	
Distribute product/ Дистрибуція продукції	
Plan Summary/ Короткий зміст плану	
This plan defines the strategy and tactical plan for responding to disruptions in order to continue business operations/ Цей план визначає стратегію і тактичний план реагування на збої в роботі з метою продовження господарської діяльності.	
Location(s)/ Місцезнаходження (Місцязнаходження)	
Country / Країна	Site/ Дільниця
Ukraine	Company Warehouse (LSP – LLC Global Logistic)/ Україна Склад Компанії(постачальник логістичних послуг (LSP) — ТОВ «Глобал Лоджистік»)
Prepared by Warehouse Manager	Підготовлено Завідуючим аптечним складом
Approved by Head of Logistics and Distribution Ukraine	Затверджено Начальником відділу логістики та дистрибуції в Україні
Approved by Security Champion Ukraine Rx	Затверджено Чемпіоном з безпеки рецептурних препаратів в Україні
Approved by Ethics and Compliance Manager Ukraine	Затверджено Начальником відділу корпоративної етики та відповідності в Україні

Table of Contents

Зміст

Business Continuity/ Безперервність бізнесу	
Response sequence (outline) / Послідовність реагування (план)	1
Notification & Activation Procedures/ Процедури сповіщення та активації	4
Team Members/ Члени Команди	5
BSP Distribution Recovery Tasks/ Завдання з відновлення BSP з дистрибуції	6
Vendors with Contact Information/ Вендори з контактною інформацією	12
BSP Distribution BIA/ Аналіз впливу на бізнес (BIA) BSP з дистрибуції	13
BSP Distribution Strategy/ Стратегія BSP з дистрибуції	22
Appendix 1 Critical skill roles details Ukraine/ Додаток 1. Критично важливі ролі в Україні	23
Appendix 2 Recovery Team Ukraine Details/ Додаток 2. Інформація про Команду відновлення в Україні	24
Appendix 3 Crisis Team/ Додаток 3. Кризовий штаб	26
Appendix 4 LSP GL BSP/ Додаток 4. План безперервності бізнесу (BSP — Business Continuity Plan) LSP «Глобал Лоджистік»	29



Notification and Activation Procedures

Facility Loss (Office/Warehouse)

Notification to Business Recovery Teams

Facility Loss (Office)

Address Prosperkt Shuhkevycha 1-B, Kyiv, 02152, Ukraine

Security Personnel of Business Centre informs Office Manager about an incident.

Office Manager informs Ethics and Compliance Manager, Head of Logistics and Distribution about incident & Crisis Management team.

Head of Logistics and Distribution informs Site Recovery Team about the fact of invoking of BCP Strategy pharmaceuticals.

Facility Loss (Warehouse (WH) – Global Logistics)

Address 121a, Kyivskiy Shlyah str., City Velyka Oleksandrivka vil., Kyivska Obl, Borispilskiy Distr, 08320, Ukraine

Security Personnel of "Global Logistics" WH informs contact persons Warehouse Manager – Warehouse Manager informs Head of Logistics and Distribution, who is Site Recovery Team Lead about an incident.

Site Recovery Team Lead informs General Manager, Finance Director, Ethics and Compliance Manager about the incident.

As well as informs Site Recovery Team about the fact of invoking of BCP.

Notes:

- Local Authorities may ask of the impacted facilities until emergency response activities are completed and control is formally returned to the company.
- Legal department will advise Site Recovery team to lead in terms of Local Authorities incident notification.
- Dependent on the local resources, the Site Recovery team may comprise trained Incident Controllers and/or staff from Environmental Health and Safety.
- Dependent on the impact and consequences of the incident, the Local Crisis Management Team may be supplemented by Regional and Corporate Crisis Management Teams.

Information Technology Loss

Tech Head is responsible for reporting technology issues and invoke their business continuity plans as required. Tech Head or Global IT will notify the business of outages, including Recovery Team Lead and provide updates on the progress of recovery for impacted technologies.

SAP Tech Support is responsible for reporting technology issues in SAP

Business Partner Loss

Процедури повідомлення та активації

Втрата об'єкта (офіс/склад)

Повідомлення Команд відновлення бізнесу

Втрата об'єкта (офіс)

Адреса: Проспект Шухевича 1-В, Київ, 02152, Україна

Служба безпеки Бізнес-центру інформує офіс-менеджера компанії про інцидент, що стався.

Офіс-менеджер інформує про інцидент Начальника відділу корпоративної етики та відповідності, Начальника відділу логістики та дистрибуції та Команду з управління кризовими ситуаціями.

Начальник відділу логістики та дистрибуції інформує Команду відновлення об'єктів про факт, що потребує застосування стратегії Плану безперервності бізнесу (BCP — Business Continuity Plan) до лікарських засобів.

Втрата об'єкта (Склад (WH) — «Глобал Лоджистік»)

Адреса: вул. Київський шлях, 121а, с. Велика Олександрівка, Київська обл., Бориспільський район, 08320, Україна

Працівники служби безпеки складу «Глобал Лоджистік» інформують Завідуючого аптечним складом компанії. Завідуючий аптечним складом інформує про інцидент Начальника відділу логістики та дистрибуції, який являється Керівником Команди відновлення.

Керівник Команди відновлення інформує про інцидент Генерального директора, Фінансового директора, Начальника відділу корпоративної етики та відповідності. А також інформує Команду відновлення об'єктів про факт активації BCP.

Примітки:

- Місцеві органи влади можуть вимагати звільнення постраждалих об'єктів до завершення заходів з ліквідації наслідків надзвичайної ситуації та офіційного повернення контролю над ними компанії.
- Юридичний відділ проконсультує Команду відновлення об'єктів щодо того, як повідомити місцеві органи влади про інцидент.
- Залежно від місцевих ресурсів, до складу Команди відновлення об'єктів можуть входити підготовлені Контролери інцидентів і/або працівники Відділу охорони праці.
- Залежно від впливу та наслідків інциденту, національна Команда з управління кризовими ситуаціями може бути доповнена Регіональними та Корпоративними командами з управління кризовими ситуаціями.

Втрата інформаційних технологій

Керівник технічного департаменту відповідає за повідомлення про технологічні і за необхідності активації його планів безперервності бізнесу. Технічний директор або Глобальний Відділ інформаційних технологій повідомляє підрозділи про збої в роботі, зокрема Керівника Команди відновлення, та надає оновлену інформацію про хід відновлення постраждалих технологій. Відділ технічної підтримки SAP відповідає за повідомлення про технологічні проблеми в SAP

Втрата бізнес-партнера

Recovery Team Lead is responsible for activation of continuity arrangements for an impacted business partner for an extended period. Business partners shall notify about their outages.

Керівник Команди відновлення відповідає за активацію заходів щодо забезпечення безперервності бізнесу щодо постраждалого бізнес-партнера на тривалий період. Бізнес-партнери повинні повідомляти про збої у своїй роботі.

Notification and Activation Procedures
Team Members

Процедури повідомлення та активації
Члени Команди

Distribution Business Continuity Plan

План безперервності бізнесу для діяльності з дистрибуції

	Position/ Посада
Site Recovery Team Lead/ Керівник Команди відновлення	Head of Logistics and Distribution / Начальник відділу логістики та дистрибуції
Back-up/ Заступник Керівника Команди відновлення	Warehouse Manager/ Завідуючий аптечним складом
Recovery Team / Команда відновлення	EHS&S National Specialist / Інженер з охорони праці
	Ethics and Compliance Manager / Начальник відділу корпоративної етики та відповідності
	Security Champion Rx/ Чемпіон з безпеки рецептурних препаратів
	Customer Service Specialists / Фахівці по роботі з клієнтами
	Quality Manager/ Начальник відділу із якості
	Deputy Warehouse Manager / Заступник завідуючого аптечним складом
	Finance Director/ Фінансовий директор
	Logistics Planner / Фахівець із питань планування логістики

Team Teleconference:

+38 (050) 0000000 Site Recovery Team Lead

Back – up telephone – +38 (050) 111 11 1
WH back-up telephone - +38 044 222 22 22
Office - +38044 333-33-33

Teams  [Click here to join the meeting](#)
call in (audio only)

 **+380 89 444 4444** Ukraine, All locations
Phone  Conference ID: 111 111 111#

 pin in case you are the 1st (organizer) 55555 If connection, internet, mobile phone lost – 12-00 every day.

Additional telephone line. Detail for call:

Dial the number: +38044 555 55 55
Room number: 0000 #
PIN: 0000 #

For iPhone: +380 (44) 555 55 55,5555#5555#

Site Recovery Team Tasks Scenario Instructions:

Телеконференція Команди:

+38 (050) 0000000 Керівник Команди відновлення

Резервний номер телефону: +38 (050) 111 11 11
Резервний номер телефону складу: +38 044 222 22 22
Офіс: +38044 333-33-33

Teams  [Натисніть тут, щоб приєднатися до зустрічі](#)
зателефонуйте (тільки голосовий дзвінок)

 **+380 89 444 4444** Україна, Всі регіони
Номер телефону  Конференц-ідентифікатор: 111 111 111#

 пін-код на випадок, якщо ви 1-й (організатор) 55555 У разі втрати зв'язку, інтернет-з'єднання, мобільного телефону — 12:00 щодня.

Додаткова телефонна лінія. Інформація для дзвінка:

Зателефонуйте за номером: +38044 555 55 55
Номер кімнати: 0000 #
PIN-КОД: 0000 #

Для айфонів: +380 (44) 555 55 55,5555#5555#

Завдання Команди відновлення об'єктів — Інструкції та сценарії відновлення:

- | | |
|---|--|
| ☐ Update the tasks list below to restore minimum essential operations within your approved Recovery Timeframe Objective. | ☐ Оновіть наведений нижче список завдань, щоб відновити мінімально необхідні операції в межах затвердженого вами Цільового часового проміжку відновлення. |
| ☐ Tasks should be action oriented and concise | ☐ Завдання повинні бути орієнтовані на конкретні дії та бути стислими |
| ☐ Some initial tasks have been provided to aid in your effort | ☐ Певні початкові завдання наведено для того, щоб допомогти у ваших зусиллях |

Workforce Impact Checklist	Контрольний список щодо впливу на персонал
When a global health issue is impacting operations (e.g. Flu Pandemic or Ebola or COVID-19 etc.): 1. Monitor the progression of global health issues and follow internal/external guidance. 2. Monitor National and Local Government plans and actions which may impact business operations or staff availability (e.g. travel restrictions) 3. Notification will be organized according to Communication Plan for IMT of Employee Health Pandemic Preparedness Plan. Responsible for preparing plan is EHS&S National Specialist, Ukraine. 4. Establish teleconference meeting times as needed (see numbers above) 5. Monitor staff availability to support critical processes: • Check availability of all Site Recovery Team Members • Create a WhatsApp (or other, preferred Viber, Telegram) group for daily monitoring of the health status of the department • Check if there are safe, alternate locations that recovery team members may work (office, warehouse, home etc.) • Consider if Site Recovery Team Members are unable to reach corporate facilities - can they work from home? Check home connections (internet, VPN etc.) for all critical roles • Encourage sick employees to stay home until symptoms are passed or/and sick leave closed, according to the MOH recommendations etc. • All employees with critical roles should take their laptops home at the end of the day and work from home if they are able to visit the office/warehouse • Office personnel who are not performing "daily essential jobs" will stay at home. • Implement of Site Access Restrictions • Checking of availability of extra antivirals (if applicable) /PPE for employees performing "daily essential jobs" • Provision of extra antivirals (if applicable)/PPE for employees performing "daily essential jobs"	Коли глобальна проблема у сфері охорони здоров'я впливає на операційну діяльність (наприклад, пандемія грипу, лихоманки Ебола, COVID-19 тощо): 1 Відстежуйте розвиток глобальних проблем у сфері охорони здоров'я та дотримуйтеся внутрішніх/зовнішніх інструкцій. 2 Відстежуйте плани та дії національних і місцевих органів влади, які можуть вплинути на господарську діяльність або доступність персоналу (наприклад, обмеження на поїздки) 3 Сповіщення буде організовано відповідно до Плану комунікації для Команди управління інцидентами (ИМТ) щодо Плану готовності працівників до пандемії. Відповідальним за підготовку плану є Інженер з охорони праці, Україна. 4 Визначте час проведення телеконференцій за потреби (див. номери телефонів вище) 5 Відстежуйте доступність персоналу для підтримки критично важливих процесів: • Перевіряйте доступність усіх членів Команди відновлення • Створіть групу у WhatsApp (або іншому месенджері, наприклад Viber, Telegram) для щоденного відстеження стану здоров'я в підрозділі • Перевіряйте, чи існують безпечні альтернативні місця, де можуть працювати члени Команди відновлення об'єктів (офіс, склад, дім тощо). • Якщо члени Команди відновлення не можуть дістатися до корпоративних об'єктів, чи можуть вони працювати з дому? Перевіряйте домашні з'єднання (інтернет, VPN тощо) для всіх критично важливих ролей • Заохочуйте хворих працівників залишатися вдома до зменшення інтенсивності симптомів або/та закриття лікарняного, відповідно до рекомендацій МОЗ тощо. • Усі працівники з критично важливими ролями повинні брати ноутбуки в кінці робочого дня додому і працювати з дому, якщо мають змогу відвідувати офіс/склад • Офісний персонал, який не виконує «щоденну важливу роботу», повинен залишатися вдома. • Впровадьте обмеження доступу до об'єктів • Перевірте наявність додаткових противірусних засобів (за необхідності) / засобів індивідуального захисту (ЗІЗ) для працівників, які виконують «щоденну необхідну роботу» • Забезпечте працівників, які виконують «щоденну необхідну роботу», додатковими противірусними засобами (за наявності) / ЗІЗ

• Ensuring of availability of respirators and masks - placement of additional masks stock in the WH on an ongoing basis. • Purchasing a thermometer to the WH. Temperature control will be done at check point before entering WH • Implementation of social distancing measures & other MOH requirements & additional sanitation and disinfection measures according to the developed schedule • Registration of special permits for movement and letters in conjunction with the legal department (if applicable). Letters confirming the criticality of being at the workplace and the impossibility of remote work. • Transportation employees performing "daily essential jobs" from home to office in case of absence of sickness symptoms (in case if agreed & required) No employee will be allowed back to the premises without any symptoms and a written document is obtained from the medical care physician that the employee is medically fit to return to work, or testing negative etc. When a global health issue is <u>no longer impacting</u> your operations: 1. Communicate HR policies and Employee Health guidance to staff 2. Monitor and actively seek to improve staff morale and emotional well being 3. Update your business continuity plan based on experience	• Забезпечте наявність респіраторів та масок. — Розмістіть додатковий запас масок на території складу на постійній основі. • Закупіть термометр для складу. Контроль температури буде здійснюватися на контрольно-пропускному пункті перед входом до складу • Впровадьте заходи соціального дистанціювання та інших вимог МОЗ, а також додаткових санітарно-гігієнічних і дезінфекційних заходів згідно з розробленим графіком • Оформлюйте спеціальні дозволи на пересування та листи спільно з юридичним відділом (за необхідності). Листи, що підтверджують критичність знаходження на робочому місці та неможливість виконувати дистанційно роботу • Забезпечте транспортування працівників, які виконують «щоденну необхідну роботу», з дому до офісу в разі відсутності симптомів хвороби (якщо це погоджено керівником компанії та вимагається) Жоден працівник не буде допущений до приміщення за наявності будь-яких симптомів та поки від лікаря не буде отримано письмовий документ про те, що працівник за станом здоров'я може повернутися до роботи або про негативний результат тесту тощо. Коли глобальна проблема у сфері охорони здоров'я <u>більше не впливає</u> на вашу діяльність: 1 Доведіть до відома персоналу політику управління персоналом та інструкції з охорони здоров'я працівників 2 Відстежуйте та активно намагайтеся покращити моральний та емоційний стан персоналу 3 Оновіть свій план безперервності бізнесу на основі отриманого досвіду
--	--

Facility Impact Checklist	Контрольний список щодо впливу на об'єкт
When notified of a facility (Office) loss or outage for your operations: 1. Head of Logistics and Distribution informs Site Recovery Team about the fact of invoking of BCP. 2. Warehouse Manager provides access for Site Recovery Team to a temporary work area in the warehouse or staff work from home. 3. Head of Logistics and Distribution agrees to inform distributors in case if needed about incident and possible delays in supplies. 4. Tech Head prepares IT resources if needed. 5. The Company acts and inform Local Authorities according to the BCP Strategy. 6. Original documents to store at outsource archive provider or in the secure safe. 7. To find department safe with documents and recover original documents from lost office. 8. Disaster Recovery Team implements plan of return to normal operations. 9. Update your business continuity plan based on experience	У разі отримання повідомлення про втрату об'єкта (офісу) або збоїв в роботі для вашої діяльності: 1. Начальник відділу логістики та дистрибуції інформує Команду відновлення про факт активації ВСР. 2. Завідуючий аптечним складом надає доступ Команді відновлення роботи до тимчасової робочої зони на складі або персонал працює з дому. 3. Начальник відділу логістики та дистрибуції зобов'язується в разі необхідності інформувати дистриб'юторів про інцидент і можливі затримки в постачанні. 4. Технічний директор готує IT-ресурси в разі необхідності. 5. Компанія діє та інформує місцеві органи влади відповідно до Стратегії щодо ВСР. 6. Оригінали документів зберігаються в архіві аутсорсингового постачальника архівних послуг або в надійному сейфі. 7. Знайдіть сейф відділу з документами та отримайте оригінали документів із втраченого офісу. 8. Команда з відновлення впроваджує план повернення до нормальної роботи. 9. Оновіть свій план безперервності бізнесу на основі отриманого досвіду
When notified of a facility (Warehouse) loss or outage for your operations: 1. Global Logistic Dispatcher informs contact person Warehouse Manager about incident. 2. What impact will the incident have on operations and who do you need to inform? Staff safety reporting: Warehouse, Logistic, Customer Service, related to internet system (delivery, income, sale operation, order management). Some Third Parties (GL locally, clients locally, State authority – Customs Agency) may be out of connection. 3. How will you prioritize critical activities? Warehouse goods security, medicines patient access - > inbound trucks (incl customs clearance), sale operations – order management, intraorganizational communication. 4. Warehouse Manager notify Head of Logistics and Distribution, Ethics and Compliance Manager of situation. Head of Logistics and Distribution Department contact Site Recovery Team members and General Manager and Customer Service and Logistics Lead. a. Advise on initial meeting location (office) and time b. Advise staff to call the site status for updates on facility status. 5. Attend Site Operations recovery planning meetings to coordinate efforts.	При отриманні повідомлення про втрату об'єкта (складу) або збоїв в роботі для вашої діяльності: 1. Диспетчер «Глобал Лоджистік» інформує про інцидент контактну особу— Завідуючого аптечним складом. 2. Який вплив інцидент матиме на операційну діяльність і кого необхідно поінформувати? Звітування про безпеку персоналу: Склад, відділ логістики, відділ обслуговування клієнтів, ролі, пов'язані з інтернет-системою (доставки, фінансів, продажів, управління замовленнями). Окремі треті сторони («Глобал Лоджистік» на місцевому рівні, клієнти, державні органи — Митна служба) можуть не мати зв'язку. 3. Як визначити пріоритетність критично важливих видів діяльності? Безпека продукції на складі, доступ пацієнтів до лікарських засобів — > в'їзд вантажівок (включно з митним оформленням), операції з продажів — управління замовленнями, внутрішньоорганізаційна комунікація. 4. Завідуючий аптечним складом повідомляє про ситуацію Начальника відділу логістики та дистрибуції в Україні, Начальника відділу корпоративної етики та відповідності, Начальник відділу логістики та дистрибуції зв'язується з членами Команди відновлення, Генеральним директором і Керівником з обслуговування клієнтів, щоб: a. Повідомити про місце (офіс) і час проведення першої наради b. Рекомендувати працівникам телефонувати на об'єкт для отримання оновленої інформації про стан об'єкта. 5. Беріть участь у нарадах з планування відновлення роботи об'єкта для координації зусиль

6. Perform initial business recovery team meeting - Provide facility updates & inventory status received from site operations - Develop work plan for completing recovery tasks. 7. To inform UL General Manager and Operation Manager to order trucks and load them with remaining goods. Global Logistics has BCP plan, we have contact possibility for recovery/or contract break in case of disaster. 8. To organize working space for WH staff (3 people) in office or at home. 9. Head of Logistics and Distribution inform the Insure or Insurer's representative about insured event occurrence immediately but in any case, not later than 24 hours from the moment the Insured and send to the Insurer the message in writing about insured event not later than 48 (forty-eight) hours from the moment the Insured. 10. To ask Distributor for possibility to sell <u>remaining</u> goods to them 11. Warehouse Manager inform State Authority about incident and stop work warehouse in 30 calendar days 12. CS specialist & Distribution Manager inform Distributors about delay of warehouse & distribution operations. 13. Initiate with Global Logistic reconstruction of facilities, timelines for reconstruction, (according to the contact - in 3 months- Receiving Licenses). 14. Global Logistic to provide another facility in 30 days. 15. To consider the placement of products in transit in the GL customs warehouse /or and delivery stop. To consider transit goods return back at site/intermediate HUB, LSP HUB, etc, if trucks don't cross the border 16. If we manage to find a spare, premises prepare new WH in current Logistics Service Provider to receive Licenses for new WH. 17. If there is no possibility to organize premises with Global Logistics or Company Consumer/Distributor to find a new WH provider (on the basis of benchmarking). 18. During the period of solving the issue with the organization of a new WH premises, Salus (logistics Hub in France) can act as a shipper of goods directly to distributors. All settings are made and in case of loss of the local WH, the goods can be shipped directly from Salus based on import contracts with local Distributors. Contracts to be prepared additionally by commercial department 19. All in-transit stock that still didn't cross UA border to be re-directed to Salus MMW France for further storage. "Multi Market Warehouse" also "MMW Salus" means the third-party CEVA FREIGHT MANAGEMENT FRANCE SAS MULTI MARKET WAREHOUSE located	6 Проведіть першу нараду Команди відновлення бізнесу, щоб: - Надати оновлену інформацію про стан об'єкта та інвентаризацію, отриману від операційної служби об'єкта - Розробити робочий план для виконання завдань з відновлення. 7 Поінформуйте Генерального директора та Операційного директора «Глобал Лоджистік» для замовлення вантажівок і завантаження їх продукцією, що залишилися. У «Глобал Лоджистік» є план BCP, у нас є можливість зв'язатися для відновлення або розірвання договору в разі стихійного лиха. 8 Організуйте робочий простір для персоналу складу (3 особи) в офісі або вдома. 9 Начальник відділу логістики та дистрибуції повинен негайно повідомити Страхувальника або представника Страхувальника про настання страхового випадку, але в будь-якому разі не пізніше ніж за 24 години з моменту настання страхового випадку, а також надіслати Страхувальнику письмове повідомлення про страховий випадок не пізніше ніж за 48 (сорок вісім) годин з моменту настання страхового випадку. 10 Зверніться до Дистриб'юторів із запитом про можливість продажу <u>залишків</u> продукції 11 Завідуючий аптечним складом повинен повідомити державні органи про інцидент і зупинити роботу складу на 30 календарних днів 12 Керівник департаменту по роботі з каналами збуту та дистрибуції інформує Дистриб'юторів про затримку складських і дистрибуційних операцій. 13 Ініціюйте з «Глобал Лоджистік» реконструкцію об'єктів; терміни реконструкції (згідно з контактною інформацією — протягом 3 місяців — отримання дозволів). 14 «Глобал Лоджистік» має надати інше приміщення на період 30 днів. 15 Розгляньте можливість розміщення товарів у дорозі на митному складі «Глобал Лоджистік» та/або зупинку доставки. Розгляньте можливість повернення транзитних товарів назад на дільницю/проміжний хаб, хаб LSP, якщо вантажівки не перетнули кордон тощо. 16 Якщо вдається знайти вільне приміщення, підготуйте новий склад у поточного постачальника логістичних послуг для отримання ліцензії на новий склад. 17 Якщо немає можливості організувати роботу з «Глобал Лоджистік» або Споживачем/Дистриб'ютором Компанії знайдіть нового постачальника складських послуг (на підставі тендеру). 18 На період врегулювання питання з організацією нового складського приміщення, склад Салюс (логістичний хаб у Франції) може виступати в ролі безпосереднього відправника продукції дистриб'юторам. Усі приготування зроблені, тому в разі втрати локального складу продукція може відвантажуватися безпосередньо з Салюс на підставі договорів щодо імпорту з місцевими дистриб'юторами. Договори готуються додатково комерційним відділом 19 Усі запаси в транзиті, які ще не перетнули кордон України, мають бути перенаправлені на склад Salus MMW France для подальшого зберігання.
--	---

at Aéroport International de Salus - ZAC N°1-Rue Henri Guillaumet - 51320 Bussy Lettrée - France. 20. Instructions to be provided by a satellite line for connections (Line to be provided proactively to KN) 21. If there is impact on WH premises 3 people shall go to office or work from home+ in case if laptops are lost - they will receive laptops in office. During intense period warehouse staff to take laptops home after warehouse visiting.	«Багатонаціональний склад» або «MMW Salus» — це третя сторона CEVA FREIGHT MANAGEMENT FRANCE SAS MULTI MARKET WAREHOUSE, розташована за адресою: Aéroport International de Salus — ZAC N°1-Rue Henri Guillaumet — 51320 Bussy Lettrée — France. 20 Інструкції, які мають бути надані по супутниковій лінії зв'язку (Лінія має бути надана заздалегідь до KN) 21 У разі ураження приміщення складу 3 особи повинні бути в офісі або працювати з дому + у разі втрати ноутбуків — отримати ноутбуки в офісі. Під час інтенсивного періоду працівники складу забирають ноутбуки додому після відвідування складу.
22 To find safe with documents and recover original documents from lost WH. Another original documents store at outsource archive provider. 23 Keep notifying key customers and critical vendors, local authorities on impact 24 Communicate regularly with site operations and Crisis Teams as required. 25 Communicate authority and regulation. 26 Plan for return to normal operations. 27 By electricity: - 2 generators as a measure done by GL for the risk of infrastructure issues or power outages - main electricity line – Village V.Oleksandrivka power - reserved electricity railway line (considered as critical infrastructure) -generators on the territory with reserved fuel – daily controlled + 2 fuel supplier (БЕСТ КАРД & ВИТОЛ) - with active operation of the complex - 52.5 hours, with limited (minimum necessary energy supply) - 81.5 hours 28 Update your continuity plan based on experience 29 In case of any risk associated with warehouse closure, road connection lost (military risk etc) Head of Logistics & Distribution dep will inform about the incident Inbound flow interested stakeholders such as E2E team, KN LCC, Security team and act in accordance with SOP-344-XX Prevention and management of CARGO theft, SOP-352-XX Distribution incident management	22 Знайдіть сейф з документами та отримайте оригінали документів з втрачених ноутбуків. Ще одне сховище оригіналів документів має бути в аутсорсингового постачальника архівних послуг. 23 Продовжуйте інформувати ключових клієнтів, критично важливих постачальників і місцеві органи влади про наслідки 24 Регулярно підтримуйте зв'язок з персоналом на об'єктах і Кризовими штабами, якщо це необхідно 25 Повідомте відповідні державні регулюючі органи про інцидент . 26 Складіть план повернення до нормальної роботи 27 Забезпечення електропостачанням: - 2 генератори як захід, вжитий компанією «Глобал Лоджистік» на випадок ризику виникнення проблем з інфраструктурою або збоїв в електропостачанні - основна лінія електропередач — с. В. Олександрівка - резервна залізнична лінія електропередач (складський комплекс розглядається як об'єкт критичної інфраструктури) - генератори на території із зарезервованим паливом — щоденний контроль + 2 постачальники палива (БЕСТ КАРД та ВИТОЛ)- при активній роботі комплексу – 52,5 години, при обмеженому (мінімально необхідному енергозабезпеченні) – 81,5 година 28 Оновіть свій план безперервності бізнесу на основі отриманого досвіду 29 У разі виникнення будь-якого ризику, пов'язаного із закриттям складу, втратою дорожнього сполучення (військовий ризик тощо), Начальник відділу логістики та дистрибуції України інформує про інцидент зацікавлені сторони, такі як команда E2E, KN LCC, служба безпеки, і діє відповідно до SOP-344-XX «Запобігання та управління крадіжками ВАНТАЖІВ», SOP-352-XX «Управління інцидентами у сфері дистрибуції»
ZNPP Impact Checklist 1. After the official notification of an incident at the ZNPP (Zaporizhzhia Nuclear Power Plant), employees must go home (during working hours) or stay at home until the next notification 2. Head of Logistics and Distribution Department contact Site Recovery Team members and General Manager and Customer Service and Logistics Lead. a. Advise on initial meeting time b. Advise staff to call the site status for updates on facility status.	Контрольний список щодо впливу ЗАЕС 1. Після офіційного повідомлення про інцидент на ЗАЕС (Запорізька Атомна Електростанція) співробітники повинні відправитися додому (в робочий час) або залишатися вдома до наступного сповіщення. 2. Начальник відділу логістики та дистрибуції зв'язується з членами Команди відновлення, Генеральним директором, Керівником з обслуговування клієнтів та Logistics Lead, щоб: a. Повідомити про час проведення першої наради

- The warehouse manager asks the warehouse provider to confirm that the ventilation in the warehouse is turned off, the premises are under security until further decisions. - Notification will be organized according to the Communication Plan for the Incident Management Team (IMT) regarding the Action Plan When the global problem with ZNPP no longer affects your activities: - Conduct radiation level measurements: Contact professional radiation measurement services to assess potential contamination of the warehouse. This will help determine the level of radiation in the warehouse and determine the necessary measures to ensure the safety of employees. - Disinfection: If radiation contamination is detected, it is important to take measures to disinfect premises and equipment. Consider hiring professional decontamination services that specialize in cleaning up radiation contamination. - It is necessary to evaluate and check the products stored in the warehouse (conducted by state bodies for product quality control). Take into account the possibility of destroying contaminated products. - Notification of security services: Notify relevant security services, medical facilities and authorities of detected radiation contamination and measures taken to minimize it. - Protection of employees : appropriate protection must be provided for employees returning to the warehouse. This may include special radiation protection, as well as training in safety and the use of special equipment.	- Рекомендувати працівникам телефонувати на об'єкт для отримання оновленої інформації про стан об'єкта. - Завідуючий аптечним складом просить складського провайдеру підтвердити, що в складі вимкнено вентиляцію та приміщення знаходяться під охороною до наступних рішень - Сповіщення буде організовано відповідно до Плану комунікації для Команди управління інцидентами (IMT) щодо Плану дій Коли глобальна проблема з ЗАЕС більше не впливає на вашу діяльність: - Здійснення замірів радіаційного рівня: Зверніться до професійних служб з вимірювання радіації для оцінки потенційного забруднення складу. Це допоможе визначити рівень радіації на території складу та визначити необхідні заходи для забезпечення безпеки працівників. - Проведення дезінфекції: Якщо виявлені забруднення радіацією, важливо вжити заходів для дезінфекції приміщень та обладнання. Розгляньте можливість залучення професійних служб з дезінфекції, які спеціалізуються на очищенні від радіаційного забруднення. - Необхідно провести оцінку та перевірку продукції, яка зберігається на складі (проводять державні органи з контролю за якістю продукції). Врахувати можливість знищення зараженої продукції. - Повідомлення служб безпеки: Повідомте відповідні служби безпеки, медичні установи та органи влади про виявлене радіаційне забруднення та вжиті заходи для його мінімізації - Захист працівників: необхідно забезпечити належний захист для працівників, які повертаються на склад. Це може включати спеціальний захист від радіації, а також навчання з питань безпеки та використання спеціального обладнання
<i>Technology Impact Checklist</i>	<i>Контрольний список щодо впливу на технології</i>
When notified of a technology loss or outage for your operations: - Assess impact on processes and critical reporting - Notify stakeholders LSP/Management/Clients/Supplier of delayed processing - Contact IT support and organize a delivery of IT equipment for key users: - Verify the accuracy and completeness of recovery data for restored applications. - Plan for return to normal operations - Current operations, if possible, to be finalized, or put on hold for additional clarification. According to the UA model patient access is not under the risk due to:Distributors IOH average 35 D Company stock at wh average 45-60 D Check Medically critical SKU enough cover at distr level and Company Wh. Weekly client's dispatches might be re-considered to monthly or after disruption finish, tenders to be	У разі отримання повідомлення про втрату або збій у роботі технології: - Оцініть вплив на процеси та критичну звітність - Повідомте зацікавлені сторони LSP/керівництво/клієнтів/постачальника про затримку в обробці даних - Зверніться до відділу IT-підтримки та організуйте доставку IT-обладнання для ключових користувачів: - Перевірте точність і повноту відновлених даних для відновлених програм. - Складіть план повернення до нормальної роботи - За можливості завершіть поточні операції або призупиніть їх для додаткового з'ясування ситуації. Згідно з моделлю України, доступ пацієнтів не перебуває під загрозою через: Дистриб'ютори IOH — в середньому 35 днів Запаси кмпанії на складі — в середньому 45-60 днів Перевірте критично важливі з медичного погляду SKU мають достатній запас на рівні дистриб'ютора та на складі компанії. Щотижневі відправлення клієнтам можна переглянути на щомісячні або після завершення

prioritized and outbound operations to be discussed with Commercial. If the warehouse system does not work, use the last saved version for work, keep records on paper with subsequent entry into the accounting system. In case if emergency dispatch is required to perform manual pick-up according to the BCP. If WMS (WH system) is available – to use the system and after CERPS renewal update accordingly. If no systems are available to use available application, for instance – Excel/Word file for orders and pick up. In case if computer/printer is not available templates are pre-print with empty lines for products on the warehouse. STP to be written & approved for emergency situation with mentioning price- list to be used (last available version or FD advise). Credit control and payment terms to be considered and approved by FD & GM separately for emergency dispatches. 7. If any cyber-attack happened, communication would be sent not to use external resources, do not browse state government sites, to limit transaction in email and browse only internal company sites with focus to secure company systems. Act according to the Company guide. 8. Discussed the risk of constantly supporting goods receipt and shipment with non-working WMS and SAP.	збоїв, визначити пріоритетність тендерів та обговорити вихідні операції з комерційним відділом. Якщо складська система не працює, використовуйте для роботи останню збережену версію, ведіть облік на папері з подальшим внесенням в облікову систему. У разі необхідності екстреного відправлення здійснюйте ручне відвантаження відповідно до BCP. Якщо доступна система WMS (складська система) — використовуйте систему і після оновлення CERPS оновіть її відповідним чином. За відсутності систем — використовуйте наявну програму, наприклад Excel/Word файл для оформлення замовлень і відвантаження продукції. На випадок відсутності комп'ютера/принтера шаблони попередньо роздруковують з порожніми рядками для продукції на складі. STP повинні бути розроблені та затверджені для надзвичайних ситуацій із зазначенням прайс-листа, який буде використовуватися (остання доступна версія або вказівка Фінансового директора (FD)). Умови кредитування та оплати мають бути розглянуті та затверджені FD та Генеральним директором (GM) окремо для екстрених відправлень. 7. У разі кібератаки має бути надіслано повідомлення з проханням не використовувати зовнішні ресурси, не переглядати сайти державних органів влади, обмежити транзакції в електронній пошті та переглядати лише внутрішні сайти компанії з наголосом на безпеці систем компанії. Дійте відповідно до інструкцій компанії. 8. Обговоріть ризик постійного отримання та відвантаження товарів при непрацюючих WMS і SAP.
---	---

9. Alternative communication lines can you use/ Альтернативні лінії зв'язку, які ви можете використовувати			
	Scenario detail/ Дані про сценарій	Impact/ Вплив	Action/ Дії
Scenario No.1 / Сценарій № 1	- Internet interruption (could be area-restricted)/ Збій у роботі інтернету (може бути обмежений територіально) - Mobil work - Mobil internet work (depends on Providers)/ Мобільний зв'язок працює - Мобільний інтернет працює (залежить від провайдера) - Electricity work/ Електропостачання працює	- Lost access to CERPS / Global services/ Втрата доступу до CERPS/глобальних сервісів - Loc Servers / Shared folders will be available only from office, not available from home/ Локальні сервери / спільні папки будуть доступні лише з офісу, не доступні з дому - Office -IP-phone depends on Vendors/ Офісний IP-телефон залежить від постачальників	- Connection via mobile (computer as well)/ З'єднання через мобільний телефон (комп'ютер також) - Test Mobil internet via other mobile providers (sim card)/ Тест мобільного інтернету через інших мобільних провайдерів (сім-карту)
Scenario No.2 / Сценарій № 2	- Internet work / Інтернет працює - Mobile interruption/ Збій у роботі мобільного зв'язку - Electricity work/ Електропостачання працює	No crucial impact as all system access are in place/ Не має критичного впливу, оскільки доступні всі системні сервіси	- Connection via messengers/ З'єднання через месенджери - Connection through IP-tel/ З'єднання через IP-телефон - Selection of sim card of another workable providers/ Вибір сім-карти іншого працездатного оператора
Scenario № 3 – / Сценарій № 3 –	- Internet interruption / Збій у роботі інтернету - Mobile interruption/ Збій у роботі мобільного зв'язку - Electricity interruption/ Збій електропостачання	Critical damage/ Збій електропостачання	- Global team work as per last available / posted materials/ Глобальна командна діє згідно з останніми доступними/опублікованими матеріалами - CSC committee materials at Global Share folder/ Матеріали комітету CSC доступні в папці Global Share
10. All information on work in SAP is stored (Journey to Cloud)-J2C Pharma Middleware B2B Interface and SFT Connectivity Setup for ULG/ Уся інформація про роботу в SAP зберігається (Journey to Cloud) — J2C Pharma Middleware B2B Interface and SFT Connectivity Setup for ULG 11. Currently, Global Logistics uses two optical Internet lines and the Starlink satellite system has been installed. The lines are independent, optical, connected underground from different sides of the Global Logistics building and from different telecommunications nodes. According to information from providers, Internet operation under existing conditions can be guaranteed for 12+ hours, based on the availability of batteries at telecommunications nodes. Option 1: Kyivstar Internet line Option 2: Inter-Telecom Internet line			

Option 3: Satellite Internet Starlink. Наразі на Глобал Лоджистік використовується дві оптичні лінії Інтернет та проведений монтаж супутникової системи Starlink. Лінії є незалежними, оптичними, підключені підземним шляхом з різних сторін будівлі Глобал Лоджистік та від різних телекомунікаційних вузлів. По інформації від провайдерів, роботу Інтернет в існуючих умовах можна гарантувати протягом 12+ годин, спираючись на наявність батарей на телекомунікаційних вузлах. Варіант 1: лінія Інтернет Київстар Варіант 2: лінія Інтернет Інтер-Телеком Варіант 3: Супутниковий Інтернет Старлінк. 12. For communication, satellite line from the office can be used, in the absence of other means of communication/ Для зв'язку можна використовувати супутникову лінію з офісу, за відсутності інших засобів зв'язку 13. Update your continuity plan based on experience/ Оновіть свій план безперервності бізнесу на основі отриманого досвіду

Business Partner Impact Checklist	Контрольний список щодо впливу на бізнес-партнерів
When notified of a business partner (Distributor/Customs Clearance Broker/Destruction of goods) loss or outage for your operations: 1. Assess impact of outage 2. Notify stakeholders of delayed processing. 3. To analyze a business alternative partner need: - o alternative broker activities through distributors if required/ using KN local representatives as an extra-mitigation measure - o several alternative distributors for goods selling – no impact to company - o destruction- agreement when needed – not urgent operations, but necessary to ensure in short term for License conditions, contact other tender participants in case of urgent need 4. To conduct negotiations with alternative partner about future way of working (f.e. increasing of turnover). 5. Plan for return to normal operations 6. Update your continuity plan based on experience	У разі отримання повідомлення про втрату або збоїв в роботі бізнес-партнера (дистриб'ютора / митного брокера / партнера з утилізації продукції): 1. Оцініть вплив збоїв у роботі 2. Повідомте зацікавленим сторонам про затримку в обробці. 3. Проаналізуйте потребу в альтернативному бізнес-партнері: a. альтернативна брокерська діяльність через дистриб'юторів, якщо потрібно / використання місцевих представників KN як додатковий захід пом'якшення наслідків b. кілька альтернативних дистриб'юторів для продажу продукції — без впливу на компанію c. утилізація — угода за необхідності — не термінові операції, але необхідні для забезпечення виконання ліцензійних умов у короткі терміни; в разі нагальної потреби зв'яжіться з іншими учасниками тендеру 4. Проведіть переговори з альтернативним партнером про майбутній спосіб роботи (наприклад, збільшення обороту). 5. Складіть план повернення до нормальної роботи 6. Оновіть свій план безперервності бізнесу на основі отриманого досвіду

Vendors with Contact Information

LLC "Global Logistics"

ПІБ
 Contact e-mail potapenko@gl.com.ua Address 121a,
 Kyivskiy Shlyah str.,
 City Velyka Oleksandrivka vil.,
 State/Province Kiyivska Obl, Borispilskiy Distr,
 ZIP/Postal Code 08320
 Country Ukraine
 Main Phone +38 (044) 444 44 44 (int. 4444)
 Alternate Phone mob. +38 (097) 1111111

ПІБ
 Contact e-mail shevchenko@gl.com.ua
 Address 121a, Kyivskiy Shlyah str.,
 City Velyka Oleksandrivka vil.,

Вендори з контактною інформацією

ТОВ «Глобал Лоджистік»

ПІБ
 Контактна електронна пошта: potapenko@gl.com.ua
 Адреса: вул. Київський шлях, 121а
 Населений пункт: с. Велика Олександрівка
 Область/Район: Київська обл., Бориспільський р-н
 Поштовий індекс: 08320
 Країна: Україна
 Основний номер телефону: +38 (044) 444 44 44 (внутр. 4444)
 Альтернативний номер телефону: моб. +38 (097) 1111111

ПІБ
 Контактна електронна адреса: shevchenko@gl.com.ua
 Адреса: вул. Київський шлях, 121а
 Населений пункт: с. Велика Олександрівка

State/Province Kiyivska Obl, Borispilskiy Distr,
ZIP/Postal Code 08320
Country Ukraine
Main Phone +38 (044) 444 44 44 (int. 1122)
Alternate Phone mob. +38 (067) 333-33-33

ПІБ

Contact e-mail ukrainka@gl.com.ua
Address 121a, Kyivskiy Shlyah str.,
City Velyka Oleksandrivka vil.,
State/Province Kiyivska Obl, Borispilskiy Distr,
ZIP/Postal Code 08320
Country Ukraine
Main Phone +38 (044) 444 44 44 (int. 2222)
Alternate Phone mob. +38 (067) 222 22 22

Область/Район: Київська обл., Бориспільський р-н
Поштовий індекс: 08320
Країна: Україна
Основний номер телефону: +38 (044) 444 44 44 (внутр. 1122)
Альтернативний номер телефону: моб. +38 (067) 333-33-33

ПІБ

Контактна електронна адреса: ukrainka@gl.com.ua
Адреса: вул. Київський шлях, 121а,
Населений пункт: с. Велика Олександрівка
Область/Район: Київська обл., Бориспільський р-н
Поштовий індекс: 08320
Країна: Україна
Основний номер телефону: +38 (044) 444 44 44 (внутр. 2222)
Альтернативний номер телефону: моб. +38 (067) 222 22 22

Business Continuity Strategy Distribution

1. WORKFORCE IMPACT (e.g., global health emergency, Flu Pandemic, Covid 19 Pandemic, regional disaster)

Business continuity will be required for critical processes when MOH will announce Pandemic situation and therefore office closure plans should be implemented. So, scenario is as follows:

- MOH announce of pandemic;
- Home office operations launch;
- Pandemic outbreaks around the world;
- Confirmed cases of pandemic in Ukraine.

Стратегія безперервності бізнесу з дистрибуції

1. ВПЛИВ НА ПЕРСОНАЛ (наприклад, глобальна надзвичайна ситуація у сфері охорони здоров'я, пандемія грипу, пандемія Covid 19, регіональна катастрофа)

Забезпечення безперервності бізнесу необхідне для критично важливих процесів, коли МОЗ оголошує пандемічну ситуацію, а отже, необхідно впроваджувати плани закриття офісів. Отже, сценарій виглядає так:

- МОЗ оголошує пандемію;
- Запуск роботи з дому;
- Спалахи пандемії по всьому світу;
- Підтверджені випадки пандемії в Україні.

Critical Skill Set/Role/ Критичні навички/ролі	Can work remotely? (Y/N)/ Чи можуть працювати віддалено? (Так/Ні)	Minimum People Required/ Мінімальна кількість необхідних людей	Total People trained in Role/ Усього людей, які пройшли підготовку з ролі	Notes/ Примітки
Managing WH - to control dispatches, incoming and WH activities. Deputy Warehouse Manager (special qualification)/ Управління складом — контроль за відправленнями, надходженням та діяльністю	N/ Hi	1	2 in department /2 у відділі	Warehouse manager — need special pharma education, courses and experience / Завідуючий аптечним складом — необхідна спеціальна фармацевтична освіта, курси та досвід роботи

на складі. Заступник завідувачого аптечним складом (спеціальна кваліфікація)				
Qualified person (to control incoming control, batch release and quality activities)/ Уповноважена особа (для здійснення вхідного контролю, випуску серій та контролю якості)	N/ Hi	1	2 in QMS/2 в системі менеджменту якості (QMS)	Need special pharma education, courses and experience/ Потрібна спеціальна фармацевтична освіта, курси та досвід роботи
CERPS system goods invoices creation/ Створення товарних накладних в системі CERPS	Y/ Так	1	3	Staff for orders operating. The need is to have computer with CERPS installed. / Персонал для роботи з замовленнями. Необхідно мати комп'ютер з встановленою системою CERPS.
Receiving Orders from distributors/ Отримання замовлень від дистриб'юторів	Y/ Так	1	3	One person can do this and the previous if needed./ Цю та попередню функцію може виконувати одна людина, якщо необхідно.
Organizing supply activities (orders, transport, logistic, import of goods, etc.)/ Організація діяльності з постачання (замовлення, транспорт, логістика, імпорту товарів тощо)	Y/ Так	1	2	Logistics Planner, Head of L&D dep as a back-up./ Фахівець із планування логістики, Начальник відділу логістики та дистрибуції, як резервний варіант.
Logistics control (documents preparation for export/import, customs clearance)/ Контроль логістики (підготовка документів для експорту/імпорту, митне оформлення)	Y/ Так	1	2	One person can do this and the previous if needed./ Цю та попередню функцію може виконувати одна людина, якщо необхідно.

Steps to improve workforce preparedness:

☐ Refresher training of process for critical role back ups

☐ Ensure laptops are taken home during public health crisis for remote work.

☐ 2. FACILITY IMPACT

Use the circumstances outlined below when completing this section:

- All resources in the work area used to accomplish the critical processes have been destroyed.
- Critical operations will be affected immediately and for at least 30 days.
- The incident occurred during peak processing period

Кроки для покращення готовності персоналу:

☐ Повторне навчання з процесів для резервних критично важливих ролей

☐ Забезпечте, щоб під час кризи у сфері охорони здоров'я працівники забирали ноутбуки додому для віддаленої роботи.

☐ 2. ВПЛИВ НА ОБ'ЄКТ

При заповненні цього розділу враховуйте обставини, викладені нижче:

- Усі ресурси в робочій зоні, що використовуються для виконання критичних процесів, були знищені.
- Критичні операції буде порушено негайно та щонайменше на 30 днів.
- Інцидент стався під час пікового періоду обробки даних

EQUIPMENT & SUPPLIES LIST ANY UNIQUE SUPPLIES and UNIQUE EQUIPMENT required for recovery of essential operations. (No need to list basic office supplies like: pen, paper, fax, stapler, etc.) / ОБЛАДНАННЯ ТА МАТЕРІАЛИ ПЕРЕЛІЧІТЬ УСІ УНІКАЛЬНІ МАТЕРІАЛИ та УНІКАЛЬНЕ ОБЛАДНАННЯ, необхідні для відновлення основних операцій. (Не потрібно перераховувати базове канцелярське приладдя, таке як: ручка, папір, факс, степлер тощо).

ПІБ	Describe equipment/supply here or indicate: None required./ Опишіть обладнання/матеріали тут або вкажіть: Не застосовується
Ukraine / Україна	6 Laptops (4 as minimum) with all installed applications and VPN excess Recovery plan: Ensure laptops are taken home during crisis/BCP for remote work, in case of fail -> IT install application and VPN on free computers or computer from non – critical role./ 6 ноутбуків (4 як мінімум) з усіма встановленими програмами та доступом до VPN

	План відновлення: Забезпечте, щоб працівники забирали ноутбуки додому під час кризи/BCP для віддаленої роботи, в разі несправності -> IT-спеціалісти встановлюють програми та VPN на вільні комп'ютери або комп'ютери працівників
Ukraine/ Україна	Warehouse Facility Before moving to a new facility we need as minimum - Warehouse 250 m². 500 pal.2 cold rooms for 70 and 20 p/m, , loading equipment – 2. Trucks available for transporting with temp monitoring and sanitary control. Office and WH in accordance to the Licenses conditions. <i>Recovery plan:</i> 1) According to GL BCP plans GL provides premises (Attachment 1) 2) Take goods to distributors, to sign contract with new WH Service Provider or Distributor – to work on behalf of Company\with GL Customs Warehouse directly until recovery complete. Distributors have wholesale and import license; they will need to sign contract and to add our products for import. 3) To have tender or benchmarking obtain license and to operate on the new WH./ Складське приміщення До переїзду в нове приміщення нам потрібно як мінімум — Склад 250 м². Місткість: 500 піддонів, 2 холодильні камери на 70 і 20 п/м, , навантажувальна техніка — 2. Вантажівки для перевезення з моніторингом температури та санітарним контролем. Офіс і побутові приміщення відповідно до ліцензійних умов. <i>План відновлення:</i> 1) Відповідно до планів BCP «Глобал Лоджистік», компанія надає приміщення (Додаток 1) 2) Передайте продукцію дистриб'юторам, підпишіть договір з новим постачальником складських послуг або дистриб'ютором — працюйте від імені Компанії/з митним складом «Глобал Лоджистік» безпосередньо до завершення відновлення. Дистриб'ютори мають ліцензію на оптову торгівлю та імпорту; їм необхідно буде підписати договір і додати нашу продукцію для імпорту. 3) Проведіть тендер або аналіз ринку для отримання ліцензії та працюйте на новому складі.
VITAL RECORDS Please list paper documentation that must be recovered./ ВАЖЛИВІ ДОКУМЕНТИ Перелічіть паперову документацію, яку необхідно відновити.	
ПІБ	Describe vital records here or indicate: None required./ Опишіть тут важливі документи або вкажіть: Не застосовується.
Ukraine/ Україна	<i>Recovery plan:</i> Primary docs for sales, discounts, returned and other original documents in the officeto store in safe lock or to send to outsourced archive./ Первинні документи щодо продажів, знижок, повернення продукції та інші оригінальні документи в офісі <i>План відновлення:</i> Зберігайте в сейфі або відправте в архів аутсорсингового постачальника архівних послуг.
Ukraine/ Україна	<i>Recovery plan:</i> Primary docs for sales, returned, state authorities docs, customs docs and other original documents on the WH, stamp to store in safe lock or to send to outsourced archive./ Первинні документи щодо продажів, повернення продукції, документи державних органів, митні документи та інші оригінали документів на складі, печатка <i>План відновлення:</i> Зберігайте в сейфі або відправити в архів аутсорсингового постачальника архівних послуг.
ASSETS Please list items that are difficult to replace and/or purchase, such as research and development samples. Expensive or special order equipment should be listed above in Equipment & Supplies./ АКТИВИ Перелічіть предмети, які важко замінити та/або придбати, наприклад зразки для досліджень і розробок. Дороге або спеціальне обладнання повинно бути перераховане вище в розділі «Обладнання та матеріали».	
ПІБ	Describe assets here or indicate: None required./ Опишіть активи тут або вкажіть: Не застосовується.
Ukraine/ Україна	Letterheads, stamp, office furniture <i>Recovery plan:</i> To reserve all things in a safe place/ Фірмові бланки, печатка, офісні меблі <i>План відновлення:</i> Забезпечте зберігання всіх предметів у безпечному місці

3. TECHNOLOGY IMPACT	3. ВПЛИВ НА ТЕХНОЛОГІЇ
Use the circumstances outlined below when completing this section:	При заповненні цього розділу враховуйте обставини, викладені нижче:
- Technology that is required to support your organization's critical processes has been destroyed. - The technology will be unavailable for at least 30 days (assume no recovery plans exist). - The incident occurred during a peak processing period.	- Технологія, необхідна для підтримки критично важливих процесів вашої організації, була зруйнована. - Технологія буде недоступна щонайменше 30 днів (припустимо, що планів відновлення не існує). - Інцидент стався під час пікового періоду обробки даних.
Equipment /Supply #1 Laptops (applicable only in natural disaster, man-made incident)	Обладнання/Постачання №1 Ноутбуки (застосовується лише у разі стихійного лиха, техногенного інциденту)
Recovery plan:	План відновлення:
1. According to the BCP Strategy laptops that are used by Sales and CTC managers will be transferred to critical roles. Should be approved by National Sales and National CTC managers. Due to the limited amount, it cannot provide with laptops to all people with critical roles. Sales and CTC managers can use iPads for day-to-day work. (Preferred option);	1. Відповідно до Стратегії BCP компанії ноутбуки, які використовуються Менеджерами з продажів та каналів збуту (СТС), будуть передані для виконання критично важливих ролей. Це має бути затверджено Національним менеджером з продажів та Національним менеджером СТС. У зв'язку з обмеженою кількістю, компанія не може забезпечити ноутбуками всіх працівників, які виконують критичні ролі. Менеджери з продажу та СТС можуть використовувати айпад для щоденної роботи. (Бажаний варіант);
List only critical applications that are required to perform your critical business processes	Перелічіть лише критичні програми, які необхідні для виконання критично важливих бізнес-процесів
Standard desktop applications do not need to be included eg. Email, Office products, Intranet, Live Meeting.	Не потрібно включати стандартні програми, наприклад електронну пошту, офісні продукти, інтранет, Live Meeting.

Critical Applications List any critical applications that are required to continue your organization's critical processes./ Критичні програми Перелічіть усі критичні програми, необхідні для продовження критично важливих процесів вашої організації.
Application #1 SAP Recovery plan: Currently application supported centrally and application support team have own DRP. Local support can't impact on the process and we don't have any additional procedures to complete day to day processes without SAP. Out of scope of local BCP. Application is hosted and maintained centrally and has its own BCP. Access to the application is performed remotely. If WMS (WH system) is available – to use the system and after CERPS renewal update accordingly. If no systems are available to use available application, for instance – Excel/Word file for orders and pick up. In case if computer/printer is not available templates are pre-print with empty lines for products. STP to be written and approved for emergency situation with mentioning price-

Critical Application Recovery (IT to provide)/ Відновлення критично важливих програм (здійснює Відділ IT-підтримки)			
Pandora ID/ Chameleon ID/ Ідентифікатор Pandora/ Ідентифікатор Chameleon	Recovery Time Objective (i.e. 1 – 365)/ Цільовий час відновлення (від 1 до 365)	Recovery Point Objective (Mins. Hours, Days)/ Цільовий час відновлення (Хвилини, години, дні)	ITCP Status (Complete, In Progress, No ITCP)/ Статус ІТСП (Завершено, У процесі, Немає ІТСП)
P000257053	24 h/24 год	10 min/10 хв	Completed SOP 00000146784 Global ERP ITCP LSOP/ Завершено SOP 00000146784 Global ERP ITCP LSOP

Critical Applications <i>List any critical applications that are required to continue your organization's critical processes./ Критичні програми</i> <i>Перелічіть усі критичні програми, необхідні для продовження критично важливих процесів вашої організації.</i>
list to be used (last available version or FD advise)./ Програма №1 SAP <i>План відновлення:</i> Зараз програма підтримується централізовано, і команда підтримки програм має власний план відновлення (DRP). Місцевий відділ IT-підтримки не може вплинути на процес, і ми не маємо жодних додаткових процедур для виконання повсякденних процесів без SAP. Поза межами сфери дії місцевого BCP. Програма розміщується та підтримується централізовано та має власний BCP. Доступ до програми здійснюється віддалено. Якщо доступна система WMS (складська система) — використовуйте систему і після оновлення CERPS оновіть її відповідним чином. За відсутності систем — використовуйте наявну програму, наприклад Excel/Word файл для оформлення замовлень і відвантаження продукції. На випадок відсутності комп'ютера.принтера шаблони попередньо роздруковують з порожніми рядками для продукції. Необхідно розробити та затвердити STP на випадок надзвичайних ситуацій із зазначенням прайс-листа, який буде використовуватися (остання доступна версія або рекомендація FD).
The application was down. Not possible to use internet, Wi-Fi, computer systems, mail. <i>Recovery plan:</i> Out of scope as this need to be assessed by IT specialist and is part of BCP Strategy. But first steps for department: 1) To use available application, for instance – Excel/Word file for orders and pick up. 2) To use telephone for orders receiving from distributors and orders sending to the warehouse (check & update client's telephone). 3) To use Excel or Word forms of invoices on the warehouse for dispatch. After systems renewal update the systems. 4) To use mobile internet – all critical roles to be aware on how to connect laptop to mobile internet. In case of specific mobile provider gives internet – to buy sim card of specific workable provider./ Програма не працювала.

Critical Application Recovery (IT to provide)/ Відновлення критично важливих програм (здійснює Відділ IT-підтримки)			
Pandora ID/ Chameleon ID/ Ідентифікатор Pandora/ Ідентифікатор Chameleon	Recovery Time Objective (i.e. 1 – 365)/ Цільовий час відновлення (від 1 до 365)	Recovery Point Objective (Mins, Hours, Days)/ Цільовий час відновлення (Хвилини, години, дні)	ITCP Status (Complete, In Progress, No ITCP)/ Статус ІТСП (Завершено, У процесі, Немає ІТСП)
N/a/ H/3	N/a/ H/3	N/a/ H/3	N/a/ H/3

Critical Applications <i>List any critical applications that are required to continue your organization's critical processes./ Критичні програми</i> <i>Перелічіть усі критичні програми, необхідні для продовження критично важливих процесів вашої організації.</i>	
Неможливо користуватися інтернетом, Wi-Fi, комп'ютерними системами, поштою . План відновлення: Виходить за межі сфери дії цього BCP, оскільки це має бути оцінено IT-спеціалістом і є частиною Стратегії BCP компанії. Але перші кроки для відділу такі: 5) Використовуйте наявні програми, наприклад Excel/Word для оформлення замовлень та відвантаження продукції. 6) Використовуйте телефон для отримання замовлень від дистриб'юторів і відправлення замовлень на склад (перевіряйте та оновлюйте телефон клієнта). 7) Використовуйте Excel або Word форми рахунків-фактур на складі для відправлення продукції. Після відновлення систем оновіть їх. 8) Користуйтеся мобільним інтернетом — необхідно знати, як під'єднати ноутбук до мобільного інтернету. 9) Якщо конкретний мобільний провайдер надає послуги мобільного інтернету — придбайте сім-картку конкретного провайдера.	
WMS If the warehouse system does not work, use the last saved version for work, keep records on paper with subsequent entry into the accounting system. Manual pick-up in emergency. / WMS Якщо складська система не працює, використовуйте для роботи останню збережену версію, ведіть облік на папері з подальшим внесенням в облікову систему. Ручне відвантаження в екстрених випадках.	

Critical Application Recovery (IT to provide)/ Відновлення критично важливих програм (здійснює Відділ IT-підтримки)			
Pandora ID/ Chameleon ID/ Ідентифікатор Pandora/ Ідентифікатор Chameleon	Recovery Time Objective (i.e. 1 – 365)/ Цільовий час відновлення (від 1 до 365)	Recovery Point Objective (Mins, Hours, Days)/ Цільовий час відновлення (Хвилини, години, дні)	ITCP Status (Complete, In Progress, No ITCP)/ Статус ІТСП (Завершено, У процесі, Немає ІТСП)
	48 hours/48 годин		

Impact on Quality related activities

Use BCP to manage Complaint Handling process for product quality complaints in the Company to ensure that all complaints are captured, evaluated, reported and monitored in accordance with regulatory requirements

Recovery plan:

- ☐ To use any of the following contacts for notification:

Вплив на діяльність, пов'язану з якістю

Використовуйте BCP для управління процесом обробки скарг на якість продукції в Компанії для забезпечення реєстрації, оцінки, звітування та моніторингу всіх скарг відповідно до регуляторних вимог

План відновлення:

- ☐ Використовуйте будь-який з вказаних нижче контактів для повідомлення:

ПІБ	Email/ Електронна адреса	Phone number/ Номер телефону
General complaints contact/ Загальна контактна особа щодо скарг	ua.complaints@mmm.com	+38 050 555 55 55

- ☐ To use LOC Product Quality Complaint Form (Form-241-XX) for recording the complaint, in stored in VQD system - VQD-347124.
- ☐ Використовуйте форму скарг на якість продукції місцевої компанії (Form-241-XX) для реєстрації скарги, яка зберігається в системі VQD — VQD-347124.
- ☐ To use mobile internet for sending the complaint records to investigation sites. In case of specific mobile provider gives internet – to buy sim card of specific workable provider.
- ☐ Використовуйте мобільний інтернет для надсилання записів про скарги до місць проведення розслідування. Якщо конкретний мобільний провайдер надає послуги мобільного інтернету — придбайте сім-картку конкретного працездатного провайдера.
- ☐ To use telephone for recording complaints and communication with investigation Sites or complainants (check & update application on the telephone and access to mailbox).
- ☐ Використовуйте телефон для реєстрації скарг і зв'язку з місцями проведення розслідувань або заявниками (перевіряйте та оновлюйте програму по телефону та отримуйте доступ до поштової скриньки)

Other Business Applications	
List other business applications that are needed to support your organization's critical processes. <i>These applications are not required to have an ITCP in place/ Інші бізнес-програми</i> Перелічіть інші бізнес-програми, необхідні для підтримки критично важливих процесів вашої організації. <i>Для цих програм не обов'язкова наявність ІТСП</i>	
Ukraine	Telephone <i>Recovery plan:</i> Use mobile phones until phone network is back up and running Use Viber/WhatsApp Teams until phone network is back up and running/ Телефон <i>План відновлення:</i> Використовуйте мобільні телефони, доки телефонна мережа не буде відновлена та запущена Використовуйте Viber/WhatsApp Teams, доки телефонна мережа не відновить роботу

Critical Data
List any critical shared areas (i.e. Team/Department File Directory)/ Критичні дані Перелічіть усі критичні спільні ресурси (наприклад, каталог файлів команди/відділу)
Department file Directory on folder need to be available / Каталог файлів відділу в папці повинен бути доступним за посиланням
Outsourced archive for primary documentation/ Архів первинної документації в аутсорсингового постачальника архівних послуг
CERPS SAP (MODCF, GSNPF modules): посилання/ CERPS SAP (модулі MODCF, GSNPF): посилання

Steps to reduce the risk and impact of an application or data loss:

4. BUSINESS PARTNER IMPACT

Use the circumstances outlined below when completing this section:

Кроки зменшення ризику та наслідків збою програми або втрати даних:

4. ВПЛИВ НА БІЗНЕС-ПАРТНЕРА

При заповненні цього розділу враховуйте обставини, викладені нижче:

- External Business Partners that enable your critical processes are not available to provide services (E.g. contingent worker agencies, off/on-site vendors, suppliers, outsourced functions).
- Зовнішні бізнес-партнери, які забезпечують ваші критично важливі процеси, не доступні для надання послуг (наприклад, агентства з найму тимчасових працівників, зовнішні/внутрішні вендори, постачальники, аутсорсингові функції).
- The impact to your business partner(s) is immediate and will continue for at least 30 days.
- Вплив на ваших бізнес-партнерів є невідкладним і триватиме щонайменше 30 днів.
- The business partner loss occurs during peak processing period.
- Втрата бізнес-партнера відбувається під час пікового періоду обробки.

Document only the external business partners that are absolutely required to achieve your Recovery Time Objective for your critical business processes with a Criticality rating 1 or 2.

Зазначте лише тих зовнішніх бізнес-партнерів, які є абсолютно необхідними для досягнення Цільового часу відновлення (RTO) для ваших критично важливих бізнес-процесів з рейтингом критичності 1 або 2.

- 1 - Single source supplier
- 1 — Єдиний постачальник
- 2 - Alternative supplier or source could be engaged without impacting RT
- 2 — Альтернативний постачальник або джерело може бути залучений без впливу на RTO

Describe business partners here or indicate: None required./ Опишіть бізнес-партнерів тут або вкажіть: Не застосовується.			
ПІБ	Critical Service Provided/ Критично важлива послуга, що надається	Criticality Rating/ Критичність Рейтинг	Vendor Status Unknown, BCP in place, No BCP/ Вендор Статус Невідомий, є BCP, немає BCP
Distributor (contacts below)/ Дистриб'ютор (контактні дані вказано нижче)	Sales of goods <i>Recovery plan:</i> To use other distributors for sale, to organize negotiations for turnover increase ./ Продаж продукції <i>План відновлення:</i> Залучити інших дистриб'юторів для продажів, організуйте переговори для збільшення товарообігу	2	Na/ H/3

Distributors contacts:/ Контактні дані дистриб'юторів:

Steps to reduce the risk and impact of a business partner loss:

- ☐ Review the Business Partner Recovery Rating and take action to reduce the continuity risk where possible

Кроки зменшення ризиків та наслідків втрати бізнес-партнера:

- ☐ Перегляньте Рейтинг відновлення бізнес-партнерів і вживайте заходів, щоб зменшити ризик для безперервності бізнесу, де це можливо

Distribution Business Continuity Plan

План безперервності бізнесу для діяльності з дистрибуції

Emergency contact Name/Surname - M +380505555555 +4855555555

Team Teleconference:
+38 (050) 333 33 33 Recovery Team Lead
Back – up telephone – +38 (050) 444 44 44 Deputy Head

Wh back-up telephone - +38 044 444 44 44 (44/55)

Office - +38044 555-55-55
Teams  Click here to join the meeting
call in (audio only)
 +380 89 324 0100, Ukraine, All locations
Phone  Conference ID: 111 111 111#

 pin in case you are the 1st (organizer) 000000
In case of connection lost – every day at 12:00

Additional telephone line. Detail for call:
Dial the number: +38044 555 55 55
Room number: 7777 #
PIN: 2222 #
For iPhone: +380 (44) 555 55 55,,7777#2222#
Appendix 2

Recovery Team Details

ПІБ М +380505555555 +4855555555

Телеконференція Команди:
+38 (050) 333 33 33 Керівник Команди відновлення
Резервний номер телефону: +38 (050) 444 44 44
заступник керівника команди
Резервний номер телефон складу: +38 044 444 44 44 (44/55)
Офіс: +38044 555-55-55
Teams  Натисніть тут, щоб приєднатися до зустрічі
зателефонуйте (тільки голосовий дзвінок)
 +380 89 324 0100, Україна, Всі регіони
Номер телефону  Конференц-ідентифікатор: 111 111 111#

 пін-код на випадок, якщо ви 1-й (організатор) 000000
У разі втрати зв'язку — 12:00 щодня

Додаткова телефонна лінія. Інформація для дзвінка:
Зателефонуйте за номером: +38044 555 55 55
Номер кімнати: 7777 #
PIN-КОД: 2222 #
Для айфонів: +380 (44) 555 55 55,,7777#2222#
Додаток 2

Інформація про Команду відновлення

	ПІБ	Position/ Посада	Mobile Phone No./ Номер мобільного телефону	Work Email/ Робоча електронна адреса
Recovery Team Lead/ Керівник Команди відновлення		Head of Logistics and Distribution Department/ Начальник відділу логістики та дистрибуції		
Back-up/ Заступник Керівника		Warehouse Manager/ Завідуючий		

Команди відновлення Recovery Team / Команда відновлення		аптечним складом		
		Ethics and Compliance Manager / Начальник відділу корпоративної етики та відповідності		
		Customer Service Specialist/ Фахівець по роботі з клієнтами		
		Customer Service Specialist/ Фахівець по роботі з клієнтами		
		Logistics Planner/ Фахівець з питань логістики та планування поставок		
		Quality Manager/ Начальник відділу із якості		
		Quality complaint handler/ Спеціаліст з розгляду скарг на якість		
		EHS&S National Specialist/ Інженер з охорони праці		
		Finance Director/ Фінансовий		

		директор		
		Security Champion Rx/ Чемпіон з безпеки Rx		

Appendix 3/ Додаток 3

Crisis Team/ Кризовий штаб

ROLE/ РОЛЬ	NAME/ ПОВНЕ ІМ'Я	MOBILE NUMBER/ НОМЕР МОБІЛЬНОГО ТЕЛЕФОНУ
Rx Office/ Офіс рецептурних препаратів		
Crisis Team Lead/ Керівник Кризового штабу		
Compliance Lead/ Начальник відділу корпоративної етики та відповідності		
Human Resources/ Відділ управління персоналом		
Log Keeper/ Реєстратор		
Legal/ Юридичний відділ		
Finance/ Фінансовий відділ		
Administrative/ Адміністративний відділ		

Tech Manager/ Технічний менеджер		
Regulatory/ Регуляторний відділ		
Procurement / Відділ закупівель		
Quality/ Відділ із якості		
CTC & Distribution/ Департамент по роботі з каналами збуту та дистрибуції		
Logistic & Distribution/ Відділ логістики та дистрибуції		
Marketing / Відділ маркетингу		
EHS/ Охорона праці		
Head of Commercial Operations and Omnichannel / Відділ комерційної ефективності		
Country Medical Manager / Національний медичний менеджер		
Plan Sponsor/ Спонсор плану		
Plan Sponsor/ Спонсор плану		
Plan Owner/ Власник плану		
Corporate-Security / Корпоративна безпека		
Cyberattack/ Кібератаки		

Appendix 4

LSP GL BCP

План заходів при загрозі ведення військових дій:

1. **План заходів при загрозі ведення військових дій** описує дії керівництва і співробітників ТОВ «Глобал Лоджистік», а також компаній-орендарів в частині, що їх стосується.

2. При виникненні **загрози ведення військових дій** відповідальність за оперативне реагування, надійне управління (створення оперативного штабу) для забезпечення діяльності та охорони логістичного комплексу, повідомлення компаній-орендарів та організацію взаємодії, покладається на керівництво ТОВ «Глобал Лоджистік».

3. План заходів при загрозі ведення військових дій призначений для організації і здійснення організаційно-технічних, соціально-економічних та інших практичних заходів, спрямованих на проведення робіт із забезпечення оперативного реагування, уточнення режиму роботи, збереження здоров'я та життя людей, зниження розмірів збитків і ін.

4. У разі виникнення надзвичайної (екстремальної) ситуації в громадському житті (**загроза війни, збройний конфлікт або серйозна погроза такого конфлікту, включаючи але не обмежуючись ворожими атаками, блокадами, військовим ембарго, дії іноземного ворога, загальна військова мобілізація та т.і.**), що унеможлиблює виконання договірних зобов'язань ТОВ «Глобал Лоджистік», здійснюється оповіщення партнерів про настання форс-мажорних обставин.

Поняття:

Вторгнення – будь які дії, в тому числі, збройний конфлікт, в результаті якого є загроза територіальній цілісності, незалежності на суверенітету України

Оперативний штаб - сформований зі складу співробітників орган оперативного реагування на загрози вторгнення/вторгненню на територію України ворожих сил, основним функціональним обов'язком якого є забезпечення збереження матеріальних цінностей Товариства, а також забезпечення ведення сталого бізнесу в умовах надзвичайної ситуації

Комплекс – адміністративно-складський комплекс ТОВ «Глобал Лоджистік», що знаходиться за адресою: 08320, Україна, Київська область, Бориспільський р-н, с. В. Олександрівка, вул. Київський шлях, 121-А

План дій:**А) при загрозі вторгнення:**

1. Створення оперативного штабу
2. Інформування персоналу комплексу щодо дій в разі загрози ведення військових дій, ознайомлення з планом евакуації та схемою найближчих бомбосховищ:
 - м. Київ: https://kyivcity.gov.ua/bezpeka_ta_pravoporiodok/bomboskhovishcha_ta_ukryttia/
 - околиці Комплексу: <https://www.google.com/maps/d/viewer?mid=1pjF8h5LffVYAJhPcPY3HOZY9ffRHusDz&ll=50.399990240314914%2C30.836077135192888&z=13>
3. **Актуалізація списку контактів орендарів** – Отримання інформації щодо представника оперативного штабу орендаря – особи, яка приймає рішення, має право підпису, печатку та можливість відпуску автомобіля при відвантаженні товару).
4. Забезпечення першочергових потреб Комплексу:
 - збереження Комплексу – воєнізована охорона
 - збереження матеріальних цінностей – *відповідальні: оперативний штаб;*
 - справність службових автомобілів - *відповідальні: механік ЮЛ;*
 - щоденне забезпечення повного паливного баку в службових авто - *відповідальні: водії закріплені за службовими автомобілями;*
 - аптечка першої допомоги (КПП, офіс) - *відповідальні: інженер з охорони праці*
 - забезпечення життєдіяльності Комплексу, а саме забезпечення альтернативною електроенергією: перевірка справності дизель генераторів та підтримка їх паливних баків в заповненому стані: керівник ТД.
 - У разі загрози отримання сторонніми особами фізичного доступу до робочих станцій (далі – РС), конфіденційної інформації або комерційної таємниці здійснити видалення критичної інформації, винесення РС та носіїв інформації за межі службових приміщень.

Б) При активному вторгненні здійснюються наступні дії:

1. **ОПОВІЩЕННЯ** (30хв – роб. час, 2 год – нероб. час) у разі отримання інформації з офіційних джерел про виникнення загрози ведення військових дій - *відповідальні: оперативний штаб.*
 - 1.1. **Оповіщення персоналу та орендарів в роб. час** шляхом подання відповідного сигналу - пожежна сирена, що повторюється тричі з інтервалом не більше 30с.
 - 1.2. **Оповіщення орендарів в нероб. час** – за умови роботи мобільного зв'язку для координації дій щодо збереження товарних запасів.
2. **Евакуація персоналу Комплексу** до укриття (бомбосховища) у разі прямої загрози життю та здоров'ю працівників в умовах відкритої військової агресії (у робочий час).

- 2.1. Після того, як пролунав сигнал евакуації, персоналу взяти особисті речі та прослідувати в місце збору. Місце збору – за межами комплексу біля автобусу, через 20хв після сигналу евакуації.
- 2.2. Відповідальні особи з кожної секції ставлять приміщення під охоронну сигналізацію, перед цим переконавшись у виході всіх працівників із секції.
- 2.3. Для евакуації використовується автобус (розвозка) та службові автомобілі.
- 2.4. Місце евакуації – м. Київ, м. Бориспільська

3. Прийняття рішення щодо подальшого режиму роботи Комплексу. Оцінка обстановки, визначення режиму діяльності оперативного штабу та ін.:

- взаємодія з компаніями-партнерами (орендарями), підрядними організаціями, поліцією охорони, аварійними та рятувальними службами, органами місцевої влади та ін.,
 - узагальнення інформації щодо функціонування систем життєзабезпечення комплексу;
- 3.1.1. За необхідності призупиняється діяльність логістичного комплексу на певний час, видається наказ щодо тимчасового призупинення роботи працівників (із збереженням заробітної плати відповідно до ст. 113 КЗпП України), обов'язки яких не пов'язані із функціонуванням систем життєзабезпечення.
 - 3.1.2. Працівники, що контролюють роботу систем життєзабезпечення, відповідають за пожежну безпеку, забезпечення збереженості ЛЗ, виконують свої обов'язки відповідно до встановленого режиму роботи та завдань.
 - 3.2. За можливості, здійснюється оповіщення керівництва компаній-партнерів (орендарів) про подальший режим роботи. Узгодження питань щодо діяльності аптечних складів, фінансового забезпечення, сервісного обслуговування, охорони та ін. (01.30 год. в робочий час., 03.30 год. в неробочий час.).

Рішення про подальші дії приймається оперативним складом разом з керівництвом компаній-партнерів (орендарів) в залежності від ситуації та наявних можливостей.