УДК 336.71+004.78+65.001.3

# КОНЦЕПЦІЯ БЕЗПЕРЕРВНОСТІ ВЕДЕННЯ БІЗНЕСУ: ТЕОРЕТИЧНІ ТА ПРИКЛАДНІ АСПЕКТИ

© 2018 **МУШИНСЬКИЙ Б. М.**

*УДК 336.71+004.78+65.001.3*

**Мушинський Б. М. Концепція безперервності ведення бізнесу: теоретичні та прикладні аспекти**

*Метою цієї статті є аналіз усіх складових елементів процесу безперервності ведення бізнесу (BCM – Business continuity management) та кризового управління та виявлення шляхів його практичного впровадження. Визначено головні елементи роботи із Планами безперервності та виділено основні помилки, на які варто звернути увагу фахівцям, при запуску BCM. Дослідження показало, що управління безперервністю бізнесу забезпечує об'єднання всіх застосовуваних на підприємстві заходів у цілісний, адекватний реальним загрозам і керований комплекс, що дозволяє компанії безперервно надавати послуги, уникнути впливу надзвичайних ситуацій на діяльність і мінімізувати можливий збиток. Показано важливість диференціювання Кризового менеджменту в окремий інтегрований напрямок зі своїми стандартами та Планами. Цей комплекс складається з багатьох складових, які повинні бути реалізовані в компанії для забезпечення безперервності надання послуг і виробництва продуктів. Описано кожен етап з прив'язкою до реальних проблем застосування та найкращих світових практик, а також вказано моменти, на які варто звернути увагу під час реалізації програми впровадження BCM.*

***Ключові слова:*** *ризик-менеджмент, кібербезпека, інформаційні системи, безперервність, відновлення, порушення, криза.*

***Рис.:*** *3.* ***Табл.:*** *1.* ***Бібл.:*** *8.*

***Мушинський Богдан Михайлович*** *– аспірант, Львівський торговельно-економічний університет (вул. Туган-Барановського, 10, Львів, 79005, Україна)*

***E-mail:*** *bohdan.mushynskyi@gmail.com*

*УДК 336.71+004.78+65.001.3*

***Мушинский Б. М. Концепция непрерывности ведения бизнеса: теоретические и прикладные аспекты***

*Целью статьи является анализ всех составляющих элементов процесса непрерывности ведения бизнеса (BCM – Business continuity management) и кризисного управления и выявление путей его практического внедрения. В данной статье определены основные элементы работы с Планами непрерывности, и выделены основные ошибки, на которые следует обратить внимание специалистам, при запуске BCM. Исследование показало, что управление непрерывностью бизнеса обеспечивает объединение всех применяемых на предприятии мер в целостный, адекватный реальным угрозам и управляемый комплекс, позволяющий компании непрерывно предоставлять услуги, избежать влияния чрезвычайных ситуаций на деятельность и минимизировать возможный ущерб. Показана важность дифференциации Кризисного менеджмента в отдельное интегрированное направление со своими стандартами и Планами. Этот комплекс состоит из многих составляющих, которые должны быть реализованы в компании для обеспечения непрерывности предоставления сервисов и производства продуктов. Описан каждый этап с привязкой к реальным проблемам применения и лучшим мировым практикам, а также указаны моменты, на которые стоит обратить внимание при реализации программы внедрения BCM.*

***Ключевые слова:*** *риск-менеджмент, кибербезопасность, информационные системы, непрерывность, восстановление, нарушение, кризис.*

***Рис.:*** *3.* ***Табл.:*** *1.* ***Библ.:*** *8.*

***Мушинский Богдан Михайлович*** *– аспирант, Львовский торгово-экономический университет (ул. Туган-Барановского, 10, Львов, 79005, Украина)*

***E-mail:*** *bohdan.mushynskyi@gmail.com*

*UDC 336.71+004.78+65.001.3*

***Mushynskyi B. M. The Conception of Business Continuity Management: Theoretical and Applied Aspects***

*The article is aimed at analyzing all components of the process of business continuity management (BCM) and crisis management, and identifying ways of its practical implementation. This article defines the basic elements of working with Continuity Plans, and allocates the main errors that should be addressed to specialists when introducing the BCM. The research showed that business continuity management ensures the consolidation of all the measures applied at the enterprise in a holistic, adequate towards real threats as well as managed complex, allowing the company to continuously provide services, to avoid impact of emergency situations on the activity and minimize possible damage. The importance of differentiation of Crisis management in a separate integrated direction with its standards and Plans is displayed. This complex consists of many components that must be implemented in the company to ensure the continuity of service delivery and production of products. The author describes each stage with reference to real problems of application and to the best world practices, also mentioning the points, on which it is necessary to pay attention at realization of program of introduction of the BCM.*

***Keywords:*** *risk management, cybersecurity, Information systems, continuity, recovery, disruption, crisis.*

***Fig.:*** *3.* ***Tbl.:*** *1.* ***Bibl.:*** *8.*

***Mushynskyi Bohdan M.*** *– Postgraduate Student, Lviv University of Trade and Economics (10 Tuhan-Baranovskoho Str., Lviv, 79005, Ukraine)*

***E-mail:*** *bohdan.mushynskyi@gmail.com*

Для кожної комерційної організації основним завданням має бути задоволення потреб свого клієнта, незалежно від профілю роботи такої компанії (сервіс-орієнтована компанія чи виробник товарів, або можливо ритейлер). Об'єднуючим фактором завжди повинен бути користувач / клієнт, і цей підхід є визначним у побудові сучасної бізнес-моделі організації.

Проте бізнес щодня піддається незліченному впливу різних внутрішніх і зовнішніх факторів, в тому числі несприятливих. Якщо такий вплив несе незначний характер або, інакше кажучи – відповідає очікуванням, то ми можемо назвати цей період життя компанії як «звичайний бізнес» («business as usual»). Прикладом впливу зовнішніх факторів при «звичайному бізнесі»

може бути скарга клієнта, запізнення поставки товару, поломка автомобіля та ін. Проте, коли такі фактори впливу мають непередбачуваний характер та наносять вагомої шкоди, організація повинна перейти на кризове управління («crisis management»).

Тому для збереження бізнесу в умовах кризових ситуацій було розроблено певний підхід до управління організації, який дістав назву Business continuity management (BCM) або Безперервність ведення бізнесу, що сформував міжнародні стандарти ISO 22301, ISO 22313, ISO/IEC 27031.

Питанням безперервності ведення бізнесу займаються провідні фахівці до сьогодні та постійно вдосконалюють найкращі практики. Основними фахівцями, які внесли свій вагомий вклад на цю тему, можна вважати: Oliver Pettit (AGL, Australia), Stacy Summers (Aon, US), Åsa Kyrk Gere (Chair of ISO/TC 292 for Security and Resilience), Chloe Demrovsky (President DRI International), Marianne Swanson (NIST), Pauline Bowen (NIST), Amy Wohl Phillips (NIST), Dean Gallup (NIST), Saul Midler (ISO/TC 292 for Security and Resilience), Gary Locke (U.S. Department of Commerce). Варто зауважити, що сам стандарт ISO 22301 знаходиться на перегляді робочої групи Міжнародної організації зі стандартизації та невдовзі може бути оновлений до стандарту ISO/CD 22301 [1].

**Метою** цієї статті є аналіз усіх складових елементів процесу безперервності ведення бізнесу та кризового управління, виявлення шляхів його практичного впровадження. У статті визначено головні елементи роботи із Планами безперервності та виділено основні помилки, на які варто звернути увагу фахівцям, при запуску BCM.

У сучасному світі спостерігається зростання загроз, що стоять перед компаніями. Деякі з цих загроз (природні або антропогенні) можуть мати настільки нищівний вплив на компанію, що це може привести до припинення нею діяльності. Тому сучасним компаніям необхідно прийняти політику неперервності бізнесу, щоб визначити критичні процеси та ресурси, а також вжити необхідних заходів з їх захисту в разі серйозних загроз.

Загалом існує декілька варіантів ведення бізнесу організацією залежно від того, яку модель вибере менеджмент. Це може бути:

Переривання бізнесу – коли під час впливу кризових ситуацій чи катастроф організація припиняє свою нормальну діяльність, допоки вплив таких чинників не завершиться або послабиться (інколи навіть повне припинення бізнесу та ліквідація).

Передача ризику – коли організація передає ризик впливу кризових ситуацій на іншу компанію, наприклад страхову компанію, або перенесення IT інфраструктури у хмарні сервіси.

Підхід толерантності до ризику – коли компанія не вживає спеціальних заходів для подолання негативного впливу, а чекає до завершення кризи. При цьому компанія має заздалегідь визначений рівень толерантності до ризику (зазвичай у грошовому еквіваленті), який вона може прийняти, але не більше цієї межі.

Підхід безперервності ведення бізнесу (BCM) – відповідно до цієї стратегії організація приймає контрзаходи, щоб прямо протистояти ризикам, які можуть спричинити значні збої критичних бізнес-процесів. Організація заздалегідь планує, як реагувати на ті чи інші несприятливі кризові явища, та впроваджує відповідну систему у свої щоденні операції задля швидкого реагування на кризу. Таким чином, організація може продовжувати свою бізнес-діяльність, не завдаючи незручностей клієнтам, партнерам і втрачаючи мінімум доходу та ресурсів.

Безперервність бізнесу (BCM) містить у собі планування та підготовку, для забезпечення можливості організації продовжувати працювати, у випадку серйозних інцидентів або катастроф та здатності відновитись до нормального стану протягом досить короткого періоду [7].

Метою BCM є продовження критичної бізнес-діяльності під впливом несприятливих чинників (таких як кризові ситуації, катастрофи). BCM складається з аварійного відновлення (disaster recovery), відновлення бізнесу (business recovery), управління кризовими ситуаціями (crisis management), управління інцидентами (incident management), управління надзвичайними ситуаціями та планування на випадок надзвичайних ситуацій (emergency management and contingency planning).

Управління неперервністю бізнесу визначене в Стандарті ISO 22301:2012 як «процес виявлення потенційних загроз бізнес діяльності організації» та як процес, «який забезпечує структуру для побудови стійкості організації зі спроможністю ефективного реагування, яке захищає інтереси ключових акціонерів, репутацію, торгову марку та діяльність зі створення цінностей» [2]. Неперервність бізнесу часто описують як «просто здоровий глузд».

За своєю суттю BCM повинен мати всеохоплюючий підхід в управлінні компанією, це не повинен бути один із напрямків, це повинен бути підхід до мислення при побудові усіх напрямків роботи компанії. Потрібно мислити, передбачаючи негативний вплив на бізнес при розробці самого процесу та закладати таку можливість задля адекватного розуміння своїх можливостей та прихованих резервів.

Особливу увагу до BCM на практиці приділяють IT-компанії та великі корпорації, а також усі фінансові установи. Для гравців у таких серйозних сферах, як фінанси, – це просто невід'ємна частина управління, позаяк контролюється національними та міжнародними регуляторами.

Управління безперервністю бізнесу значною мірою перебуває у сфері управління якістю та управління ризиками (quality and risk management), з деякими перехрестями у відповідні сфери, такі як керівництво, інформаційна безпека та комплаєнс. Управління ризиками є важливим інструментом для безперервності бізнесу, оскільки забезпечує структурований

спосіб визначення джерел переривань бізнесу й оцінку їх ймовірності та шкоди. Очікується, що всі бізнес-функції, операції, запаси, системи, відносини тощо, які є надзвичайно важливими для досягнення оперативних цілей організації, аналізуються та включаються до плану безперервності бізнесу (BCP). Важливо розуміти, що не всі процеси у діяльності вашої організації потребують безперервної роботи, тому не потрібно до усіх них застосовувати однаковий підхід – це як мінімум витратно, а як максимум – безглуздо. Додаткового захисту потребують лише критичні процеси та ресурси, які їх забезпечують.

Якщо не існує плану безперервності бізнесу, а організація, про яку йдеться, стикається з досить серйозною загрозою або катастрофою, яка може призвести до банкрутства, реалізація BCP та результати, якщо не занадто пізно, можуть значно зміцнити шанси на «виживання» організації та її безперервність діяльності.

У процесі BCM є важливі поняття, які варто розуміти однозначно:

Криза (Crisis) – це ситуація з високим рівнем непевності, яка порушує ключову діяльність та/або надійність організації та вимагає негайних дій;

Інцидент (Incident) – подія, здатна привести до втрати або порушення операцій, сервісів або функцій організації, який, якщо ним не управляти, може перерости у надзвичайну подію, кризу або катаклізм. Інцидент – це настання загрози.

Катаклізм (Disaster) – фізична подія, яка має потенціал достатньо перервати бізнес-процес, щоб загрожувати життєдайності організації.

Відповідно, залежно від характеру впливу на організацію існують і різні елементи BCM, за допомогою яких організація може відповідати на них. Загалом набір таких елементів, політики та планів складає собою Систему управління безперервністю ведення бізнесу (BCM Framework).

У Системі управління безперервністю ведення бізнесу повинні бути як мінімум Стратегія безперервності ведення бізнесу, Політика безперервності ведення бізнесу, Політика кризового управління, Плани безперервності ведення бізнесу (BCP), План відновлення після катаклізму (DRP). Видів, назвемо їх «планами дій», у цьому напрямку є досить багато. Проте організація не повинна мати їх усі, потрібно з розумом підходити до цього питання та спочатку оцінити ризики від відсутності певного типу плану та можливі наслідки, а потім порівняти ці наслідки з витратами на створення такого плану, реагування та його впровадження, тестування, перегляд. Візуально це можна зобразити за допомогою визначення точки Балансу витрат:

У табл. 1 описано найпоширеніші типи планів та дано їх коротку характеристику.

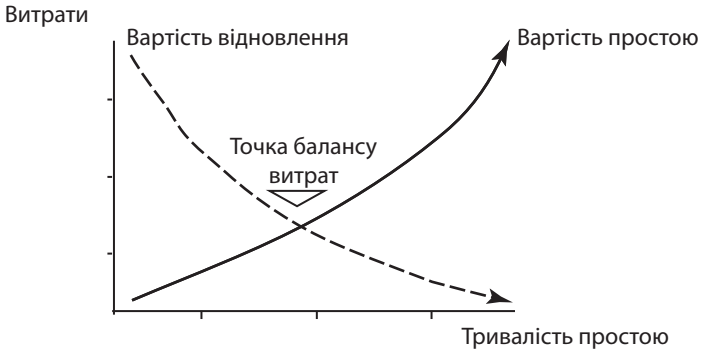


**Рис. 1. Визначення точки Балансу витрат**

**Джерело:** складено автором на основі [3].

Після створення Стратегії організації щодо безперервності ведення бізнесу у своїй Політиці або в окремому документі потрібно визначити методи аналізу бізнес-процесів, оцінки активів компанії та ресурсів. Такий процес також має уже визначену форму та складові і носить назву «Аналіз впливу на бізнес» (Business Impact Analysis – BIA). Метод аналізу впливу на бізнес дозволяє досліджувати вплив інцидентів на ключові види діяльності і процеси компанії. Ґрунтуючись на проведеному BIA, можна чітко зрозуміти сферу застосування BCM та критичні ділянки, на які слід звертати увагу під час планування.

На етапі BIA передбачається детальне вивчення процесів компанії. Для цього проводиться інтерв'ю з керівництвом відділів, що входять у галузь проекту. Під час бесіди запитується інформація про діяльність відділу, і складається перелік процесів / функцій, які він здійснює. Далі для детального вивчення процесів / функцій беруть інтерв'ю у власників процесів, і визначається тип впливу на бізнес (матеріальний, репутаційний) і ступінь залежності процесу від IT і зовнішніх сервісів. На основі проведених опитувань (BIA) та консолідації усіх отриманих даних необхідно визначити такі критичні для подальшого планування показники, як RPO, RTO,WRT [4]:

**RPO** – Recovery Point Objective – точка часу в минулому, після якої дані будуть відновлені. Якщо ми кажемо, що RPO 15 хв – це означає, що кожні 15хв. роботи сервісу дані копіюються, і у разі виходу з ладу дані можна відновити з втратою останніх 15 хв роботи.

**RTO** – Recovery Time Objective – проміжок часу, протягом якого відбудеться відновлення ураженого ресурсу (відлік починається після підтвердження кризи та

**Таблиця 1**

**Типи планів**

| Назва | Мета | Сфера застосування |
|---|---|---|
| План Безперервності ведення бізнесу (BCP) | Забезпечує процедури для підтримки критичного бізнес-процесу під час відновлення від значного порушення | Може створюватися для конкретної критичної функції або для операцій загалом (тоді носить назву Continuity of Operations (COOP) Plan), на період до 1 місяця |
| План комунікації під час кризи (Crisis communication plan – CCP) | Забезпечує процедури для внутрішніх і зовнішніх комунікацій під час кризи; повинен забезпечити надання інформації про статус кризи, контролюючи чутки | Комунікація з персоналом та громадськістю; не зосереджений на інформаційних ресурсах |
| План реагування на IT-інциденти (Cyber Incident Response Plan – CIRP) | Забезпечує процедури для пом'якшення негативного впливу та реагування на кібератаку, таку як вірус, хробак або троян, вірус-вимагач, DDoS та ін. | Спрямований на мінімізацію негативного впливу та ізоляцію уражених систем, очищення, зниження ймовірності втрати інформації |
| План відновлення після катаклізму (Disaster Recovery Plan – DRP) | Забезпечує процедури переміщення роботи інформаційних систем до альтернативної локації | Активується після значних системних порушень із довгостроковими ефектами |
| План неперервності інформаційних систем (Information System Contingency Plan – ISCP) | План відновлення системи, мереж і основних додатків після аварії | Цей план необхідно розробити для кожної критичної системи і / або додатки |
| План дій персоналу під час надзвичайних ситуацій (Occupant Emergency Plan – OEP) | В цьому плані визначається порядок забезпечення безпеки життя та здоров'я персоналу та процедури евакуації в разі надзвичайних ситуацій (наприклад пожежа, замінування, мітинг тощо) | Фокусується на персоналі та активах конкретного об'єкта. Не відноситься до процесів чи інформаційних систем |
| План кризового управління (Crisis management action plan – CMAP) | Запровадження основних принципів управління в кризовій ситуації, які компанія вирішила прийняти з метою встановлення належної системи управління в кризовій ситуації для управління будь-якими негативними обставинами, які можуть перерости у кризу | Застосовується при настанні кризи та фокусується на роботі організації загалом; збереження її як функціональної бізнес-одиниці |

**Джерело:** складено автором на основі [5].

активації BC або DR плану). Якщо ми кажемо, що RTO 15 хв – це означає, що протягом 15 хв є змога відновити працездатність сервісу практично з нуля.

**WRT** – Work Recovery Time – час, протягом якого відбувається перевірка коректності відновлення, консистентності даних та підтверджується повне відновлення.

**MTD** – Maximum Tolerable Downtime – (RTO+WRT) загальний період часу, протягом якого порушення роботи бізнес-процесу не призведуть до критичних для компанії наслідків.

Багато хто зупиняється на показнику RTO та будує BCP, відштовхуючись від нього, проте в результаті на практиці отримаємо неможливість виконання такого плану, тому важливо включити в планування WRT та, як результат, відштовхуватись від MTD.

Активацію планів безперервності ведення бізнесу повинна виконувати кризова команда, у склад якої мають входити представники основних напрямків компанії (HR, COO, CEO, IT, безпека). Склад такої команди повинен визначатися керівництвом самостійно, виходячи зі специфіки внутрішньої структури та мандату керівників окремих напрямків. Також потрібно визначити кворум команди, щоб не очікувати на збори усіх учасників для прийняття рішення про активацію плану, що є дуже сенситивним до витраченого на це часу. Якомога швидше повинні прийматися рішення та використовуватися усі наявні канали комунікації (найшвидше за допомогою мобільного зв'язку).

Окремим напрямком слід зазначити Кризове управління (Crisis management – CM). Не слід об'єднувати BCM та CM в один процес, хоча й чіткої межі також проводити не слід. Кризове управління базується на Плані кризового управління (Crisis management action plan – CMAP) та має на меті забезпечити стабільну діяльність усіх критичних процесів і роботу банку загалом. План кризового управління є універсальним та не несе в собі конкретних покрокових дій при настанні кризи, а лише описує загальну схему реагування та ескалації проблеми. Кризове управління не фокусується на критичних бізнес процесах, а на контрзаходах щодо кризових явищ, які загрожують організації загалом (наприклад, природні катастрофи, тех-

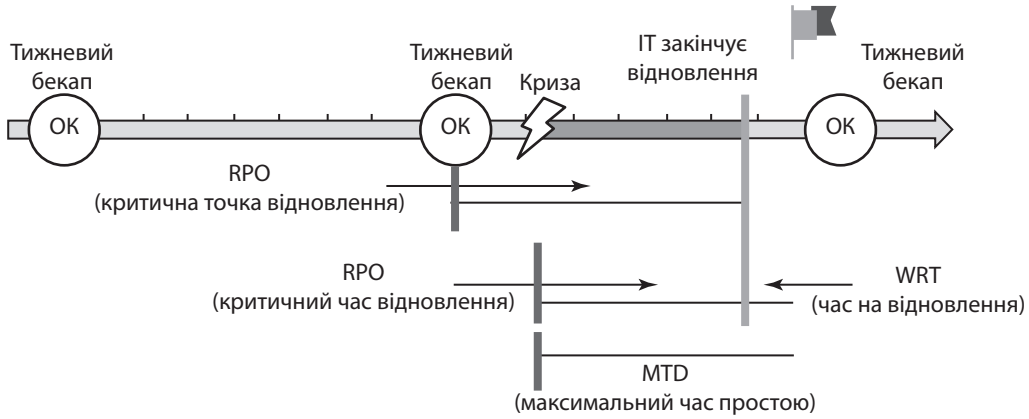


**Рис. 2. Максимальний час простою**

**Джерело:** авторська розробка.

нологічні кризи, конфронтація, організаційні помилки, насильство на робочому місці, чутки, терористичні напади / техногенні катастрофи, кіднепінґ тощо) [8].

Неперервність бізнесу та управління в кризовій ситуації – це два взаємопов'язаних процеси, які мають на меті захист компаній від загроз, як природних, так і антропогенних. CMAP є першою реакцією на кризу, яку має застосувати організація, тому він повинен містити відповідну інформацію, щоб чітко визначити виконавців, котрі повинні владнати інцидент.

Не всі інциденти переростають у кризові ситуації та не всі кризові ситуації вимагають активізації стратегій неперервності бізнесу, але обидва процеси є частинами тієї ж самої стратегії, якої необхідно належним чином дотримуватися. Тому BCM середовище повинне мати приблизно таку взаємозалежність:


**Рис. 3. Система управління безперервністю ведення бізнесу**

**Джерело:** авторська розробка.

Для застосування усіх технік, які передбачає BCM, також необхідно розуміти так званий гранулярний рівень проблеми – життєвий цикл самої кризової ситуації. Він складається з 4 етапів:

1. **Етап оцінки** (evaluation) – Аналіз інформації про подію та оцінка її наслідків.

2. **Етап реагування на кризу** (crisis response) – Виявлення відповідного рішення безперервності для кризового сценарію. Активація плану.

3. **Етап відновлювальних робіт** (recovery) – Проведення всіх необхідних заходів у зв'язку з кризою для перезапуску критичних процесів і відновлення стандартних операційних процесів.

4. **Етап повернення до нормальної діяльності** (back to business) – Здійснення цих заходів необхідно для того, щоб повернутися до нормальної діяльності. Перегляд виконаних дій та робота над помилками [5].

Таким чином, з точки зору функціонування BCM в організації, можна виділити певний постійний цикл, який поділяється на планування та підготовку, реакцію на кризу та відновлення [6].

Останнім, однак, не за важливістю, елементом має бути постійне тестування та перегляд наявних планів та політики BCM. Тестування здійснюється для перевірки працездатності планів при виникненні певного набору обставин, що впливають на діяльність компанії. План тестування вибирається з урахуванням типу компанії і її цілей. Для напрямку BCM дуже критично мати актуальні документи, оскільки за надзвичайної ситуації один неоновлений номер телефону може звести на нуль увесь ефективний план і завдати більше збитків, ніж витрати на створення такого плану.

Такі тестування та тренінги по BC планах здійснюються на основі плану тестувань та тренінгів (Test, Training, and Exercise – TTE). Такий план рекомендується складати на кожен рік та включати у нього усі плани, які є в організації. Окремо потрібно розробити процес перегляду внутрішніх документів за напрямком BCM, наприклад, таких як BCM-Стратегія чи Політика, щоб вчасно реагувати на зміну зовнішніх чинників і вплив загальної стратегії компанії або інших внутрішніх факторів.

Залежно від наявних ресурсів і підходу менеджменту компанія може обрати для себе кілька варіантів проведення тестування, в тому числі комбінуючи їх. Тестування можна розподілити за такими групами:

**Повний тест (Full test)**. Приклад: повне відключення енергопостачання будівлі без попереднього повідомлення та переміщення здійснення діяльності.

**Тестування діяльності (Activity test).** Приклад: переміщення здійснення діяльності до іншого місця;

відновлення існуючої роботи з віддаленого місця; часткова евакуація працівників – попередньо погоджено наказом / розпорядженням.

**Симуляція (Simulation exercise or Imitation)**. Приклад: визначення конкретного сценарію (наприклад, вихід з ладу основної банківської системи); оцінка можливого впливу, документація, що могла бути підготовлена (наприклад, повідомлення пресі).

**Перегляд (Walkthrough or Tabletop test)**. Приклад: задіяна особа «проходиться» по планах під час робочих нарад, користуючись допоміжними матеріалами (перелік, форми, плани приміщень...).

## ВИСНОВКИ

Управління безперервністю бізнесу забезпечує об'єднання всіх застосовуваних на підприємстві заходів у цілісний, адекватний реальним загрозам і керований комплекс, що дозволяє компанії безперервно надавати послуги, уникнути впливу надзвичайних ситуацій на діяльність і мінімізувати можливий збиток.

Цей комплекс складається з багатьох складових, які повинні бути реалізовані в компанії для забезпечення безперервності надання послуг і виробництва продуктів. Для впровадження системи в управління безперервністю бізнесу потрібно чітко диференціювати кризовий менеджмент та процес відновлення під час катастрофи. Не менш важливою складовою також є своєчасне тестування планів безперервності для їх відповідності реальним загрозам і сучасним реаліям.

Таким чином, менеджменту організації необхідно дотримуватися найкращих світових практик впровадження та підтримки системи BCM задля стабільної роботи компанії та уникнення непередбачених операційних витрат. ■

## ЛІТЕРАТУРА


**1.** Saul Midler ISO 22301 Security and resilience – Business continuity management systems – Requirements // ISO/TC 292 Technical Committee. URL: http://www.isotc292online.org/projects/iso-22301-revision/

**2.** Societal security – Business continuity management systems – Requirements ISO 22301:2012 // International Organization for Standardization. URL: https://www.iso.org/standard/50038.html

**3.** Marianne Swanson, Pauline Bowen, Amy Wohl Phillips, Dean Gallup, David Lynes. Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems // NIST. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf

**4.** Семь шагов к непрерывности бизнеса // Softline. URL: https://habr.com/company/softline/blog/261053/

**5.** Special Publication 800-84 «Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities» // NIST, Department of Homeland Security. URL: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

**6.** Dr Jim Watterston, Business Continuity Management Framework 2014 -18 // Queensland Government, Australia. URL: https://qed.qld.gov.au/det-publications/managementandframeworks/Documents/business-continuity/business-continuity-management-framework.pdf

**7.** Margaret Rouse Business continuity management (BCM) // SearchCIO. URL: https://searchcio.techtarget.com/definition/business-continuity-management-BCM

**8.** Business Continuity and Crisis Management [Naeem Ahmed Subhani (KUFPEC Pakistan Group), Muhammad Zafar Iqbal (KUFPEC Pakistan Group), Muhammad Mehmood Khan (KUFPEC Pakistan Group)] / Society of Petroleum Engineers, 2016. URL: https://www.onepetro.org/conference-paper/SPE-185315-MS



**Науковий керівник – Копилюк О. І.**,
доктор економічних наук, професор, завідувач кафедри фінансово-економічної безпеки та банківського бізнесу Львівського торговельно-економічного університету


## REFERENCES


"Business Continuity and Crisis Management [Naeem Ahmed Subhani (KUFPEC Pakistan Group), Muhammad Zafar Iqbal (KUFPEC Pakistan Group), Muhammad Mehmood Khan (KUFPEC Pakistan Group)]" Society of Petroleum Engineers, 2016. https://www.onepetro.org/conference-paper/SPE-185315-MS

"Dr Jim Watterston, Business Continuity Management Framework 2014 -18" Queensland Government, Australia. https://qed.qld.gov.au/det-publications/managementandframeworks/Documents/business-continuity/business-continuity-management-framework.pdf

"Margaret Rouse Business continuity management (BCM)" SearchCIO. https://searchcio.techtarget.com/definition/business-continuity-management-BCM

"Saul Midler ISO 22301 Security and resilience – Business continuity management systems – Requirements" ISO/TC 292 Technical Committee. http://www.isotc292online.org/projects/iso-22301-revision/

"Sem shagov k nepreryvnosti biznesa" [Seven steps to business continuity]. Softline. https://habr.com/company/softline/blog/261053/

"Societal security - Business continuity management systems - Requirements ISO 22301:2012" International Organization for Standardization. https://www.iso.org/standard/50038.html

"Special Publication 800-84 «Guide to Test, Training, and Exercise Programs for IT Plans and Capabilities»" NIST, Department of Homeland Security. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-84.pdf

Swanson, M. et al. "Special Publication 800-34 Rev. 1 Contingency Planning Guide for Federal Information Systems" NIST. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-34r1.pdf