https://www.sworldjournal.com/index.php/swj/article/view/swj28-00-034
DOI: 10.30888/2663-5712.2024-28-00-034

УДК 338.242:330. 658:005

THE ROLE OF SITUATION CENTERS IN ENSURING BUSINESS CONTINUITY

РОЛЬ СИТУАЦІЙНИХ ЦЕНТРІВ У КОНТЕКСТІ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

Soliar V.V. / Соляр В.В.
c.e.s., as.prof. / к.е.н., доц.
ORCID: 0000-0002-2093-6303
H.S. Skovoroda Kharkiv National Pedagogical University,
Kharkiv, Alchevskyh 29, 61002
Харківський національний педагогічний університет імені Г.С. Сковороди,
м. Харків, вул. Алчевських 29, 61002

Анотація. *Підприємці в усьому світі все більше замислюються про стійкість бізнесу до негативних впливів природного, техногенного, політичного чи соціального характеру. Прогресивні керівники знають, наскільки важливо, щоб підприємства функціонували без перебоїв, і вживають необхідних заходів, спрямованих на забезпечення безперервності бізнесу. У зв'язку з цим у мистецтві управління організаціями зростає роль ситуаційних центрів як форми реалізації системи підтримки прийняття рішень, що ґрунтується на технологіях моделювання та аналізу ситуацій. На основі порівняння різних підходів до визначення поняття «безперервність бізнесу» та сучасних моделей ситуаційних центрів, автор зазначає переваги їх застосування залежно від цільової спрямованості.*

Ключові слова: *безперервність бізнесу, ситуаційний центр, максимально допустимий час простою, цільовий час відновлення, система підтримки прийняття рішень.*

Вступ.

Необхідність збереження стійкості в динамічних умовах господарювання ставить перед сучасними організаціями складну проблему ситуативного управління, насамперед з позицій їх стійкого функціонування та розвитку в цілому. Компенсувати обмеження консервативного менеджменту за таких обставин покликані менш точні механізми управління — ситуаційні центри. Підприємства та організації зацікавлені в ефективному функціонуванні усіх підсистем, включаючи виробничу, і не лише в короткостроковому періоді, а й на досить тривалу перспективу, гнучко реагуючи на зміни. Захист матеріальних і нематеріальних активів організації, у тому числі її репутації, демонструють навіть галузеві монополісти та органи державної влади. Тому далі під словом «організація» ми будемо мати на увазі державну, комерційну або некомерційну структуру, зацікавлену в підтримці безперервності бізнесу (ББ) (діяльності). ББ є важливою складовою загальної стійкості організації та допомагає їй мінімізувати збитки, пов'язані з непередбачуваними та надзвичайними ситуаціями. Існує декілька причин, чому ці інструменти стають все більш важливими для українських організацій:

- нестабільність геополітичної ситуації – війна в Україні призвела до значної нестабільності та невизначеності;
- зростання кіберзагроз, які стають все більш складними та небезпечними (захист від кібератак та швидке відновлення після них);
- зростання залежності діяльності організацій від ІТ-систем. Тому усе більше

приватних підприємств, фінансових та державних установ долучаються до системи забезпечення безперебійної діяльності критичних служб та захисту від ризиків і втрат.

Виклад основного матеріалу.

Забезпечення безперервності бізнесу спрямоване на пом'якшення наслідків негативного впливу, що перериває ділову активність організації, скорочення часу вимушеної заміни активів і витрат, викликаних цією заміною. Термін «безперервність бізнесу» не зовсім збігається зі своїм англійським еквівалентом (business continue). На відміну від англійського контексту, слово «бізнес» в українській лексиці має яскраво виражений відтінок підприємництва, що провокує незручні формулювання, такі, наприклад, як «забезпечення безперервності бізнесу податкової інспекції». У контексті дослідження «безперервність бізнесу» використовується у значенні неперервність діяльності або ділової активності як здатності організації до відновлення критичних для її діяльності процесів протягом нормативного терміну.

Для порівняння підходів наведемо визначення ББ деяких авторів. Роберт Джексон, ББ — це не просто план на випадок надзвичайних ситуацій, культура стійкості, яка пронизує всю організацію. Це не є одноразовий проект, а постійний процес, який потребує вдосконалення та адаптації [1].

Діана Лоуренс, ББ — це захист не лише IT-систем, а всього, що має значення для бізнесу, включаючи людей, дані та репутацію, це не витрата, це інвестиція, яка може окупитися багатократно в разі надзвичайної ситуації [2].

Джон Вільямс, ББ — це готовність до надзвичайних ситуацій, швидке та ефективне відновлення після них, це командна робота, яка потребує співпраці усіх членів організації, щоб бути успішною [3].

У системі ISO 22301, міжнародному стандарті, який надає рекомендації щодо впровадження та керування системами ББ, прописано, що ББ — це система менеджменту, яка допомагає організаціям підготуватися, реагувати та відновлюватися після надзвичайних ситуацій. ISO 22301 представлена професійною організацією BCI, яка сприяє розвитку та поширенню найкращих практик у галузі ББ. Вона пропонує широкий спектр ресурсів, включаючи навчання, сертифікації та публікації, щоб допомогти організаціям впровадити ББ [4, 5].

Управління безперервністю бізнесу (Business Continue Management, BCM) — це цілісний процес управління, в рамках якого ідентифікуються потенційні загрози діяльності організації, оцінюються можливі впливи на бізнес-операції у разі реалізації цих загроз, а також створюється система приписів для забезпечення здатності організації відновлювати свою діяльність та ефективно реагувати на інциденти, що дозволяє гарантувати дотримання інтересів зацікавлених сторін, забезпечити захист репутації, бренду та створюють цінність операцій. Серед них мають значення інформаційні технології захисту інформації ISO/IEC 27031:2011 — настанови щодо готовності інформаційно-комунікаційних технологій до неперервності бізнесу. Це міжнародний стандарт, який надає практичні рекомендації щодо керування безперервністю інформаційно-комунікаційних технологій (ІКТ) (Information and Communication

Technology Continuity Management, ICTCM) в організаціях [6].

Мета стандарту:

- допомогти організаціям забезпечити стійкість та доступність ІКТ-інфраструктури та сервісів у разі виникнення надзвичайних ситуацій;
- мінімізувати негативний вплив на бізнес-процеси та репутацію організації;
- забезпечити відповідність вимогам законодавства та нормативних актів.

Стандарт ISO/IEC 27031:2011 базується на моделі життєвого циклу ICTCM, яка включає такі етапи [4]:

1) визначення критичних ІКТ-активів та послуг, а також потенційних загроз для їх безперервності;
2) оцінка ймовірності та впливу загроз на ІКТ-активи та послуги;
3) розробка та впровадження стратегії ICTCM — плану дій для запобігання надзвичайним ситуаціям, реагування на них та відновлення після них;
4) регулярне тестування плану ICTCM та навчання персоналу діям у надзвичайних ситуаціях;
5) постійний моніторинг ефективності системи ICTCM та внесення необхідних змін.

Впровадження ISO/IEC 27031:2011 у ситуаційному управлінні організацією має переваги за рахунок підвищення стійкості та доступності ІКТ-інфраструктури та сервісів; зниження ризиків збоїв та втрат даних; покращення здатності організації швидко відновлюватися після надзвичайних ситуацій; підвищення довіри клієнтів та партнерів; зниження витрат, пов'язаних з перебоями в роботі ІКТ [4, 6]. ISO/IEC 27031:2011 є цінним інструментом для будь-якої організації, яка прагне забезпечити стійкість та доступність своїх ІКТ-систем.

Очевидно, безперебійність діяльності організації не може бути абсолютною, перерви неминучі, тому опишемо критерій безперервності бізнесу. Порушення безперервності завдає організації очевидної шкоди. Розмір шкоди залежить від часу вимушеного простою, який витрачається на відновлення діяльності, хоча б в обмеженому обсязі життєво важливих для організації процесів. Динаміка зростання таких втрат має галузевий характер, але у більшості випадків відома межа, перевищення якої зробить процес незворотнім. Відрізок часу, протягом якого шкода стане неприйнятною, називають «максимально допустимий час простою» (Maximum Tolerable Outage, MTO) — це критичний показник, який використовується в ситуативному управлінні для визначення максимально допустимого періоду часу, протягом якого критична система або процес можуть бути недоступними без серйозних наслідків для бізнесу.

MTO визначається для кожної критичної системи або процесу окремо, з урахуванням таких факторів:

- вплив простою на бізнес (які фінансові, репутаційні та інші збитки може понести організація внаслідок простою?);
- залежність від системи (наскільки критична дана система для роботи інших систем та процесів?);
- можливість відновлення (скільки часу знадобиться для відновлення роботи

системи після простою?);

- вартість запобігання простою (які ресурси потрібно витратити на те, щоб запобігти простою або мінімізувати його наслідки?).

Важливо зазначити, що МТО не є статичним показником. Він може змінюватися з часом залежно від змін у бізнес-середовищі, технологіях та інших факторах. МТО успішно використовується в ситуативному управлінні. Так, компанія, яка, наприклад, надає послуги онлайн-банкінгу, може визначити МТО для свого веб-сайту в 2 години. Це означає, що сайт не може бути недоступним більше 2 годин без того, щоб це не призвело до серйозних збитків для компанії. Лікарня може визначити МТО для своєї системи електронних медичних записів (EMR) в 1 годину. Це означає, що система EMR не може бути недоступною більше 1 години без того, щоб це не вплинуло на надання медичної допомоги пацієнтам. Виробнича компанія може визначити МТО для своєї конвеєрної лінії у 30 хвилин. Це означає, що конвеєрна лінія не може бути зупинена більше ніж на 30 хвилин без того, щоб це не призвело до значних втрат продукції.

Існує декілька методів розрахунку МТО. Один з поширених методів ґрунтується на аналізі ризиків. Цей метод передбачає визначення потенційних загроз для системи або процесу, оцінку ймовірності виникнення кожної загрози та її впливу на бізнес, розрахунок загального ризику простою. Інші методи розрахунку МТО включають використання бенчмарків (порівняння МТО для схожих систем або процесів в інших галузях), запит думок експертів про те, який МТО є прийнятним для даної системи або процесу, використання комп'ютерних моделей для прогнозування впливу простою на бізнес.

Важливо вибрати метод розрахунку МТО, який найкраще відповідає потребам організації. На практиці підприємства використовують різні методи визначення МТО, залежно від специфіки їх бізнесу та IT-інфраструктури. Згідно з дослідженнями Gartner, середній МТО критичних для бізнесу IT-систем становить 2 години. А дослідження Uptime Institute вказують, що 98% підприємств вважають, що МТО в 1 годину або менше є критичним для їх бізнесу. Згідно з дослідженням Forrester, 1 година простою IT-системи може призвести до збитків у розмірі $100 000 для середнього підприємства [7-9].

Наближатися впритул до МТО небезпечно, і керівництво організації вибирає «цільовий час відновлення» (Recovery Time Objective, RTO), при якому фактична шкода не перевищить заданого «порогу шкоди» (Financial Threshold, FT). У практичній моделі безперервності бізнесу складна динаміка зростання шкоди від простою замінюється впорядкованою парою параметрів: порогом шкоди, пов'язаного з вимушеним простоєм (FT); часом, протягом якого діяльність має бути відновлена (RTO). Значення RTO не слід обирати «з запасом», оскільки кожна година зниження цього нормативу може обернутися серйозними витратами. Незважаючи на те, що практично будь-який керівник назве граничний термін простою керованої ним організації, перевищення якого призведе до її краху, наявність нормативу відновлення діяльності — все ще рідкість. Проте прогресивні керівники служб безпеки стали включати завдання забезпечення неперервності бізнесу до переліку своїх службових обов'язків.

Практика господарювання знає два основних інструменти забезпечення

безперервності. Перший — це «план забезпечення безперервності бізнесу» (Business Continuity Plan, BCP). Для більшості організацій зруйновані в результаті впливу активи, такі як обладнання, приміщення та, як це не цинічно, персонал, можуть бути замінені. У відношенні даних / інформації організації ситуація принципово інакша. Втрата даних може призвести до серйозних збитків для бізнесу, включаючи втрату клієнтів, шкоду репутації та перебої в роботі. Тому у цьому сенсі, коли регламентувати порядок дій у будь-якій ситуації неможливо, є продуктивним використання роботи ситуаційних центрів.

Сучасне поняття «ситуаційний центр» трактується як сукупність програмно-технічних засобів, науково-математичних методів та інженерних рішень для автоматизації процесів відображення, моделювання, аналізу ситуацій та прийняття управлінських рішень. Ситуаційний центр — це форма реалізації системи підтримки прийняття рішень (СППР), яка ґрунтується на технологіях моделювання та аналізу ситуацій, а також на максимально концентрованому представленні інформації. Іншими словами, ситуаційний центр системи підтримки прийняття рішень це комплексна система, яка об'єднує:

- програмно-технічні засоби: комп'ютери, програмне забезпечення, датчики, мережі та інші технології, які використовуються для збору, обробки та візуалізації даних;
- науково-математичні методи: алгоритми, моделі та інші методи, які використовуються для аналізу даних та прогнозування розвитку ситуації;
- інженерні рішення: технічні рішення, які забезпечують надійну та ефективну роботу ситуаційного центру.

Ситуаційні центри виконують важливі функції. Ситуаційний центр збирає інформацію з різних джерел, таких як датчики, системи моніторингу, бази даних та звіти. Ця інформація обробляється та аналізується для отримання актуальної картини ситуації. Він може використовувати математичні моделі для прогнозування розвитку ситуації та оцінки можливих наслідків різних рішень.

Ситуаційний центр використовує різні способи візуалізації інформації, такі як графіки, діаграми, карти та відео, щоб допомогти користувачам швидко та легко її зрозуміти. Надає користувачам інформацію та аналітику, необхідні для прийняття обґрунтованих рішень.

Ситуаційні центри використовуються в різних сферах, таких як державне управління, бізнес, транспорт, енергетика тощо для моніторингу та управління надзвичайними ситуаціями, такими як стихійні лиха, терористичні атаки та епідемії; для моніторингу ринкових умов, конкурентної активності та інших факторів, які можуть вплинути на діяльність компанії; здійснення моніторингу трафіку, управління транспортними потоками та забезпечення безпеки перевезень, роботи електромереж, прогнозування попиту на енергію та управління енергоспоживанням.

Ситуаційні центри слід віднести до нового покоління інструментів управління. На відміну від плану забезпечення безперервності, елемента консервативного менеджменту, продукт ситуаційного центру - не інструкція, а інформаційна підтримка прийняття рішення. У той же час алгоритми та моделі роботи з даними, що використовуються в ситуаційному центрі, слід відносити до

елементів консервативного менеджменту.

За цільовою спрямованістю фахівці виділяють п'ять типів ситуаційних центрів: ситуаційний центр контролю та спостереження за станом складного об'єкта або системи; ситуаційний центр управління, головне завдання якого - постійне та активне управління об'єктом; кризовий ситуаційний центр, активна робота якого здійснюється лише при виникненні надзвичайних (кризових) ситуацій; ситуаційний центр навчання, призначений для навчання оперативного та обслуговуючого персоналу ситуаційного центру; багатоцільовий ситуаційний центр, що поєднує в собі різні можливості.

Але на наш погляд, за призначенням має сенс виділяти три типи ситуаційних центрів: надзвичайних ситуацій, забезпечення безперервності бізнесу, управління ризиками. Межу між ситуаційними центрами надзвичайних ситуацій та забезпечення безперервності бізнесу важко розрізнити, але вона існує. Перша відмінність у тому, що у ситуаційного центру забезпечення неперервності існує вимірюваний критерій успішності – цільовий час відновлення (RTO). Інша відмінність у тому, що сигналом для початку роботи ситуаційного центру надзвичайних ситуацій служить зовнішнє повідомлення, тоді як ситуаційний центр забезпечення безперервності постійно працює в режимі моніторингу, скануючи тривожні сигнали систем організації. І останнє: задача забезпечення неперервності діяльності значно більше занурена в контекст операційної діяльності організації.

Нерідко ситуаційними центрами називають BI-системи (Business Intelligence), застосування яких націлене на пошук закономірностей у даних, що породжуються механізмами консервативного менеджменту. Така трактовка призначення ситуаційного центру характерна для банків і страхових компаній, інших організацій з високою IT-залежністю. Обидва типи систем збирають, обробляють та аналізують дані з різних джерел. І ситуаційні центри, і BI-системи використовують різні методи візуалізації даних, щоб допомогти користувачам швидко та легко зрозуміти інформацію. Обидва типи систем надають користувачам інформацію та аналітику, необхідні для прийняття обґрунтованих рішень. Але якщо ситуаційні центри, як правило, зосереджені на моніторингу та управлінні поточними ситуаціями, то BI-системи, з іншого боку, більше орієнтовані на аналіз минулих даних та прогнозування майбутніх тенденцій. Ситуаційні центри зазвичай використовуються керівництвом та операторами, які потребують швидкого доступу до інформації для прийняття рішень. BI-системи, навпаки, можуть використовуватися широким колом користувачів, включаючи аналітиків, менеджерів та рядових співробітників.

Висновки.

Використання й розширення сфери застосування ситуаційних центру може призвести до більш гнучкого та адаптивного стилю управління. Це пов'язано з тим, що керівництво зможе використовувати центр для збору інформації та прийняття рішень у режимі реального часу, покращити комунікацію та координацію між різними підрозділами організації. Центр може слугувати централізованим сховищем інформації та платформою для обміну даними.

Застосування ситуаційного центру також пов'язане з деякими додатковими витратами – значними інвестиціями у нові технології, програмне забезпечення та підготовку відповідного персоналу. Проте, ми вважаємо, що потенційні переваги розширення сфери застосування ситуаційного центру як от мінімізація збитків, швидке відновлення після надзвичайних ситуацій та захист репутації переважують ризики. Ситуаційні центри забезпечення безперервності можуть стати потужним інструментом для покращення ефективності, стійкості та адаптивності організацій.

Література:

1. Jackson, Robert. National Education Consultant. URL: https://www.robertjacksonmotivates.com/
2. Lawrence, Diana. Business Continuity Management. URL: https://drii.org/resources/professionalpractices/EN
3. Williams, John. What is the BCI? URL: https://www.thebci.org/
4. BPM: інструмент для трансформації бізнесу: Офіційний сайт Deloitte Україна URL: https://www2.deloitte.com/il/en/pages/technology/solutions/Business_Process_Management_BPM.html
5. ISO/IEC 27031:2011 - Information technology - Security techniques - Guidelines for ICT continuity management. URL: https://www.iso.org/standard/44374.
6. DNV GL - ISO/IEC 27031:2011 ICT Continuity Managemen. URL: https://www.dnv.com/se/assurance/businesscontinuity/
7. Forrester. URL: https://www.forrester.com/
8. Gartner Press Release. URL: https://www.gartner.com/en/documents/4891031
9. Uptime Institute. URL: https://uptimeinstitute.com/

References:

1. Jackson, Robert. National Education Consultant. URL: https://www.robertjacksonmotivates.com/ [in English]
2. Lawrence, Diana. Business Continuity Management. URL: https://drii.org/resources/professionalpractices/EN [in English]
3. Williams, John. What is the BCI? URL: https://www.thebci.org/
4. BPM: a tool for business transformation: Official website of Deloitte Ukraine. URL: https://www2.deloitte.com/il/en/pages/technology/solutions/Business_Process_Management_BPM.html [in Ukrainian]
5. ISO/IEC 27031:2011 - Information technology - Security techniques - Guidelines for ICT continuity management. URL: https://www.iso.org/standard/44374. [in English]
6. DNV GL - ISO/IEC 27031:2011 ICT Continuity Managemen. URL: https://www.dnv.com/se/assurance/businesscontinuity/ [in English]
7. Forrester. URL: https://www.forrester.com/ [in English]
8. Gartner Press Release. URL: https://www.gartner.com/en/documents/4891031 [in English]
9. Uptime Institute. URL: https://uptimeinstitute.com/ The World Bank [in English]

Abstract. *The article is devoted to the study of the role of situational centers - modern mechanisms for managing an organization in order to compensate for the shortcomings of conservative management and ensure uninterrupted operations in the short term and in the future.*

The relevance and effectiveness of their application in conditions of instability for organizations of various subordination, industries and forms of ownership are proven. The sustainability of business activity is chosen as the criteria for business continuity. This is the ability of an organization to restore processes critical to its activities within the regulatory period. The effectiveness of compliance with international standards that provide recommendations for the implementation and management of business continuity systems is proven. The use of a critical indicator in situational management is important to determine the maximum permissible period of time during which a critical system or process may be unavailable without serious consequences for the business. It is concluded that the potential benefits of expanding the scope of application of the situational center outweigh the risks (minimization of losses, rapid recovery from emergencies, reputation protection). Situational continuity centers can be a powerful tool for improving the efficiency, resilience, and adaptability of organizations.

Keywords: *Business Continuity, Situation Center, Maximum Tolerable Outage, Recovery Time Objective, Decision Support System.*

Стаття підготовлена відповідно до наукової теми 0122U201101 «Соціально-економічні умови та інноваційні чинники забезпечення економічного зростання національної економіки» кафедри менеджменту та економіки ХНПУ імені Г.С.Сковороди та в рамках проведення однойменного методологічного семінару

Стаття відправлена: 24.11.2024 р.