ISO та менеджмент безперервності бізнесу

В. Ситніченко, кандидат технічних наук, директор,
Г. Кісельова, завідувач сектору,
Є. Стоякін, завідувач сектору,
НТЦ «Станкосерт», м. Одеса

ISO и менеджмент непрерывности бизнеса
В. Ситниченко, кандидат технических наук, директор,
А. Киселева, заведующий сектором,
Е. Стоякин, заведующий сектором,
НТЦ «Станкосерт», г. Одесса

ISO and Business Continuity Management
V. Sytnichenko, Candidate of Technical Scientist, Director,
H. Kiselyova, Section Chief,
Ye. Stoyakin, Section Chief,
Scientific and Technical Centre «Stankocert», Odesa

Керівник вищої ланки повинен проголосити на майбутнє політику: зберігати бізнес, забезпечувати співробітників роботою й створювати нові робочі місця.
Демінг Е. Передмова до книги «Вихід із кризи»


В. Ситніченко


Г. Кісельова


Є. Стоякін

Як видно із епіграфа, збереження бізнесу та його безперервності завжди було, є й буде актуальним завданням, бо у навколишньому бізнес-просторі існує безліч загроз для успішної діяльності підприємства, з різним рівнем ризику та наслідками від їх реалізації.

Ефективним методом боротьби із загрозами є системний підхід, реалізований через упроваджені в організації системи менеджменту (СМ) різної спрямованості. У табл. 1 наведено приклади усунення ризиків за допомогою відомих СМ. Насправді, ризиків дуже багато й деякі з них виходять за рамки сфери діяльності зазначених СМ.

У табл. 2 подано неповну класифікацію переривників (ризиків) бізнесу [1].

Зрозуміло, що ці переривники виникли не сьогодні, але їхня дія стає все хворобливішою для бізнесу. Дослідження, проведене Техаським університетом, виявило наступну статистику [2]:

- 85 % організацій сильно або повністю залежать від обчислювальних систем;
- у середньому на 6-й день перерви у роботі компанія втрачає 25 % щоденного доходу, а на 25-й день — 40 %;
- після перерви у роботі спостерігається швидке зростання фінансових втрат і погіршення функціонування;
- через два тижні після припинення роботи обчислювальних систем у 75 % компаній втрата функціонування стає критичною або повною;
- 43 % компаній, що не мають плану безперебійного функціонування, у разі виникнення переривника не відновляють свою діяльність, а через два роки продовжує функціонувати лише 10 % компаній.

Таблиця 1. Ризики, які розглядають у СМ

Система управління якістю (СУЯ)	Втрата клієнтів через незадовільну якість, невиконання нормативних вимог, невиконання строків з вини постачальників	Розрив безперервності бізнесу
Система управління навколишнім середовищем (СУНС)	Можливі зупинки виробництва й фінансові втрати через невиконання екологічних вимог	
Система управління безпекою праці (СУБП)	Можливі збої у виробництві й керуванні через травми й хвороби, необхідність залучення менш компетентних фахівців	
Система менеджменту безпеки ланцюга постачання (СМБЛП)	Втрата клієнтів через зрив поставок, стосовно яких домовлялися зазделегідь	
Система менеджменту інформаційної безпеки (СМІБ)	Збої у керуванні виробництвом через інформаційні крадіжки та інформаційні атаки	
Система менеджменту енергозаощадження (СМЕ)	Фінансові втрати та збої у виробництві через енергетичні проблеми	

Дослідження показало, що організації, які склали план дій у непередбачених обставинах, мали суттєво менші, у 2,5 рази втрати доходів. У зв'язку із цим, увага до питань менеджменту безперервності бізнесу постійно підсилюється. Суттєво посилилась увага до безперервності бізнесу у зв`язку з «проблемою 2000 року», коли напередодні цієї дати багато компаній почали ряд попереджувальних заходів у сфері інформаційної безпеки, логістики, енергозаощадження. Вважається, що збиток багатьох компаній США від теракту 11 вересня 2001 року був значною мірою сдемпфірований саме попереджувальними заходами [1]. Ряд країн і міжнародних організацій розробили й застосовують у себе стандарти безперервності бізнесу (табл. 3).

Згодом цією проблемою почала опікуватися ISO та створила програму розробляння цілого ряду стандартів з менеджменту безперервності бізнесу (табл. 4).

Основний стандарт серії ISO 22301 «Соціальна безпека. Системи менеджменту безперервності бізнесу. Вимоги» [3] опублікований 15.06.2012. У ньому наведено вимоги до розробляння й керування ефективною СМ безперервності бізнесу (Business Continuity Management System — BCMS). Відповідно до методології, прийнятої ISO, стандарт ISO 22301 за формою, структурою та основним підходом ідентичний раніше розробленим стандартам на СМ, наприклад ISO 14001, ISO 50001 тощо.

BCMS, як і всі інші СМ, має ключові компоненти:

а) політика;

б) співробітники, що несуть певну відповідальність;

в) процеси керування, спрямовані на:

1) політику;

2) планування;

3) упровадження й роботу;

4) оцінювання роботи;

5) аналіз з боку керівництва;

6) поліпшення;

г) документація, на якій засновано аудит;

д) усі процеси управління безперервністю бізнесу, що ставляться до організації.

Стандарт використовує відому модель PDCA — «plan — do—check — act» (ПВПД — «плануй — виконуй — перевіряй — дій») стосовно процесів BCMS (рисунок).

Використання моделі PDCA у системі BCMS, діє у рамках моделі PDCA (табл. 5)

Терміни, використовувані у стандарті, здебільшого взяті з раніше опублікованих стандартів, але є й свої специфічні терміни, наприклад:

▪ **Менеджмент безперервності бізнесу** (business continuity management). Глобальний процес менеджменту, який ідентифікує потенційні загрози для організації та вплив на бізнес у випадку їх реалізації, створює інфраструктуру для забезпечення швидкого відновлення організації з можливістю ефективного реагування для захисту інтересів основних акціонерів, репутації, бренда й фінансових операцій.

▪ **Мінімальні завдання безперервності бізнесу** (minimum business continuity objective). Мінімальний рівень послуг і/або продукції, прийнятний для організації з метою виконання завдань, що стосуються бізнесу, у період деструкції.

▪ **Максимальний прийнятний час простою** (maximum acceptable outage) або **максимальний припустимий час деструкції** (maximum tolerable period of disruption). Час, необхідний на нейтралізування шкідливого впливу, який може виникнути в результаті припинення виробництва, надання послуг або проведення заходів.

▪ **Час відновлення** (recovery time objective)**.** Період часу, що випливає за інцидентом, під час якого:

Таблиця 2. Класифікація переривників (ризиків) бізнесу (не вичерпна)

Тип переривника бізнесу	Англійська назва переривника	Українська назва переривника
Підприємницький	Business Relocation	Переїзд підприємства або організації в інше приміщення або офіс
	Espionage	Промислове шпигунство
	Loss of Records	Втрата архіву
	Mergers & Acquisitions	Злиття / придбання підприємств / організацій
	Negative Publicity	Негативна інформація про компанію в пресі
	IS swop	Перехід із ручної на автоматизовану інформаційну систему або з однієї автоматизованої системи на іншу
	Mask Show	«Наїзд» кримінальних, комерційних або державних структур (рейдерство)
Людський	Labor Disputes	Трудовий конфлікт (страйк, локаут тощо)
	Loss of Workforce	Організований відхід співробітників або їх втрата у результаті, наприклад, нещасного випадку
	Staffing Issues	Неможливість набрати співробітників
	Succession Planning	Відсутність планування заміщення посад
	The Human Factor	Людський фактор, тероризм у будь-якій формі та із застосуванням будь-якої зброї
	Unauthorized Access	Несанкціонований доступ
	White Collar Crime	Злочини «білих комірців»
	Workplace Violence	Силові конфлікти на робочих місцях
Техногенний	Blackouts	Віялове відключення електроенергії
	Computer Failure	Відмови комп'ютерів
	Computer Harking	Атаки хакерів
	Computer Viruses	Комп'ютерні віруси
	Environmental Hazards	Аварії систем життєзабезпечення (прорив каналізації, трубопроводів гарячої й холодної води, відмова повітряводів тощо)
	Multi-Tenant Sites	Проблеми, зумовлені розміщенням в одному будинку декількох компаній
	Power Outages	Перебої в електропостачанні
	Sick Building Syndrome	Синдром, зумовлений наявністю у матеріалах, з яких побудований будинок, шкідливих для здоров'я домішок
	Transportation Disruptions	Порушення роботи суспільного транспорту
Природний	Blizzards	Снігова буря
	Earthquakes	Землетрус
	Electrical Storms	Електромагнітні бурі
	Hurricanes	Урагани
	Tornadoes	Торнадо
Природно-техногенний	Winter Weather	Зимова погода
	Biological Hazards	Епідемії
	Fine	Пожежа
	Flooding	Повінь
	Artificial and natural objects landing	Падіння штучних (наприклад, літаків) і природних (наприклад, метеоритів) об'єктів із неба

Таблиця 3. Чинні стандарти у сфері безперервності бізнесу

Австралія	HB 221:2004. Менеджмент безперервності бізнесу HB 292-2006. Практичний посібник з менеджменту безперервності бізнесу AGN 232.1. Оцінка ризику й менеджмент безперервності бізнесу
Великобританія	BS 25999-1:2006. Менеджмент безперервності бізнесу — Ч.1: Практична настанова
	BS 25999-2:2007. Менеджмент безперервності бізнесу — Частина 2: Вимоги
	BS 25777:2008. Менеджмент безперервності бізнесу у сфері інформаційних технологій. Практична настанова
	BIP2142:2007. Менеджмент безперервності бізнесу. Посібник із упровадження відповідно до вимог BS серії 25999 BIP 2151:2008. Аудит планів у сфері безперервності бізнесу
	Практичний посібник з менеджменту безперервності бізнесу, 2006 (FSA, Bank of England and HM Treasury)
Ізраїль	SI 24001. Системи менеджменту безпеки й безперервність. Вимоги й посібник із застосування
США	NFPA 1600:2007. Керування в аварійних / надзвичайних ситуаціях і програми безперервності бізнесу ANSI/ASIS/BSI BCM.01-2010. Системи менеджменту безперервності бізнесу. Вимоги й посібник із застосування
Сінгапур	SS 540:2008. Менеджмент безперервності бізнесу
Міжнародна організація зі стандартизації (ISO)	ISO/PAS 22399:2007. Соціальна безпека — провідні вказівки для менеджменту безперервності операцій та готовності до інцидентів IWA 5:2006. Готовність до аварійних ситуацій Проект ISO/IEC WD 27031. Готовність IT до безперервності бізнесу
Японія	Вказівки щодо складання плану безперервності бізнесу. Міністерство економіки, торгівлі й промисловості Японії (2005 рік). Посібник з безперервності бізнесу. Центральна Рада з менеджменту надзвичайних ситуацій. Урядовий кабінет Японії (2005 рік)

- продукція або послуги повинні бути відновлені;
- діяльність повинна бути відновлена;
- ресурси повинні бути відновлені.

Примітка. Для продукції, послуг і діяльності час відновлення повинний бути менше часу, витраченого на шкідливий вплив, який може виникнути в результаті припинення виробництва, припинення надання послуг або проведення заходів.

▪ **Точка відновлення** (recovery point objective). Точка, у якій інформація, використана для діяльності, повинна бути збережена для того, щоб ця діяльність була відновлена.

Перший етап розробляння, упровадження й використання BCMS «Планування» необхідно починати з усвідомлення та розуміння контексту (суті) конкретної організації. Для цього треба під час аналізування визначити її та обов'язково документувати, щоб виключити суб'єктивне тлумачення:

▪ свою діяльність, функції, послуги, продукцію, партнерство, ланцюги постачання, взаємини із зацікавленими сторонами й потенційний вплив у випадку деструктивних ситуацій;

▪ зв'язок між політикою безперервності бізнесу й завданнями організації, а також з іншими напрямками політики, у тому числі стратегією керування ризиками в цілому;

▪ відношення організації до ризиків.

Це необхідно для того, щоб визначити: яка продукція або послуги, надавані організацією, є ключовими для її благополуччя; процеси й дії, які підтримують випуск цієї ключової продукції або надання ключових послуг. Необхідно позначити всі залежності ключових параметрів від третіх сторін.

Нарешті, треба визначити та оцінити кількісно, який вплив на діяльність організації може мати переривання критичних процесів або критичних активностей як через внутрішні, так і зовнішні, незалежні від організації, причини. Таким чином, маємо досить докладний і глибокий аналіз впливу різних чинників на бізнес конкретного підприємства.

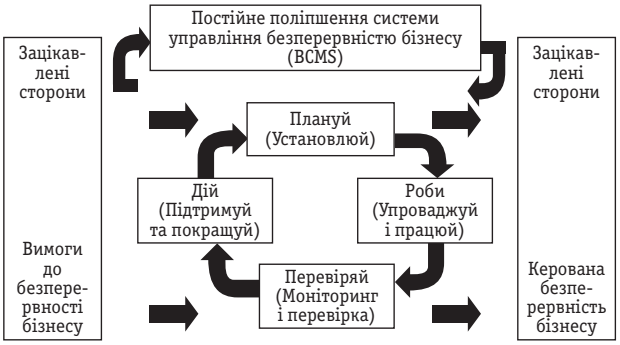
Природно, що для формування документованої інформаційної основи для прийняття рішень із забезпечення безперервності бізнесу, слід провести ідентифікацію та оцінку ризиків. Тут дуже важливо не заплутати в широкому полі різних ризиків — від

Таблиця 4. Стандарти ISO з менеджменту безперервності бізнесу

ISO 22300	Соціальна безпека. Основні положення й словники
ISO 22301	Соціальна безпека. Системи менеджменту безперервності бізнесу. Вимоги
ISO 22311	Соціальна безпека. Відеоспостереження
ISO 22312	Соціальна безпека. Технологічні можливості
ISO 22313	Соціальна безпека. Система менеджменту безперервності бізнесу. Управління
ISO 22320	Соціальна безпека. Надзвичайний менеджмент. Вимоги до реагування на інцидент
ISO 22322	Соціальна безпека. Надзвичайний менеджмент. Публічне оповіщення
ISO 22323	Соціальна безпека. Системи менеджменту організаційною стійкістю. Вимоги й посібник із застосування
ISO 22324	Соціальна безпека. Надзвичайний менеджмент. Колірне кодування попередження
ISO 22351	Соціальна безпека. Надзвичайний менеджмент. Загальна ситуаційна поінформованість
ISO 22397	Соціальна безпека. Державно-приватне партнерство. Посібник зі створення партнерських угод
ISO 22398	Соціальна безпека. Керівні принципи для навчань і випробувань
ISO 22399	Соціальна безпека. Посібник з підготовки до інциденту й менеджмент безперервності роботи

техногенних, інформаційних до особистісних — і виявити максимум знань, об'єктивності, тверезості у виділенні саме тих ризиків, які характерні саме для цієї організації та цього регіону. Наприклад, компанії «КПМГ у Росії й СНД» і «Linxdatacenter» у липні—серпні 2010 року провели дослідження у сфері забезпечення безперервності й відновлення діяльності у компаніях фінансового сектору [4].

За результатами опрацювання анкет, отриманих від російських і закордонних компаній фінансового сектору, з'ясувалося, що спочатку компанії основною ціллю вважали захист бізнес-процесів та IT-сервісів



Модель PDCA для BCMS

від ризиків, пов'язаних з порушеннями телекомунікаційних та інженерних систем, а також від природних і кліматичних аномалій. На практиці виявилося, що основні ризики — це не збої інженерних систем та порушення телекомунікацій, а виходи з ладу або некоректна робота IT-устаткування й відключення електроенергії. Сильно переоціненими також виявилися ризики виникнення катаклізмів як природного характеру (повені / землетрусу), так і антропогенного (тероризм / вандалізм) характеру.

На наш погляд, у процесі розробляння СМ безперервності бізнесу, фахівці підприємства повинні ближче познайомитися зі стандартами у сфері інформаційної безпеки [5], стандартами у сфері енергоменеджменту [6] і, за необхідності, стандартами з безпеки ланцюга постачання [7].

З ділової практики відомо, що вихід із кризових ситуацій за заздалегідь розробленим планом коштує дешевше, ніж вирішення проблем у міру їх виникнення. Тому після визначення й виділення всіх значних ризиків виникнення несприятливих інцидентів і, у першу чергу, інцидентів, причини яких не залежать від організації або від її впливу, розробляється план(и) безперервності бізнесу й реагування на інцидент(и). Істотна деталь полягає в тому, що ці плани повинні охоплювати всі фази відновлення діяльності, наприклад, первинне реагування, управління безперервністю бізнесу й повернення в штатний режим роботи.

Природно, що плани повинні містити опис інциденту, необхідні дії, відповідальних виконавців, ресурси, осіб, що ухвалюють розв'язання з активації тих або інших дій у випадку, якщо відповідальні виконавці не наділені такими повноваженнями. Необхідно відобразити усі внутрішні й зовнішні комунікації, залучення зовнішніх організацій тощо.

Необхідність опису в планах усіх перерахованих даних визначається складністю та серйозністю самого інциденту, а також кваліфікацією та рівнем підготовленості виконавців. Усі виконавці або групи виконавців повинні бути добре навчені й натреновані.

Таблиця 5. Дії у рамках моделі PDCA

Плануй	Розробляння політики безперервності бізнесу, мети, засобів керування, процесів та процедур поліпшення безперервності для отримання результатів, що узгодяться з політикою й цілями всієї організації
Виконуй	Упровадження й функціонування політики безперервності бізнесу, засобів управління, процесів і процедур
Перевіряй	Моніторинг і перевірка відповідності роботи цілям безперервності, надання керівництву результатів для аналізу, визначення повноважних дій для виправлень і поліпшення
Дій	Підтримка та поліпшення BCMS шляхом виконання коригувальних дій, заснованих на результатах аналізу з боку керівництва й перегляду галузі застосування BCMS, політики й цілей безперервності бізнесу

Плани повинні обов'язково обновлятися за результатами перевірок і реагування на інциденти.

Неспецифічні системні вимоги подібні вимогам відомих СМ:

- облік законодавчих вимог;
- моніторинг, виміри, аналіз та оцінювання результатів моніторингу й вимірювання;
- оцінка процедур безперервності бізнесу з метою забезпечення їх постійної адекватності й ефективності;
- внутрішній аудит;
- аналіз із боку керівництва;
- ідентифікація невідповідностей і проведення необхідних коригувальних дій;
- безперервне поліпшення.

Комерційні вигоди від упровадження BCMS за ISO 22301 [3]

1. Забезпечення безперервності бізнесу робить зрозумілішою для керівництва підприємства значимість упровадження СУЯ, екології, охорони праці, інформаційної безпеки, безпеки ланцюга постачання, енергоменеджменту, які мінімізують ризики підприємства за різних напрямків і тим самим зміцнюють упевненість у виживанні за несподіваних катастроф.

2. Виявляються основні загрози безпеці для існуючих бізнес-процесів (видів діяльності).

3. Розраховуються ризики та ухвалюються розв'язання на основі стратегічних і поточних бізнес-цілей підприємства.

4. Забезпечується ефективне управління підприємством у критичних ситуаціях, враховуючи загрози рейдерських атак.

5. Постійно здійснюється реалізація політики безпеки, тобто перебувають і виправляються слабкі місця у системі інформаційної безпеки.

6. Забезпечується інтеграція менеджменту організації та діяльності із забезпечення безперервності бізнесу.

7. Управління ризиками стає активним засобом ефективного управління, адже ключові рішення, пов'язані з виділенням ресурсів, ухвалюються на основі оцінювання ризиків.

8. Забезпечується поліпшення порівняльного аналізу, вимірювання, документування та звітності з підвищення стійкості підприємства й прогнозування впливу різних ризиків на безперервність бізнесу.

9. Забезпечується прозорість та взаємодія з менеджментом постачальників енергоресурсів, матеріалів, що комплектують, інформації.

10. Оцінюються нові технології у сфері інформаційної безпеки й вибір пріоритетів у їхнім застосуванні.

11. Поширюється ідеологія забезпечення безперервності бізнесу на весь ланцюг забезпечення енергоресурсами, матеріалами, що комплектують, інформацією.

12. Чітко визначаються обов'язки й особиста відповідальність.

13. Чіткий поділ відповідальності й підзвітності дозволяє раціонально управляти всіма наявними ресурсами.

14. Без труднощів здійснюється інтеграція з діючими СУЯ, екології, охорони праці, безпеки ланцюга постачання інформаційної безпеки.

15. Ґрунтуючись на циклі PDCA, система менеджменту з ISO 22301 цілком органічно вписується в інтегровану СМ підприємства на основі ISO 9001, ISO 14001, OHSAS 18001.

16. Постійна готовність щодо забезпечення безперервності бізнесу підвищує капіталізацію й кредитний рейтинг підприємства.

17. Раннє попередження й своєчасні коригувальні заходи збільшують потенціал поліпшення витрат на страхування та їх покриття.

18. Підвищується організаційна стійкість підприємства та здатність відповідати очікуванням зацікавлених сторін за найнесподіваніших обставин, тобто знижується ризик, що підприємству буде нанесено непо-

правний збиток від різних інцидентів, що впливають на його діяльність, фінансове здоров'я чи репутацію.

19. Забезпечується відповідність критеріям інвесторів і одержання доступу до фінансування за рахунок конкурентних переваг у швидкому й ефективному реагуванні на інциденти.

20. Завдяки відповідності міжнародному стандарту підкреслюється прозорість і чистота бізнесу перед законом, у т.ч. дотримання правових і нормативних вимог.

21. Гарантується демонстрація всім зацікавленим сторонам, і у тому числі, суспільству, надійність бізнесу, що сприяє міжнародному визнанню й зростанню авторитету компанії як на внутрішньому, так і на зовнішньому ринках.

Системи менеджменту безперервності бізнесу через інтегральний характер можна віднести до найефективніших інструментів виживання у сьогоднішніх кризових нестабільних умовах.

ЛІТЕРАТУРА

1. Альтерман Б.Д., Дрожжинов В.И., Моисеенко Г.Е. Обеспечение непрерывности деятельности организации в нештатных ситуациях [Електронний ресурс]. — Режим доступу: http://citforum.ru/security/articles/continuity/
2. Christensen, S. R., et. al «Financial and functional impacts of computer outages on businesses», Center for Research on Information Systems, The University of Texas at Arlington.
3. ISO 22301. Societal security — Business continuity management systems — Requirements (Социальная безопасность. Системы менеджмента непрерывности бизнеса. Требования).
4. Вестник КПМГ — Вып. 5. — Май 2011 [Електронний ресурс]. — Режим доступу: www.kpmg.ru
5. Ситніченко В., Кісельова Г., Стоякін Є. Формування інформаційної безпеки на основі стандарту ISO/IEC 27001:2005 // Стандартизація, сертифікація, якість. — 2010. — № 2. — С. 50—56.
6. Ситніченко В., Кісельова Г., Стоякін Є. Нові стандарти систем енергетичного менеджменту // Стандартизація, сертифікація, якість. — 2011. — № 3. — С. 53—58.
7. Ситніченко В., Кісельова Г., Стоякін Є. Системи управління безпекою ланцюга постачання за ISO 28000. Практичні аспекти // Стандартизація, сертифікація, якість. — 2010. — № 1. — С. 53—56.