УДК 004.891.3:004.056(045)

А.І. Гізун, аспірант (Національний авіаційний університет, Україна),
В.О. Гнатюк (Хмельницький національний університет, Україна),
О П. Дуксенко, старший викл. (Міжрегіональна академія управління персоналом, Україна),
А.О. Корченко, асистент (Національний авіаційний університет, Україна)

СУЧАСНІ ПІДХОДИ ДО ЗАХИСТУ ІНФОРМАЦІЙНИХ РЕСУРСІВ ДЛЯ ЗАБЕЗПЕЧЕННЯ БЕЗПЕРЕРВНОСТІ БІЗНЕСУ

У роботі піднімається питання забезпечення надійності функціонування бізнес-процесів в умовах впливу негативних чинників кризових ситуацій. Крім того висвітлена концепція безперервності бізнесу. Дано визначення поняттю «кризова ситуація», наведені підходи до їх класифікації. Також, виділені фундаментальні терміни даної концепції – BCP і DRP, розглянуті відмінності між ними і наведено життєвий цикл планування BC.

З розвитком можливостей ІТ у сучасному світі на передній план виходить автоматизація управлінських, технологічних, виробничих та інших процесів. Таким чином інформаційні системи займають провідні ролі в системі функціонування бізнесу, причому взаємозв'язок ІТ та бізнес-процесів стає настільки тісним, що життєздатність підприємств повністю залежить від надійності технологій, що забезпечують підтримку найбільш важливих критичних бізнес-процесів.

Десять-п'ятнадцять років тому провідні світові компанії, в першу чергу - фінансовий сектор ринку, усвідомили ступінь залежності бізнесу від інформаційних технологій. Великі корпорації почали цілеспрямовано впроваджувати технології забезпечення безперервності бізнесу (ЗББ) в непередбачених ситуаціях [3].

У розвинених країнах ринок технологій і послуг, що забезпечують безперервність бізнесу (ББ), динамічно розвивається. Рівень його зростання становить близько 25% на рік і обумовлений, головним чином, тим, що середні компанії слідом за лідерами індустрії активно впроваджують у себе технології управління кризовими ситуаціями (КС) [2]. При цьому все більш актуальним стає забезпечення захисту від не катастрофічних, але більш ймовірних надзвичайних ситуацій.

Управління безперервністю бізнесу (УББ) на даний момент є одним з найбільш актуальних і динамічно розвиваючихся напрямків стратегічного та оперативного менеджменту сучасних підприємств [3]. Так, проаналізувавши досвід вітчизняних компаній, можна виділити такі основні проблеми: відсутність формалізованого опису БП, нерегулярний або неповний аналіз впливів на критично важливі бізнес-процеси, недостатня системна обробка предметної області, невідповідність підготовки персоналу тощо [1]. Таким чином, визначення основних термінів значно підвищило ефективність ЗББ. Саме в цьому полягає актуальність даної роботи.

Метою даної роботи є аналіз сучасних підходів захисту інформаційних ресурсів для ЗББ шляхом виділення основних понять ББ, їх визначення та класифікації для формалізації УББ, а також визначення проблем у даному питані та шляхів їх вирішення.

В роботах [1-7] наведені відомості законодавчого, науково-теоретичного та практичного характеру щодо ББ. Здійснивши аналіз даних та інших відомих джерел визначимо основні поняття УББ. Дослідження доцільно розпочати з визначення основних понять. Розглянемо деякі основні терміни, що використовуються в області технологій УББ.

Визначення кризових ситуацій та існуючі підходи їх класифікації

УББ спрямоване на захист активів та ресурсів підприємства чи організації від впливу КС. Тому найперше потрібно дати визначення терміну «кризова ситуація». Так стандарти та нормативні документи в галузі ЗББ дають наступні визначення:

Криза – ненормальна ситуація, яка загрожує операціям, персоналу, клієнтам і репутації підприємства [7].

Інцидент – подія, здатна привести до втрати чи порушення діяльності організації, послуг або функцій підприємства. Причому у випадку відсутності контролю вона може перерости в надзвичайну ситуацію, кризу або стихійне лихо [4-6].

Надзвичайна ситуація – загальний термін з різними інтерпретаціями в залежності від регіону. У США він означає широкомасштабну катастрофу, що вимагає федеральної підтримки і запуск фінансування Федеральної агенції управління надзвичайними ситуаціями. В інших країнах – вважається еквівалентними за змістом серйозним інцидентам [6].

Громадянська надзвичайна ситуація – подія або ситуація, яка може нанести серйозних збитків людському добробуту, навколишньому середовищу в будь-якому місці чи порушити безпеку цього місця [4,5].

Катастрофа – фізичне подія, що перериває бізнес-процеси достатньо, щоб загрожувати життєздатності організації [6].

Усі вищеназвані явища та процеси, хоча і мають різний характер та природу, негативно впливають на функціонування бізнес-процесів і бізнесу в цілому. Для уникнення проблем та непорозумінь в розвитку УББ дамо єдиний загальний термін для їх визначення. Кризова ситуація в аспекті безперервності бізнесу – це певна ситуація чи подія, що має місце на деякій території (організації, підприємстві), потенційно здатна нанести серйозних збитків організації, призвести до порушення діяльності організації, втрати послуг або функцій підприємства в достатньому об’ємі щоб загрожувати життєздатності організації.

Існує декілька підходів до класифікації КС. Однією з найбільш популярних є класифікація «переривників бізнесу» залежно від їх типу. Виділяють п’ять основних типів КС в залежності від природи негативного чинника:

1) підприємницький (переїзд підприємства чи організації в інше приміщення або офіс; промислове шпигунство; втрата архівів; злиття/придбання підприємств/організацій; перехід з ручної на автоматизовану інформаційну систему або з однієї автоматизованої системи на іншу; випадки рейдерства з боку кримінальних, комерційних чи державних структур);

2) соціальний (трудовий конфлікт, страйк; організований вихід співробітників або їх втрата в результаті, наприклад, нещасного випадку; неможливість набрати співробітників; людський фактор, тероризм у будь-якій формі і з застосуванням будь-якої зброї; несанкціонований доступ; злочини "білих комірців");

3) техногенний (відключення електроенергії; збої комп'ютерів; атаки хакерів; комп'ютерні віруси; аварії систем життєзабезпечення (прорив каналізації, трубопроводів та ін.); перебій у електропостачанні; порушення роботи громадського транспорту);

4) природний (снігова буря; землетрус; електромагнітні бурі; урагани; торнадо);

5) природно-техногенний (зимова погода; епідемії; пожежа, повінь).

Окрім даної класифікації КС можна поділити на види відносно можливості їх прогнозування (передбачувані і несподівані), за масштабом (кризові ситуації в рамках окремого бізнес-процесу, підприємства, на рівні групи підприємств) і т.п.

Проте жодна з існуючих класифікацій не є повної та не охоплює всіх аспектів. Тому в подальшому є необхідним провести систематизацію КС.

Планування ББ і аварійного відновлення як фундаментальні поняття УББ

Визначивши і розглянувши поняття «кризова ситуація», що є одним з центральних об’єктів УББ, перейдемо до розгляду його фундаментальних основ – процесів стратегічного менеджменту. Проаналізувавши напрацювання фахівців Інституту безперервності бізнесу (Business Continuity Institute, BCI), Міжнародного інституту відновлення після катастроф (Disaster Recovery Institute International, DRII) і інші наукові публікації та нормативно-правові акти виділимо два напрямки розвитку концепції: планування ББ і відновлення бізнес-процесів після аварій та катастроф. Розглянемо основні терміни стосовно названих напрямків захисту інформаційних ресурсів підприємства чи організації:

Безперервність бізнесу (Business Continuity, BC) - стратегічні й тактичні можливості організації для планування та реагування на інциденти і збої БП з метою продовження ділових операцій на прийнятному рівні [4-7].

Планування безперервності бізнесу (Business Continuity Planning, BCP) – процес попередньої розробки механізмів та процедур, які дозволяють організації реагувати на події таким чином, що критичні бізнес-функцій можуть продовжувати своє функціонування протягом запланованого часу порушення. Кінцевим результатом цього процесу є план ББ [6].

План забезпечення безперервності бізнесу - задокументована сукупність процедур та механізмів, яка розроблена, складена і підтримується в готовності для використання в умовах інциденту для того, щоб організація могла продовжувати здійснювати свої критичні функції і послуги на прийнятному рівні [4-7].

Аварійне відновлення (Disaster Recovery, DR) - стратегії і плани для відновлення організації технологічної інфраструктури та можливостей підприємства після серйозної перерви. В даний час зазвичай використовується тільки по відношенню до організації відновлення в області IT і телекомунікацій [6].

Планування аварійного відновлення (Disaster Recovery Planning, DRP) - діяльність, пов'язана з забезпеченням доступності IT-інфраструктури та її відновлення після настання кризової ситуації [6,7].

В уявлені бізнесу, а часто і IT-спеціалістів, поняття УББ нерідко ототожнюється з відновленням після катастроф. Необхідно чітко розуміти, що основною метою УББ є підтримання в актуальному стані достатньої кількості структур, операцій і ресурсів (активів), необхідних для стабільного функціонування організації в КС. Зазначене розуміння УББ істотно відрізняється від поняття АВ, яке тісно, якщо не виключно, пов'язане з IT. Сьогодні фокус уваги УББ зміщується на організацію в цілому, на критично важливі для бізнесу процеси, розширюючи горизонти розгляду проблеми за межі виключно інформаційних систем, незважаючи на їх важливість для сучасних компаній [1].

Існує декілька підходів до виділення етапів захисту інформаційних ресурсів. Проаналізувавши роботи фахівців та стандарти в цій області була запропонована модель поділу на етапи процесу застосування методів та технологій ЗББ. Так, основними етапами життєвого циклу систем УББ за даною моделлю є:

1) планування безперервності бізнесу

2) реалізація (введення в дію, експлуатація, тестування) розробленого плану.

На першому етапі повинен бути проведений аналіз загроз, ризиків, визначені активи та критично важливі ресурси, розроблена документація та проведене навчання персоналу. На другому етапі проводиться введення превентивних заходів та встановлення засобів, що забезпечують процедуру відновлення роботи критичних IT-процесів і бізнесу взагалі.

Деякі дослідники даного питання, серед яких і розробники стандарту BS25999 [4,5], використовують чотирьох етапну модель УББ, яка зображена на рис. 1.

Рис. 1. Життєвий цикл систем ЗББ

Існує ще третій підхід, за яким виділяють наступні стадії: аналізу, проектування, тестування та підтримки [2].

Таким чином, на даний момент в науковій літературі не існує єдиного підходу визначення сутності УББ та його фундаментальних напрямків – планування ББ та планування аварійного відновлення, що є суттєвою проблемою. Шляхом її вирішення може бути детальна систематизація сутності УББ.

Висновки

В даній роботі визначені основні поняття та положення УББ. Являючись одною з найбільш динамічно розвиваючихся теорій менеджменту, управління безперервністю бізнесу є ще не повністю формалізованим та структурованим. На території СНГ концепція знаходиться все ще в зародковому стані. Тому існує велика кількість проблем головним чинном через недостатню формалізацію та відсутність єдинного підходу до процесів захисту інформаційних ресурсів при ЗББ.

У першій частині визначене одне з центральних понять УББ – «кризова ситуація». Оскільки головним завданням систем та методів ЗББ є нейтралізація впливу КС на БП та інформаційні системи, що підтримують їх функціювання, або попередження їх винекнення, то необхідним є детальний розгляд даного поняття, його природи, характеристик, видів та приведення його до чіткого упорядкованого виду. Результати аналізу підходів до визначення КС показали недостатній рівень формалізації та необхідність систематизації даного поняття, що буде зроблено в подальших роботах. Саме точна та охоплююча всі аспекти УББ класифікація КС є найбільш ефективним шляхом вирішення проблем захисту інформаційних ресурсів від КС.

У другій частині розглянуті фундаментальні поняття УББ – планування ББ і планування аварійного відновлення. Часто ці два терміни отожнюються, але такий підхід є помилковим, тому що це два різних напрямки в розвитку ББ. Так як планування ББ є більш загальним поняттям, то основну увагу в дослідженні приділено йому. В роботі визначено власне значення вищезазначених термінів, основні підходи виділення стадій життєвого циклу планування неперервності бізнесу. Аналіз наукових публікацій показав відсутність єдиної точки зору на це питання. Кожен з наведених методів висвітлює процес ЗББ з певної сторони, проте жоден не охоплює всіх аспектів систем УББ. Таким чином доцільно було б в подальшому працювати над цим питанням в наступних роботах з метою виділення єдиного підходу до визначення суті процесів УББ, їх класифікації та формалізації.

Список літератури

1. Петренко С.А., Беляев А.В. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться. – М.: ДМК Пресс, Компания АйТи, 2011. – 400 с.

2. Jan Van Bon. ИТ СЕРВИС–МЕНЕДЖМЕНТ. Вводный курс на основе ITIL. – Van Haren Publishing, по заказу ITSMF Netherlands, 2003. – 72 с.

3. Harris S. CISSP Certification All-in-One Exam Guide. – 5th edition. – McGraw-Hill Osborne Media, 2010. – 1216 p.

4. Business continuity management. Code of practice: BS25999-1:2006 – BSI British Standards, 2006 – 28 p.

5. Business continuity management. Specification: BS25999-2:2007 – BSI British Standards, 2007. – 38 p.

6. Singapore Standard for Business Continuity Management: SS540:2008 – SPRING Singapore, 2008. – 54 p.

7. Business continuity – Managinig disruption-related risk: AS/NZS 5050 – Standards Australia, 2010. – 53 p.