© Gizun A., Lozova I. Analysis of «crisis» definition and basic aspects of business continuing planning concept // Ukrainian Scientific Journal of Information Security, 2016, vol. 22, issue 1, p. 99-108.

АНАЛІЗ ДЕФІНІЦІЙ ПОНЯТТЯ КРИЗОВА СИТУАЦІЯ ТА ОСНОВНИХ АСПЕКТІВ КОНЦЕПЦІЇ УПРАВЛІННЯ БЕЗПЕРЕРВНІСТЮ БІЗНЕСУ

Андрій Гізун, Ірина Лозова

Національний авіаційний університет, Україна

ГІЗУН Андрій Іванович, к.т.н.

Рік та місце народження: 1987 рік, м. Нетішин, Хмельницька область, Україна.
Освіта: Національний авіаційний університет, 2010 рік.
Посада: доцент кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, управління інцидентами інформаційної безпеки, комплексні системи захисту інформації, штучні імунні системи, управління безперервністю бізнесу та правове забезпечення захисту інформації.
Публікації: більше 50 наукових публікацій, серед яких наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: andriy.gizun@gmail.com

ЛОЗОВА Ірина Леонідівна

Рік та місце народження: 1983 рік, м. Енгельс, Російська Федерація.
Освіта: Національний авіаційний університет, 2005 рік.
Посада: старший викладач кафедри безпеки інформаційних технологій.
Наукові інтереси: інформаційна безпека, криміналістичний аналіз комп'ютерних систем, криптографічний захист інформації, бази даних, управління безперервністю бізнесу.
Публікації: наукові статті, матеріали і тези доповідей на конференціях, авторські свідоцтва.
E-mail: kira1983@yandex.ru

Анотація. *Концепція управління безперервністю бізнесу як перспективний напрям оперативного та стратегічного менеджменту визначає важливість захисту інформаційних ресурсів в умовах впливу кризових ситуацій. Таким чином, основним елементом даної концепції є поняття «кризова ситуація», яке не має чіткого визначення і змінюється в залежності від галузі науки і техніки. У цій статті проведений аналіз відомих дефініцій поняття «кризова ситуація», зокрема в галузях економіки, політики, медицини, психіатрії, менеджменту та інших сфер, на основі чого сформовано визначення в рамках концепції управління безперервністю бізнесу. Також розглянуто основні підходи до періодизації процесу управління кризами, підходи до класифікації кризових ситуацій, висвітлених в стандартах, практиках та нормативних документах управління безперервністю бізнесу і роботах провідних науковців в даному напрямі. Крім того, обґрунтовано віднесення систем управління кризовими ситуаціями до окремого класу в структурі системи менеджменту інформаційної безпеки та визначені їх функціональні взаємозв'язки з іншими захисними системами, такими як системи виявлення та попередження вторгнень, системи аналізу та оцінки ризиків, системи антивірусного захисту, системи управління інцидентами інформаційної безпеки.*

Ключові слова: *кризова ситуація, дефініція, управління, система, менеджмент інформаційної безпеки, класифікація кризових ситуацій, концепція управління безперервністю бізнесу, етапи процесу кризового управління.*

Вступ

З розвитком можливостей інформаційних технологій (ІТ) у сучасному світі пріоритетним напрямом є автоматизація управлінських, технологічних, виробничих та інших процесів. Інформаційні системи (ІС) займають провідну роль в системі функціонування бізнесу та держави, причому взаємозв'язок ІТ та бізнес-процесів (БП) стає настільки тісним, що життєздатність підприємств повністю залежить від надійності технологій, що забезпечують підтримку найбільш важливих критичних БП підприємства, організації, установи. Проблема реагування на кризові ситуації (КС) в сфері ІТ є надзвичайно важливою та ще не достатньо вивченою. Адже серйозно нею розпочали займатися лише з кінця 80-х років минулого сторіччя, причому на території країн СНД початок даних досліджень припав на середину першого десятиліття теперішнього сторіччя. З розвитком ІТ та їх можливостей невпинно зростає роль систем

реагування на кризові явища в процесі управління та підтримки життєздатності підприємств, установ та організацій усіх форм власності. Недаремно концепція управління безперервністю бізнесу (КУББ) в останні роки є одним із напрямків оперативного та стратегічного менеджменту, які найбільш динамічно розвиваються.

Дослідження 114 компаній з списку 1000 найбільших корпорацій показало, що в середньому вони стикаються з кризовими ситуаціями 10 разів на рік [1]. Так, 10-15 років тому провідні світові компанії, в першу чергу фінансовий сектор ринку, усвідомили ступінь залежності бізнесу від ІТ. Великі корпорації почали цілеспрямовано впроваджувати технології забезпечення безперервності бізнесу (ЗББ) в непередбачених ситуаціях [2,3,4]. Важливість даної проблеми підтверджена і статистикою появи КС різного характеру в теперішній період розвитку людства. Так, наведені в [5] статистичні дані, чітко показують, що кількість гідрометеорологічних кризових ситуацій на 2000 рік в порівнянні з 1950 зросла майже в 25 разів, геологічних – в 8 разів, а біологічних – близько в 50. За даними [6], у 2010 році кількість зареєстрованих лих наближається до середнього значення протягом 2000-2009 років (387). Число жертв зросло з 198 700 000 у 2009 році до 217,3 млн. чол. у 2010 році, але залишилася нижче середньорічного числа жертв 227 500 000 протягом 2000-2009 років. Економічні збитки від стихійних лих в 2010 році більш ніж в 2,5 рази вищі, ніж в 2009 (47,6 млрд. $ США) і зросли на 25,3% у порівнянні з середньорічним показником (98,9 млрд. $ США).

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 своїй діяльності технології управління КС [3]. При цьому все більш актуальним стає забезпечення захисту від не катастрофічних, а більш ймовірних, над-звичайних ситуацій.

Однак, залишається досить багато проблем в КУББ. Зокрема, слід відзначити наявність багатьох різних трактувань основних моментів КУББ та недостатній рівень реалізації технічних систем управління КС (СУКС), у першу чергу, в інформаційній сфері. Тому основною метою даної статті є аналіз основних дефініцій поняття «кризова ситуація», виділення ключових аспектів КУББ та визначення місця і ролі систем управління КС в системі менеджменту інформаційної безпеки (СМІБ).

Основна частина дослідження

Здійснивши аналіз відомих джерел у галузі забезпечення ББ, визначимо основні поняття та терміни, що використовуються в області КУББ. Оскільки вона спрямована на захист активів та ресурсів підприємства чи організації від впливу КС, то необхідно дати визначення терміну «кризова ситуація». На жаль, загальноприйнятого тлумачення цього терміну немає. Розглянемо найбільш вживані варіанти терміну «кризова ситуація» та суміжні з ним поняття і сформуємо коректне та відповідне темі роботи визначення КС.

Поняття «криза» має багато рівнів і трактувань. Вираз «криза» походить від грецького слова «crisis», яке означає «вирок, рішення по якомусь питанню, чи в сумнівній ситуації» [7]. Спочатку дане поняття використовувалось в медицині, а з XVII-XVIII сторіччя – стосовно процесів, що відбуваються в суспільстві, як-то військові, політичні кризи. При цьому використовувалося майже незмінене значення кризи, взяте з медицини. З XIX сторіччя з'являються тлумачення криз в економічній сфері. Класичне економічне поняття кризи, що сформувалося в той час, означає небажану і драматичну фазу в капіталістичній економічній системі, що характеризується коливаннями і негативними явищами, перешкодами. У цьому розумінні поняття кризи довгий час займало особливе місце в схемі теорій кон'юнктур у розвитку економіки. Так, циклічна схема Shpithoff'a містить стадії: спад – перший підйом – другий підйом – пік – брак капіталу – криза [8,9].

В медицині, особливо в психіатрії, КС стали основою напряму терапевтичних досліджень, названих кризовим втручанням. Виникнення теорії кризових втручань зазвичай пов'язують з дослідженням Lindemann'ом реакції пацієнтів на горе [10], в якому він визначив симптоматику криз в 101 пацієнта, які нещодавно втратили близьких. Подальший розвиток теорії і практики кризових інтервенцій в психіатрії здійснили Poal [11], Caplan і його колеги з Гарварда. Caplan запропоновував визначення кризи [12, 13]. Він вважає, що кризи з'являються тоді, коли людина опиняється перед проблемою, яка немає рішення і така ситуація не може бути подолана з використанням звичайних методів вирішення проблем. Кризова теорія Caplan'a заснована на понятті гомеостазу, а кризою вважається порушення гомеостатичного балансу. Проте, на думку Taplinj [14], поняття гомеостазу не відділяє адаптивну і неадаптивну нестійкість, не може ефективно характеризувати важливі аспекти людської поведінки: ріст, розвиток, зміни та актуалізацію.

Відоме визначення в авіаційній галузі: КС – ситуація, яка склалася внаслідок вчинення протиправних і навмисних дій, пов'язаних з посяганням на нормальну, регулярну і безпечну діяльність цивільної авіації, що спричинили нещасні випадки з людьми, майнові збитки, акти незаконного втручання в діяльність цивільної авіації або які створили реальну загрозу настанню таких наслідків [15]. У фінансово-страховому секторі КС – це ситуація, яка може мати місце в майбутньому через вплив зовнішніх та/або внутрішніх чинників і яка призводить до суттєвих фінансових втрат страховика [16]. У галузі ядерної безпеки під терміном КС розуміють ситуацію, що склалася або може скластися внаслідок вчинення або загрози вчинення диверсії, крадіжки чи будь-якого іншого незаконного вилучення ядерних матеріалів [17].

У даний час розроблено декілька підходів до визначення поняття КС. Так, деякі автори визначають кризу як порушення, зміну в гіршу сторону одного або декількох параметрів, характеристик будь-якої системи – людини, групи людей, організації, економіки, екології, суспільства в цілому. Інші сучасні автори характеризують кризу як такий стан організації, при якому вона не здатна жити далі, не зазнаючи деяких внутрішніх змін [18]. Відоме ще визначення, наведене в [19], за яким криза – це крайнє загострення внутрішньовиробничих і соціально-економічних відносин, а також відносин організації із зовнішньоекономічним середовищем. Деякі автори визначають кризу через опис її характеристик. Наприклад, Горєлов вказує, що «… виникнення КС супроводжується: наявністю загроз для реалізації найбільш важливих цілей організації; дефіцитом часу для прийняття рішення по врегулюванню кризи; тиском на осіб, котрі приймають рішення» [20].

З точки зору кризового управління (менеджменту), криза – це припинення нормального процесу, непередбачена подія, що ставить під загрозу стабільність підприємства, раптова серйозна подія, яка має потенціал пошкодити або навіть зруйнувати репутацію компанії. Під позаштатними або надзвичайними ситуаціями розуміються зовнішні впливи, що призводять до унеможливлення функціонування підприємства в звичайному режимі. Окрім прямих втрат, організації несуть витрати, пов'язані з порушенням процедур виробничого та фінансового обліку, втратою розташування замовників, погіршенням іміджу і зниженням конкурентоспроможності [7,21].

Крім того, в даній галузі відомі спроби надати визначення КС багатьма авторами, проте вони не дали загальноприйнятого поняття. Деякі визначення сконцентровані на їх впливі на організації. Наприклад, Coombs в [22] визначив кризу як ситуацію, яка викликає небажані або негативні наслідки для організації. Lerbinger [23] розглядає кризу як випадок, який приносить шкоду репутації компанії, становить небезпеку для її дохідності, зростання і, можливо, існування організації. Miller під кризою розуміє випадок, що вимагає швидкої реакції, створює невпевненість і напругу, загрожує репутації, активам, постійно зростає в аспекті інтенсивності і вимагає змін організації [24]. Інші дослідники вказують на те, що КС впливає не лише на організацію, але й на систему в цілому. Fearn-Banks в [25] визначає кризу як явище з потенційно негативними наслідками, що охоплюють організацію, компанію, промисловість, а також суспільство, продукцію, послуги або ім’я (репутацію, марку), в той же час Pauchant і Mitroff в [26] вважали, що криза – це деструктивний чинник, який фізично впливає на систему в цілому і вимагає прийняття відповідальності на себе, загрожує суб’єктивному екзистенціальному ядру організації. Деякі дослідники на перший план ставлять такі характеристики КС, як непередбачуваність, двозначність тощо. Наприклад, Pearson и Clair [27] під кризою розуміють малоймовірний випадок з високим рівнем впливу, що загрожує життєздатності організації і характеризується двозначністю ситуації, ефектів і засобів вирішення, а також необхідністю швидкого прийняття рішень.

Один із провідних фахівців в галузі управління кризами Regester визначає [28] кризу як подію, з вини якої компанія потрапляє в центр «не завжди доброзичливої» уваги засобів масової інформації та інших зовнішніх цільових аудиторій, в тому числі акціонерів, профспілкових організацій, рухів на захист навколишнього середовища, які з тієї чи іншої причини цілком законно цікавляться діями організації.

Виникнення КС зазвичай спричинене певними інцидентами. 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 [29,30]. Надзвичайна ситуація (лихо, катастрофа) – це подія, яка має негативний вплив на функціонування сервісу або системи, вимагає значних зусиль для відновлення початкового рівня продуктивності. Тобто, надзвичайна ситуація набагато серйозніша, ніж інцидент. Надзвичайна ситуація – це стан на певній території або акваторії, що склалася в результаті аварії, небезпечного природного явища, катастрофи, стихійного чи іншого лиха, які можуть призвести до людських жертв, нанести шкоду здоров'ю людей або навколишньому середовищу, значні матеріальні втрати. В КУББ, зокрема, в міжнародних стандартах в даній галузі та найбільш відомих практиках це питання розглядають в такому контексті: криза – ненормальна ситуація, яка загрожує операціям, персоналу, клієнтам і репутації підприємства [31]; надзвичайна ситуація – загальний термін з різними інтерпретаціями в залежності від регіону. У США він означає широкомасштабну катастрофу, що вимагає федеральної підтримки і запуску фінансування Федеральної агенції управління надзвичайними ситуаціями [32]. В інших країнах вважається еквівалентним за змістом серйозним інцидентам [29-31]; громадянська надзвичайна ситуація – подія або ситуація, яка може нанести серйозних збитків людському добробуту, навколишньому середовищу в будь-якому місці чи порушити безпеку цього місця [30]; катастрофа – фізична подія, що перериває бізнес-процеси достатньо, щоб загрожувати життєздатності організації [29,31].

Відповідно до законодавства України, надзвичайна ситуація – порушення нормальних умов життя і діяльності людей на об'єкті або території, спричинене аварією, катастрофою, стихійним лихом або іншими чинниками, що призвели (можуть призвести) до загибелі людей, тварин і рослин, значних матеріальних збитків та (або) завдати шкоди довкіллю, а небезпека у надзвичайних ситуаціях – стан, за якого існує наявна або ймовірна загроза виникнення вражаючих чинників і їх впливу (дії) на населення, об'єкти економіки та довкілля [33].

Усі вищезгадані явища та процеси, хоча і мають різний характер та природу, застосовуються в різних галузях суспільного життя, негативно впливають на життєдіяльність людей, функціонування бізнес-процесів і бізнесу в цілому, держави, знижують ефективність управління ресурсами. Для уникнення проблем та непорозумінь дамо єдиний загальний термін для його визначення, що будемо використовувати у дослідженні. КС в аспекті безперервності бізнесу – це певна ситуація чи подія, що має місце на деякій території (в фізичному чи організаційному сенсі), потенційно здатна нанести серйозних збитків, призвести до порушення діяльності, загибелі чи поранення персоналу організації та інших категорій населення, втрати послуг або функцій підприємства в достатньому об'ємі, щоб загрожувати життєздатності організації [2].

Кризові ситуаційні центри як основа систем управління великими (корпоративними) структурами під час КС на сучасному етапі розвитку ІТ знаходять все більше і більше поширення. Невід'ємною частиною кризових ситуаційних центрів є автоматизовані системи підтримки прийняття рішень і, зокрема, елементи штучного інтелекту – бази знань. В основі їх формування знаходиться модель знань в предметній області, для якої створюється інформаційна система. Для кризових ситуаційних центрів – це знання про ситуації, що вимагають оперативного прийняття рішення. Не останнє місце серед таких даних займає класифікація КС. Так, згідно із законодавством України, КС залежно від джерела небезпеки може бути: природна, техногенна, соціально-політична, воєнна; залежно від масштабу: загальнодержавна, регіональна, місцева й об'єктова [33,34].

У літературі зустрічається досить багато моделей окремих вузькоспеціалізованих видів надзвичайних ситуацій, однак, відсутня універсальна модель, що дозволяє описати широкий клас КС. Тож необхідним є виділення базових характеристик, формування універсальної, достатньо повної моделі їх класифікації.

Огляд відомих класифікацій був здійснений в [35,36]. З метою вдосконалення процесів антикризового управління багатьма вченими були зроблені спроби класифікувати КС. [23,37-40]. Наприклад, Mitroff і Killman [40] ідентифікували сім типів КС в менеджменті організацій: фальсифікація продукту, дефект продукції, піратство, хибне звинувачення, обмежене мислення, містифікації та культурна не чуттєвість. Meyers [39] виділив дев'ять типів ділових криз, а саме: зміни суспільних настроїв, різкі зміни ринку, дефекти продукції, наслідуваність (спадкоємність) менеджменту, фінансові втрати, відносини між керівництвом і персоналом, корпоративні поглинання бізнесу, негативні міжнародні події, а також впливи, що пов'язані з регулюванням або відмовами державного контролю промисловості. Lerbinger [23] пропонував чотири класи криз, названі технологічними кризами, конфронтаційними кризами, кризами недоброзичливості і кризами організаторської відмови.

Проте, одна з найбільш цікавих і корисних типологій КС була запропонована Coombs в [37], а згодом вдосконалена в роботі Coombs і Holladay [38]. Ці типології базуються на основі рівня розуміння організацією самої КС і розуміння нею відповідальності [41]. В Coombs [37] КС класифіковані по дев'яти основних категоріях, до яких віднесені стихійні лиха, недоброзичливість, технічні збої, саботаж, виклики, катастрофічні пошкодження, організаційні злочини, насилля на робочому місці і чутки. Використовуючи поняття організаційної відповідальності, вони були об'єднані в п'ять груп: чутки, природні КС, недоброзичливість, нещасні випадки і злочини [42]. В типології [38] автори запропонували дещо змінену класифікацію і набір з 10 стратегій реагування на КС. Так, було виділено 13 кризових типів, що розприділено в 3 групи: КС, в яких організація відчуває себе жертвою; випадкові КС, що виникають внаслідок ненавмисних дій; КС, які можна уникнути, пов'язані в основному з цілеспрямованим впливом та людським чинником. Крім того, в класифікаціях КС виділяють інші показники і ознаки для класифікації.

Відповідно до причин походження подій, що можуть зумовити виникнення КС (джерел) Державний класифікатор надзвичайних ситуацій виділяє 4 типи КС: техногенного характеру; природного характеру; соціально-політичного характеру, пов'язані з протиправними діями терористичного і антиконституційного спрямування; воєнного характеру, пов'язані з наслідками застосування звичайної зброї або зброї масового ураження [34]. На Заході виділяють п'ять основних типів КС: підприємницькі, соціальні, техногенні, природні та природно-техногенні [5].

Розглянемо також інші характеристики, які використовуються в різних джерелах для класифікації КС. За можливістю прогнозування кризи можуть бути передбаченими (закономірними) і несподіваними (випадковими). Різновидом передбачених криз є циклічна криза [8,19,20,44]. За ступенем прояву дослідники виділяють кризи явні і латентні (приховані). Перші протікають помітно і легко виявляються. Інші є прихованими, протікають відносно непомітно і тому найбільш небезпечні [8,44]. За глибиною вияву кризових явищ кризи бувають деструктивними, глибокими і легкими. Деструктивні КС часто ведуть до руйнування різних структур соціально-економічної системи. Глибокі КС не ведуть до руйнування різних структур соціально-економічної системи, а лише до їх суттєвих змін. Легкі кризи протікають більш послідовно і безболісно, ними легко управляти. Дана характеристика притаманна в основному для економічних КС, тому в досліджені носить другорядне значення [20,44]. За характером виникнення кризи бувають такими, що виникають за рахунок впливу суб'єктивних, тобто залежних від волі, переконань, помилок певних суб'єктів-учасників відносин, в яких виникла криза, та об'єктивних причин, незалежних від дій та бажань

оточуючих [8,44]. За масштабом прояву КС слід розглядати з двох позицій: в географічному та в організаційно-підприємницькому аспекті. Так, за даною характеристикою в географічному аспекті КС можуть бути локальними, регіональними, державними та глобальними. А в іншому аспекті доцільно виділити наступні види: КС в межах окремого бізнес-процесу, підприємства, на рівні групи підприємств [19,44]. Яскравим прикладом може служити порушення нормального функціонування електронної пошти. При відмові поштового клієнта певного відділу, скажімо бухгалтерії – це КС в межах окремого бізнес-процесу, а у випадку відмови поштового сервера провайдера та в залежності від масштабів надання послуг провайдерами, КС переходить на рівень підприємства чи групи підприємств. За часом дії негативних чинників можна виділити довго-, середньо-, короткотривалі та миттєві надзвичайні події. Стосовно відображення даної характеристики в числовому значенні існує велика кількість підходів, кожен з яких має свої особливості. Ще більше проблема ускладнюється невизначеністю стосовно того, чи дія наслідків КС входить в час дії самої кризи, чи обраховуються окремо. Так, КС можуть діяти в найрізноманітніших часових інтервалах – від долі секунди (удар блискавки, перепад в мережі електроживлення) до років (війни, кліматичні зміни). За потенційною загрозою людському життю та здоров'ю виділяють два види КС: що несуть потенційну загрозу і що не несуть. Ті КС, які потенційно можуть нести загрозу людині класифікуються ще за двома характеристиками: за кількістю загиблих та постраждалих осіб, не залежно від категорії. Відносно кількості загиблих можна виділити три категорії КС: катастрофи (понад 500 осіб), КС з великою (понад 100 осіб) та невеликою кількістю жертв. Інколи дану характеристику оцінюють не за абсолютним показником загиблих, а за відношенням їх на 100 000 населення [34,44,45]. Проте однозначної точки зору на числові значення даної шкали немає. Подібна ситуація із шкалою кількості постраждалих. У ній прийнято виділяти аналогічні категорії КС як і з кількістю загиблих. Тому, надалі пропонується використовувати лише характеристику кількості жертв, що охоплює в собі загиблих та постраждалих осіб від КС і виділяти наступні категорії: катастрофічні, з великою та невеликою кількістю жертв. Нищівні, з великими, помірними та невеликими збитками, практично невідчутні – основні класи КС, що можна виділити за рівнем завданих економіці збитків. Оцінка кризової ситуації у даному випадку здійснюється за абсолютним показником суми витрачених на ліквідацію її наслідків грошей або за часткою цієї суми в ВВП країни [5,6,44]. В результаті нищівних КС все господарство на території ураження зазвичай зруйноване, і витрати на їх ліквідацію складають порядку 10% ВВП. Натомість невідчутні КС не несуть ніяких руйнацій і витрат на їх ліквідацію.

Визначивши і розглянувши поняття «кризова ситуація», що є одним з центральних об'єктів КУББ, перейдемо до розгляду його фундаментальних основ – процесів стратегічного менеджменту. Багато науковців розглядають кризове управління як довготривалий процес і пропонують різні моделі його стадій. Всі вони охоплюють часовий проміжок від підготовки перед кризою і до відновлення після неї. Ці моделі представляють різні підходи і відрізняються кількістю етапів. Кризове управління розділяють на три [46-48], чотири [49,50], п'ять [51,52], шість [53] і навіть вісім стадій [54]. Основні етапи названих моделей представлені у вигляді табл. 1.

Зокрема, Міністерство внутрішніх справ Великобританії запропонувало виділити вісім етапів, а саме: керівництво, збір інформації, написання планів, консультація, публікація, учбова ратифікація, підтвердження/перегляд (Harrison [54]).

Основні етапи моделей процесу кризового управління Таблиця 1

Загальні стадії	Smith	Richardson	Coombs	Myers	Jaques	Pearson і Mitroff	Fink	Augustine
Перед кризами	Криза управління	Передкризова стадія	Передкризова стадія	Нормальні операції	Підготовка до кризи	Виявлення сигналу	Кризове зниження	Запобігання криз
						Підготовка	Планування	Підготовка
Під час криз	Експлуатаційна криза	Кризовий вплив / спасіння	Кризова стадія	Надзвичайна відповідь	Запобігання криз	Стримання	Попередження	Визнання кризи
							Відповідь	Стримання
				Тимчасова обробка	Кризове управління інцидентами			
Після криз	Криза легітимізації	Відновлення / спаду	Посткризова стадія	Відновлення	Посткризове управління	Відновлення	Реагування	Вирішення
						Вивчення		Оцінка

Слід зазначити, що трьохетапна модель є найбільш відомою і на ній базуються інші моделі, що утворені шляхом деталізації визначених трьох етапів. Деякі дослідники даного питання, серед яких і розробники міжнародного стандарту BS25999 [55,56], використовують чотирьохетапну модель УББ, яка зображена на рис. 1а. На рис. 1б представлений відповідний стандарту цикл розробки систем забезпечення ББ. Існує ще підхід, за яким виділяють такі стадії: аналізу, проектування, тестування та підтримки [3].

Проаналізувавши роботи фахівців та стандарти в цій області, було запропоновано модель поділу на етапи процесу застосування методів та технологій ЗББ [2]. Так, основними етапами життєвого циклу систем УББ (систем управління КС) 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 загалом [2].

Хоча немає чіткого алгоритму створення плану BCP (Business Continuity Plan – план забезпечення ББ), час від часу з'являються різні практики його проведення. Зокрема, NIST (National Institute of Standards and Technology – Національний інститут стандартів і технологій США) відповідає за розробку кращих практик та забезпечення загального доступу до них. NIST передбачив такі кроки в документі SP 800-34 «Керівництво з планування безперервності для IT-систем» [57]:

1) Розробити політику планування безперервності бізнесу (continuity planning policy statement). Написати політику, яка міститиме необхідні керівні принципи для розробки плану BCP і визначить необхідних уповноважених осіб для виконання покладених на них завдань, в тому числі і осіб, що приймають рішення.

2) Провести аналіз впливу на бізнес (BIA – business impact analysis). Ідентифікувати критичні функції і системи, категоризувати (пріоритезувати) їх на основі ступеня їх критичності. Виявити уразливості, розрахувати ризики.

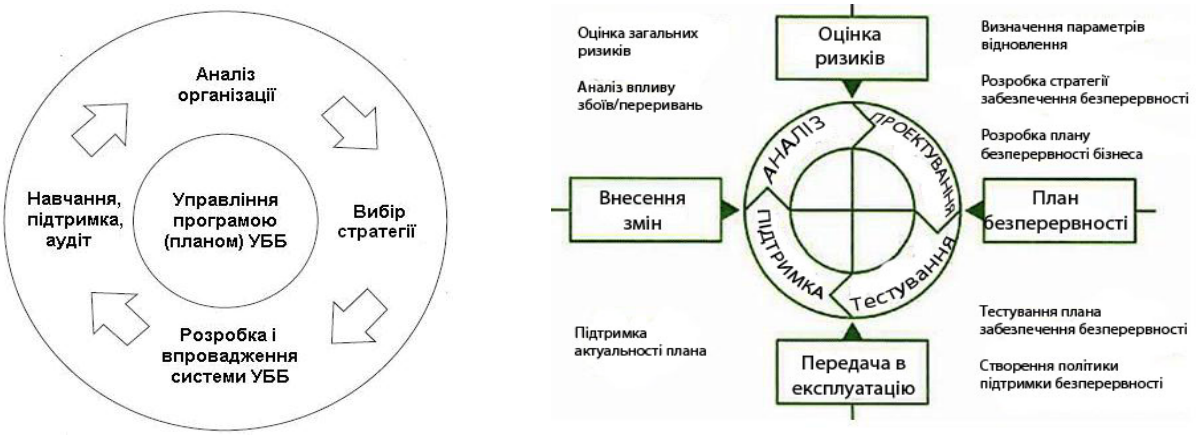
3) Визначити превентивні захисні заходи. Після виявлення загроз, вибрати і впровадити захисні заходи і контролі для зниження рівня ризиків компанії економічно доцільним способом.

4) Розробити стратегії відновлення (recovery strategy). Описати методи, що забезпечують оперативне відновлення працездатності критичних систем, функцій.

5) Розробити план дій на випадок надзвичайних ситуацій (contingency plan). Описати процедури, розробити керівництва, які забезпечать продовження функціонування компанії в аварійному стані.

6) Протестувати план, провести тренінги і навчання. Перевірити план для виявлення недоліків у ньому, провести тренінги та навчання для належної підготовки людей на випадок КС.

7) Підтримувати актуальність плану.



а) б)

Рис. 1. Життєвий цикл концепції управління безперервністю бізнесу (а) та розробки систем забезпечення безперервності бізнесу (б)

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.

В роботі [58] запропонований прототип системи виявлення КС і ліквідації їх наслідків, заснований на застосуванні методів нечіткої логіки, її базова архітектура, а в [59,60] описані відповідні методи, на яких вона реалізується. Крім того, відомі роботи щодо розробки і створення подібних методів [61] та систем [62] для виявлення порушника інформаційної безпеки в комп'ютерних системах та мережах. Тому, для ефективного забезпечення стану інформаційної безпеки та безперервності бізнесу необхідною вбачається розробка системи виявлення інцидентів/потенційних кризових ситуацій (СВІПКС) та системи оцінки критичності ситуації, спричиненої виявленим інцидентом (СОКС). Покажемо місце і роль цих систем в менеджменті інформаційної безпеки.

Серія міжнародних стандартів ISO 27k регламентує і визначає основні процеси управління інформаційною безпекою, в тому числі охоплює питання управління ризиками, інформаційними ресурсами, комунікаціями, інцидентами інформаційної безпеки тощо. Згідно із стандартами, створення систем менеджменту інформаційної безпеки (СМІБ) здійснюється в чотири етапи: планування та створення ІС; впровадження та використання; моніторинг та аудит; підтримка та вдосконалення ІС, що повністю відповідають циклу Шухарта-Демінга (цикл PDCA). Таким чином, захист інформації реалізується завдяки використанню сукупності різноманітних систем проектування, моніторингу, аудиту, керування інформаційною

безпекою і іншими сферами обслуговування та управління ІС. Серед таких систем доцільно виділити системи антивірусного захисту (САЗ), системи виявлення/попередження вторгнень (IDS/IPS), системи аналізу та оцінки ризиків (САОР), системи управління інцидентами інформаційної безпеки (СУІІБ, що включають в себе програмне та апаратне забезпечення для команд реагування на комп'ютерні інциденти (CERT) щодо фіксації, ідентифікації, обробки, реагування, ліквідації інцидентів, збирання статистичних даних тощо). Визначені системні засоби функціонують на кожному з етапів циклу PDCA і інтегруються в системах менеджменту (управління) інформаційної безпеки (СМІБ).

Отже, виходячи з функціоналу і взаємодії між собою зазначених захисних систем, проектовані СВІПКС та СОКС разом з САЗ і IDS/IPS утворюють особливий клас СМІБ – СУКС. Серед основних функцій СУКС слід виділити виявлення, ідентифікацію КС, проведення їх оцінки, забезпечення прийняття рішень в умовах КС та автоматизацію цього процесу, підбір засобів реагування, ліквідація КС і т.п. Сьогодні в світі даний клас реалізований у вигляді вузько-спеціалізованих засобів, які в основному не застосовуються в сфері інформаційної безпеки, а також не можуть бути використані в умовах нечіткості. Детальний аналіз відомих СУКС наведено в [63]. Місце СУКС в менеджменті інформаційної безпеки та взаємозв'язки даного класу систем з іншими системами захисту інформації представлено на рис. 2.

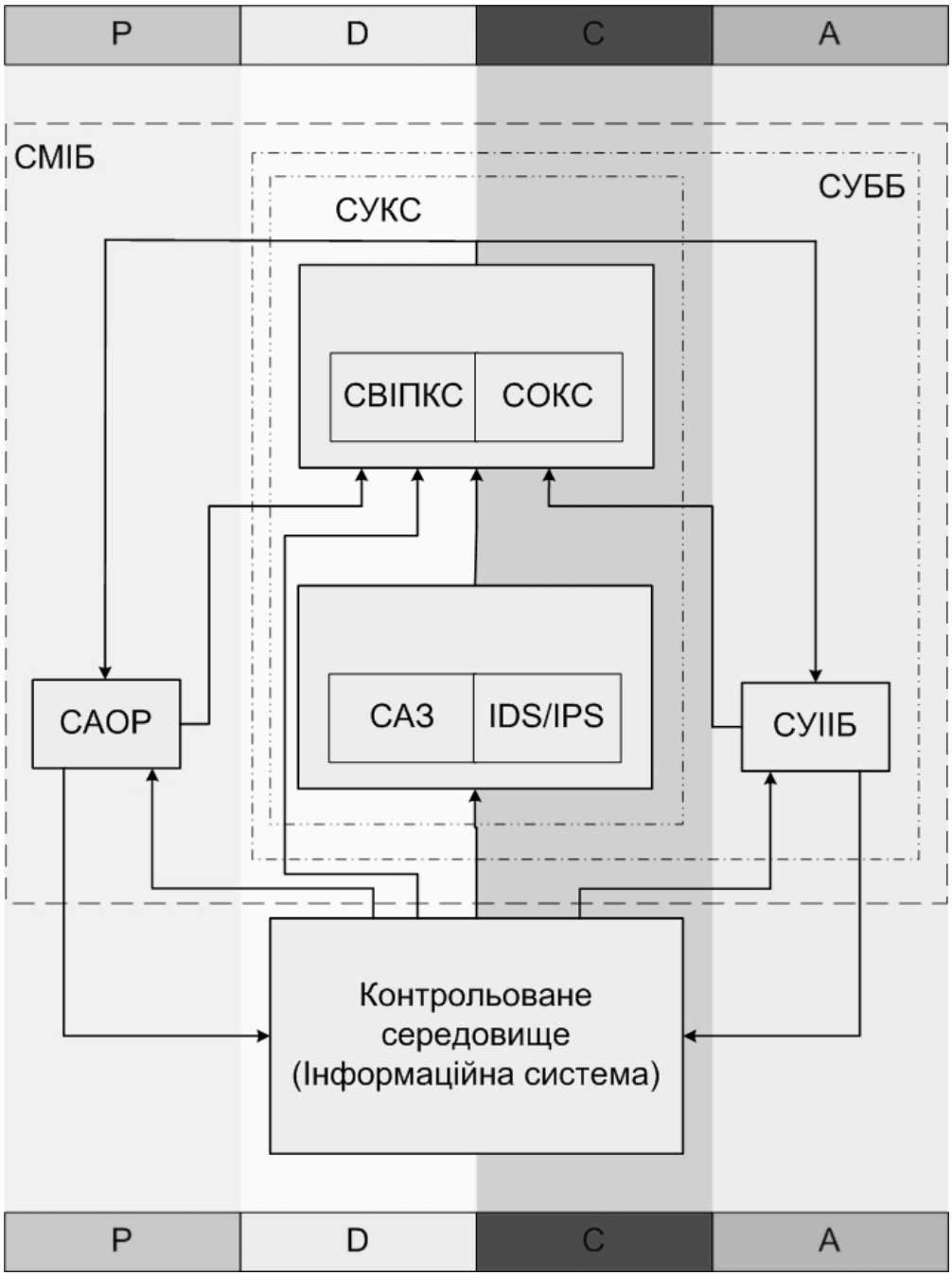


Рис. 2. Взаємозв'язки СУКС з компонентами СМІБ

Як видно з рисунку, САОР переважно використовуються на етапі планування і створення ІС, СА3 та IDS/IPS переважно взаємодіють з ІС, що захищається, на стадіях впровадження та моніторингу, а СУІБ – на етапі підтримки та вдосконалення. Слід зазначити, що СВІПКС і СОКС на етапах впровадження та моніторингу взаємодіють з ІС безпосередньо або через СА3 та IDS/IPS і є основою класу СУКС. В поєднанні з СУІБ СУКС утворюють клас систем управління безперервності бізнесу (СУББ), який разом з САОР формують загальний клас СМІБ. Розроблені системи СВІПКС та СОКС в якості вхідних даних використовують параметри, зняті давачами в контрольованому середовищі (тобто ІС), а також інформацію з САОР, СА3, IDS/IPS, СУІБ і, крім того, мають зворотний зв'язок з САОР та СУІБ, що забезпечує можливість корегування їх роботи, оновлення даних та формування статистики. Таким чином, запропоновані системні засоби є невід'ємною складовою СМІБ і разом утворюють окремий клас СУКС, що може функціонувати для вирішення задач захисту інформації в поєднанні з відомими захисними системами, розширюючи їх функціональні можливості, або автономно замінюючи більшість з них.

Висновки

Проаналізовано базові поняття КУББ, зокрема, поняття кризової ситуації, розглянуті існуючи підходи до класифікації КС. Проведений аналіз показав, що в різних трактуваннях даний термін завжди включає такі характеристики як збитки, загрози функціонування, наявність жертв, непередбачуваність та раптовість. Крім того, на сьогодні відсутня універсальна класифікація КС, що відображала б усі аспекти пов'язані з безперервністю бізнесу (роботи ІС) та необхідні для формування інтегрованої моделі представлення ІПКС, розробки методів та засобів управління КС.

Визначено місце та взаємозв'язки СУКС з компонентами СМІБ, а саме окреслено їх виділення в окремий клас захисних систем і встановлено особливості взаємодії з іншими системами захисту інформації.

Література

[1] Mitroff I.I. Can Your Company Handle a Crisis / I.I. Mitroff, T. Pauchant, P. Shrivastava // *Business and Health* . – 1989. – №. 7. – P. 41-44.

[2] Гізун А.І. Сучасні підходи до захисту інформаційних ресурсів для забезпечення безперервності бізнесу / А.І. Гізун, В.О. Гнатюк, О.П. Дуксенко, А.О. Корченко // Матеріали X Міжнародної науково–технічної конференції «АВІА–2011». – К.: НАУ, 2011. – Т1 – С. 2.5-2.9.

[3] Петренко С.А. Управление непрерывностью бизнеса. Ваш бизнес будет продолжаться / С.А. Петренко, А.В. Беляєв – М.: ДМК–Пресс, Компания АйТи, 2011. – 400 с.

[4] Harris S. CISSP Certification All–in–One Exam Guide / S. Harris. – McGraw–Hill Osborne Media, 2010. – 5th edition. – 1216 p.

[5] EM–DAT: The OFDA/CRED International Disaster Database [Електронний ресурс] / UCL – Brussels, Belgium. – Mode of Acces: World Wide Web. – URL: http: //www.em–dat.net.

[6] Guha–Sapir D. Annual Disaster Statistical Review 2010 [Електронний ресурс] / Debby Guha–Sapir, Femke Vos, Regina Below, Sylvain Ponserre // Centre for Research on the Epidemiology of Disasters (CRED). – Mode of Acces: World Wide Web. – URL: http://www.cred.be/sites/default/files/ADSR_2010.pdf.

[7] Рубан В.М. Теоретичні аспекти кризи та антикризового управління / В.М. Рубан // Вісник ОНУ імені І.І. Мечникова. – 2014. – Т. 19. – Вип. 2/2. – С. 154–157.

[8] Антикризисное управление: [учеб. для вузов по экон. спец.] / [Э.М. Коротков, А.А. Беляев, Д.В. Валовой и др.]; Под ред. Э.М. Короткова. – М.: Инфра-М, 2002. – 431 С.

[9] Самуэльсон П.А. Економіка / П.А. Самуэльсон, В.Д Нордхаус. – М.: Вильямс, 2014. – 1360 с.

[10] Lindemanne E. Symptomatology and management of acute grief / Erich Lindemanne // American Journal of Psychiatry/ – 1944. – pp. 141 -148.

[11] Poal P. Introduction to the theory and practice of crisis intervention / Pilar Poal // Quaderns de Psicologia. – 1990. – 10. – P. 121-140.

[12] Caplan G. Principles of Preventive Psychiatry / G. Caplan. – New York: Basic Books, Inc., 1964. – 320 p.

[13] Caplan G. Support Systems and Community Mental Health: Lectures on concept development / G. Caplan. – New York: Behavioral Publications, 1974. – 267 p.

[14] Taplinj R. Crisis Theory: critique and reformulation / R. Taplinj // Community Mental Health Journal. – 1971. – 7 (l), – P. 13-23.

[15] Про Державну програму авіаційної безпеки цивільної авіації: закон України № 545–IV / Верховна Рада України // Відомості Верховної Ради України – 25.04.2003р. – № 17. – С. 140.

[16] Про затвердження Методичних рекомендацій щодо загальних підходів до застосування страховиками стрес–тестів : Розпорядження №6496 від 05.12.2006 / Державна комісія з регулювання ринків фінансових послуг України. – Режим доступу: World Wide Web. – URL: http://uazakon.com/documents/date_8u/pg_grwksy.htm.

[17] Про затвердження Загальних вимог до систем фізичного захисту ядерних установок та ядерних матеріалів і Загальних вимог до систем фізичного захисту ядерних матеріалів при їх перевезенні : Наказ № 156 від 28.08.2008 / Держатомрегулювання України // Офіційний вісник України – 03.11.2008. – № 81. – С. 164. – ст. 2753.

[18] Колісник М.К. Фінансова санкція і антикризове управління підприємством [текст] / М.К. Колісник, П.Г. Ільчук, П.І. Відлий – К.: Кондор, 2007. – 272 с.

[19] Жарковская Е. П. Антикризисное управление: учебник / Е. П. Жарковская,

Б. Е. Бродский, И.Б. Бродский. – 7–е изд., испр. и доп. – М. : Омега-Л, 2011. – 467 с.

[20] Антикризисное управление человеческими ресурсами / под ред. Н.А. Горелова. – СПб.: Питер, 2010. – 429 с.

[21] Killmeyer Jan. Information Security Architecture: An Integrated Approach to Security in the Organization / Jan Killmeyer. – Second Edition. – Auerbach Publications, 2006. – 424 p.

[22] Coombs W.T. Ongoing crisis communication: Planning, managing and responding / Coombs W.T. – 2nd edition. – CA: Sage, 2007. – 224 p.

[23] Lerbinger O. The Crisis Manager: Facing Risk and Responsibility / O. Lerbinger. – New Jersey: Lawrence Elbaum Associates Publishers, 1997. – 370 p

[24] Miller D. Exposing the errors: An examination of the nature of organizational crisis, in / D. Miller. // Responding to crisis: A Rhetorical approach to crisis communication. – Mahwah, NJ, London: Lawrence Erlbaum Associates, 2004. – 19 -31 p.

[25] Fearn–Banks K. Crisis communications: A casebook approach / K. Fearn–Banks. Mahwah. – NJ: Lawrence Erlbaum Associates, 2007. – 408 p.

[26] Pauchant T.C. Transforming the crisis–prone organization: Preventing individual, organizational, and environmental tragedies / T.C. Pauchant, I.I. Mitroff. – San Francisco, CA: Jossey–Bass, 1992. – 275 p.

[27] Pearson C. M. Reframing crisis management. / C.M. Pearson, J.A. Clair // Academy of management review. – 1998. – 23(1). – P. 59-76.

[28] Regester M., Risk Issues and Crisis Management: A Casebook of Best Practice. / M. Regester, J. Larkin – London: The Institute of Public Relations, 1998. – 264 p.

[29] BCMpedia. Definition of Business Continuity and Disaster Recovery Terminologies [electronic resource]. – 2008. – Mode of Acces: World Wide Web. – URL: http://www.bcmpedia.org.

[30] Bird L. Dictionary of Business Continuity Management Terms / Lyndon Bird. – FBCI, 2011. – 37 p.

[31] Hiles A. Definitive Handbook of Business Continuity Management / Andrew Hiles. – 2nd edition. – Wiley, 2008. – 666 p.

[32] The Federal Response Plan 9230.1–Pl. – Washington, DC: Federal Emergency Management Agency, 1992. – 304 p.

[33] ДСТУ 3891:2013 Безпека у надзвичайних ситуаціях. Терміни та визначення основних понять [Текст]. – На заміну ДСТУ 3891–99 ; Чинний від 2014–01–01. – Київ : Мінекономрозвитку України, 2014. – IV, 17 с. – (Національний стандарт України).

[34] ДК 019:2010 Класифікатор надзвичайних ситуацій. – К.: Держспоживстандарт України, 2010. – 19 с.

[35] Hwang P. Anatomy of organizational crises / Peter Hwang, J. David Lichtenthal // ISBM Report 28. – 1999. – 37 p.

[36] Mejri M. Crisis Management: Lessons Learnt from the BP Deepwater Horizon Spill Oil / Mohamed Mejri, Daniel De Wolf // Business Management and Strategy. – 2013. – Vol. 4. – №. 2. – P. 67-90.

[37] Coombs W.T. Ongoing crisis communication: Planning, managing and responding / Coombs W.T. – 2nd edition. – CA: Sage, 2007. – 224 p.

[38] Coombs W.T. Helping Crisis Managers Protect Reputational Assets Initial Tests of the Situational Crisis Communication Theory / W.T. Coombs, S.J. Holladay // Management Communication Quarterly. – 2002. – 16(2). – P. 165-186.

[39] Meyers G.C. Managing Crisis: A Positive Approach / G.C. Meyers. – Boston: Houghton Mifflin, 1988. – 271 p.

[40] Mitroff I.I. Corporate tragedies: Product tampering, sabotage, and other catastrophes / I.I. Mitroff, R.H. Kilmann. – New York: Praeger, 1984. – 140 p.

[41] Coombs W. T. Protecting organization reputations during a crisis: The development and application of situational crisis communication theory / W.T. Coombs // Corporate Reputation Review. – 2007. – 10(3). – P. 163-176.

[42] Coombs W.T. Conceptualizing crisis communication / W.T. Coombs // Handbook of crisis and risk communication. – New York : Routledge, 2009. – P. 100 - 119.

[43] Антикризисное управление: [учеб. для вузов по экон. спец.] / [Э.М. Коротков, А.А. Беляев, Д.В. Валовой и др.]; Под ред. Э.М. Короткова. – М.: Инфра-М, 2002. – 431 с.

[44] Стасюк О.І. Базові характеристики та класифікація кризових ситуацій в ІТ–сфері / О.І. Стасюк, А.І. Гізун // Інфокомунікації – сучасність та майбутнє: Всеукр. наук.–практ. конф. 6–7 жовтня 2011 р. : тези доп. – Одеса: ОНАЗ, 2011. – С. 62-65.

[45] Про затвердження Порядку класифікації надзвичайних ситуацій за їх рівнями : Постанова Кабінету Міністрів України від 24.03.2004 № 368 // Офіційний вісник України. – 2004. – № 12. – Ст. 740.

[46] Coombs W.T. Crisis Management and Communication. Institute for Public Relations / W.T. Coombs. [electronic resource]. – 2007. – Mode of Acces: World Wide Web. – URL: http://www.instituteforpr.org/topics/crisis–management–and–communications/.

[47] Richardson B. Socio–technical disasters: profile and prevalence. / B. Richardson // Disaster Prevention and Management. – 1994. – 3(4). – P. 41-69.

[48] Smith D. Beyond contingency planning: Towards a model of crisis management / D. Smith // Organization and environment. – 1990. – 4(4). – P. 263-275.

[49] Jaques T. Issue management and crisis management: An integrated, non–linear, relational construct / T. Jaques // Public Relations Review. – 2007. – 33(2). – P. 147–157.

[50] Myers K. N. Total Contingency Planning for Diasters: Managing Risk... Minimizing Loss... Ensuring Business Continuity / K. N. Myers. – John Wiley and Sons, Inc., 1993. – 270 p.

[51] Fink S. Crisis management: Planning for the inevitable / S. Fink. – New York: iUniverse, 200. – 245 p.

[52] Pearson C. M. From crisis prone to crisis prepared: A framework for crisis management /

C.M. Pearson, I.I. Mitroff. The academy of management executive. – 1993. – 7(1). – P. 48-59.

[53] Augustine N.R. Managing the crisis you tried to prevent / N.R. Augustine // Harvard Business Review. – 1995. – 73(6). – P. 147-158.

[54] Harrison, S. Disasters and the media: managing crisis communications / S. Harrison. – Basingstoke: Macmillan Press, 1999. – 238 p.

[55] BS25999–1:2006 Business continuity management. Code of practice – BSI British Standards, 2006 – 28 p.

[56] BS25999–2:2007 Business continuity management. Specification – BSI British Standards, 2007. – 38 p.

[57] NIST SP 800–34 Rev. 1. Contingency Planning Guide for Federal Information Systems. – Gaithersburg, MD, United States: National Institute of Standards & Technology, 2010 – 150 p.

[58] Іванченко Є.В. Базова архітектура експертної системи прогнозування та попередження кризових ситуацій / Є.В. Іванченко, О.В. Гавриленко, А.І. Гізун // Захист інформації. – 2012. – № 3. – С. 94-104.

[59] Карпінський М.П. Метод виявлення інцидентів/потенційних кризових ситуацій / М.П. Карпінський, А.О. Корченко, А.І. Гізун // Захист інформації. – 2015. – Т.17. – №2. – С. 124-130.

[60] Корченко А.О. Метод оцінки рівня критичності для систем управління кризовими ситуаціями / А.О. Корченко, В.А. Козачок, А.І. Гізун // Захист інформації. – 2015.– Т.17. – №1. – С. 86-98.

[61] Корченко А.О. Метод виявлення та ідентифікації порушника в інформаційно-комунікаційних системах / А.О. Корченко, А.І. Гізун, В.В. Волянська, С.О. Гнатюк // Захист інформації. – 2013. – Т.15. – №4. – С. 387-393.

[62] Корченко А.О. Система виявлення та ідентифікації порушника в інформаційно-комунікаційних мережах / А.О. Корченко, В.В. Волянська, А.І. Гізун // Безпека інформації. – 2013. – Т.19. – №3. – С. 158-162.

[63] Гізун А.І. Аналіз сучасних систем управління кризовими ситуаціями / А.І. Гізун, А.О. Корченко, С.О. Скворцов // Безпека інформації. – 2015. – Т.21. – №1. – С. 87-101.

УДК 004.056.53:004.492.3 (045)

Гизун А.И., Лозова И.Л. Анализ дефиниций понятия кризисной ситуации и основных аспектов концепции управления непрерывностью бизнеса

Аннотация. *Концепция управления непрерывностью бизнеса как перспективное направление оперативного и стратегического менеджмента определяет важность защиты информационных ресурсов в условиях воздействия кризисных ситуаций. Таким образом, основным элементом данной концепции является понятие «кризисная ситуация», которое не имеет четкого определения и меняется в зависимости от области науки и техники. В этой статье проведен анализ известных определений понятия «кризисная ситуация», в частности в области экономики, политики, медицины, психиатрии, менеджмента и других сфер, на основе чего сформировано определение в рамках концепции управления непрерывностью бизнеса. Также рассмотрены основные подходы к периодизации процесса управления кризисами, подходы к классификации кризисных ситуаций, которые описаны в стандартах, практиках и нормативных документах управления непрерывностью бизнеса и работах ведущих ученых в данном направлении. Кроме того, обоснованно отнесение систем управления кризисными ситуациями к отдельному классу в структуре системы менеджмента информационной безопасности и определены их функциональные взаимосвязи с другими защитными системами, такими как системы обнаружения и предотвращения вторжений, системы анализа и оценки рисков, системы антивирусной защиты, системы управления инцидентами информационной безопасности.*

Ключевые слова: *кризисная ситуация, дефиниция, управления, система, менеджмент информационной безопасности, классификация кризисных ситуаций, концепция управления непрерывностью бизнеса, этапы процесса кризисного управления.*

Gizun A., Lozova I. Analysis of «crisis» definition and basic aspects of business continuing planning concept

Abstract. *The concept of business continuity management as a promising area of operational and strategic management determines the importance of protecting information resources in conditions of crisis. Thus, the main element of this concept is the concept of "crisis", but that is not clearly defined and varies depending on the field of science and technology. This article analyzed the known definitions of the term "crisis", in particular in the fields of economics, politics, medicine, psychiatry, management and other areas, which formed the basis for the definition within the concept of business continuity management. As well as the basic approach to periodization process of crisis management, approaches to the classification of crisis situations covered in the standards, practices and regulations of business continuity management and leading researchers in this field. In addition, a valid assignment of crisis management to a class in the structure of the management system of information security and defined their functional relationships with other protective systems, such as detection systems and intrusion prevention systems, analysis and risk assessment system antivirus protection, management information security incidents.*

Key words: *crisis, management, system, method, developments, detection, model, software, forecast, emergency procedures, evacuation, support systems.*

Отримано *16 лютого 2016 року*, затверджено редколегією *3 березня 2016 року*