Годишник Телекомуникации 2014, том 1, с. 109 - 118

Yearbook Telecommunications 2014, vol. 1, p. 109 - 118

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

КРИТЕРИЙ НА СИСТЕМА ЗА УПРАВЛЕНИЕ НА НЕПРЕКЪСВАЕМОСТТА НА БИЗНЕСА В ТЕЛЕКОМУНИКАЦИОННИТЕ СТРУКТУРИ

Кристиан Томов

CRITERIA FOR BUSINESS CONTINUITY MANAGEMENT SYSTEMS IN TELECOMMUNICATION STRUCTURES

Kristian Tomov

Резюме: Представената работа разглежда въпросите за извеждане на подходящи критерии на система за управление на непрекъсваемостта на бизнеса в телекомуникационните структури, както и за насоките относно нейната ефективност. Въз основа на анализ на характерни инциденти, са разгледани примери на свързаните съществуващи стандарти. Представена е последователността от стъпки на процеса за управление на непрекъсваемостта, дадена е схема за реакция спрямо вид инциденти, подход за анализ на въздействие върху бизнеса, както и модел за развитие на криза и възстановяване на бизнес операциите.
Ключови думи: управление на непрекъсваемостта на бизнес процеси, анализ на въздействия върху бизнеса, модел за реакция при кризи.

Abstract: This work addresses the issues of forming appropriate criteria for a business continuity management system in telecommunication structures and guidelines regarding its effectiveness. The results are based on an analysis of typical incidents and examples of existing internationally recognized standards. Presented is a sequence of process continuity management steps, a scheme for reactions to different types of incidents, an approach to analyzing the impact on the business operations and the development of a crisis and recovery business continuity model.
Keywords: business continuity management, business impact analysis, crisis response model.

1. ВЪВЕЖДАНЕ В ПРОБЛЕМАТИКАТА

Според Центъра за изследване на епидемиологията на бедствия (CRED - Centre for Research on the Epidemiology of Disasters), между 2000 и 2008 г., средният брой на бедствията годишно е бил 392, а средните годишни икономически щети са били $ 102,6 милиарда в глобален план. През 2009 г. е имало 335 бедствия и икономически щети от $ 41,3 милиарда. САЩ претърпяха най-лошото икономическо въздействие през 2009 г. ($ 10.8 млрд.), следвани от Китай ($ 5,2 млрд.) и Франция (3,2 млрд. долара). Броят на бедствията се увеличават всяка година.

Примери (за по-конкретно пояснение):

28.08.2012

Дружеството „United Airlines“ е имало масивни неизправности в оперативните си системи, които причиниха хаос в повечето американски летища. Такива инциденти не са нови, но тези изглеждат доста впечатляващо по отношение на силното им въздействие върху бизнеса на дружеството.

21.04.2011

Отпадането на услугата на Amazon облака на 21-ви април, привлече голямо внимание, комуникациите на глобални играчи (клиенти) бяха офлайн за няколко дни. Amazon реагира официално на отпадането на услугата си, близо след седмица и предложи на клиентите си извинение и кредити в облака.

15.04.2011

От 15.04.2011 до 25.04.2011 “Toyota Motor Engineering & Manufacturing North America, Inc.” намали производството си в американските си заводи с 50%, поради

липсващ план за управление на непрекъсваемостта във връзка с „Just In Time Supply Chain“.

Използваните в текста литературни източници са изключително стандарти и се разкриват последователно в текста с цитати на точния стандарт.

2. ТЕРМИНОЛОГИЯ

НЕИЗПРАВНОСТ (Malfunction)

Неизправност е ситуация, при която процеси или ресурси на една организация не работят по предназначение. Вредите са резултат от неизправност. За "ниска" класифицирана повреда в този смисъл е повреда, която е пренебрежимо малка в сравнение с годишните резултати на една фирма или общия бюджет на правителствена агенция, или само има незначителен ефект върху способността на дружеството или правителствена агенция да изпълнява своите задачи. Повредите обикновено се елиминират по време на изпълнение на ежедневните процедури по отстраняване на проблемите, интегрирани в рутинни бизнес операции. Неизправността трябва да бъде оценявана по спешност, да се наблюдава критично, документира внимателно и да се елиминира незабавно.

АВАРИЯ (Emergency)

Авария е събитие, в което процеси или ресурси на организацията не функционират както е планирано. Наличието на съответните процеси или ресурси не могат да бъдат възстановени в необходимия срок. Бизнес операциите са сериозно засегнати. Това може да се изразява в невъзможност да се потвърди всяка съществуваща SLAs (service level agreement - споразумения за ниво на обслужване). Получените щети могат да бъдат оценени на високи до много високи, когато повлияват годишните резултати на една фирма или способността на правителствената агенция да изпълни задачите си толкова значително, че тази вреда да е неприемлива. Извънредни ситуации не могат да се обработват по време на общите ежедневни бизнес операции и изискват специална организация за непрекъснатост на бизнес отговор.

КРИЗА (Crisis)

Криза се разбира като ситуация на отклонение от нормалното състояние, което може да се случи по всяко време, независимо от превантивните предпазни мерки, прилагани в компанията или правителствената агенция, и които не могат да бъдат манипулирани от нормалните организационни и оперативни структури. Управление на кризи се активира в този случай. Не са налице процесуални планове за реагиране при кризи, само общи инструкции и условия. Характерна особеност на кризата е уникалността на събитието.

Извънредни ситуации, които могат да се отразят неблагоприятно на непрекъснатостта на бизнес процесите могат да ескалират и да станат кризи. Криза в този случай се разбира като сериозна извънредна ситуация, в която съществуването на организацията или здравето и живота на хората са изложени на риск. Кризата се концентрира върху фирма или правителствена агенция и няма широко разпространен ефект върху околната среда или обществения живот. Криза може да се управлява, поне за по-голямата си част от самата организация.

Въпреки това, съществуват редица кризи, които не влияят на бизнес процесите. Примери за подобни кризи са икономически кризи, управление на кризи, ликвидни кризи, измами, изнудване на продукт или злоупотреба, отвличане и бомбени заплахи. Кризи, разгледани в рамките на този стандарт, представляват подмножество на тези кризи.

БЕДСТВИЕ (Disaster)

Бедствието е мащабно вредно събитие, което е трудно да се ограничава хронологично и на местно ниво. То има или може да има широкообхватни ефекти върху хората, активите и собствеността. Съществуването на организацията или живота и здравето на хората са изложени на риск. Общественият живот също е сериозно засегнат. Едно бедствие не може да се обработва само от организацията. Поради географското

разпространение на бедствието и неговото въздействие върху населението, в частност, са необходими екипи за възстановяване след бедствие. Това е отговорност на държавите. В Германия се дава и подкрепата на федералното правителство. От гледна точка на организацията, бедствието се счита за криза и се обработва вътрешно от непрекъснатост на бизнес-екип отговор на организацията в сътрудничество с външни организации за помощ.

3. СТАНДАРТИ ЗА НЕПРЕКЪСВАЕМОСТ

Предметът на управлението на непрекъснатостта се обработва в различни стандарти, както и в национални и де-факто стандарти. Някои стандарти са представени накратко по-долу (списъкът не е пълен).

BS 25999-1 / BS 25999-2

BS 25999-1 “Business Continuity Management (BCM) - Part 1: Code of Practice”, публикуван през ноември 2006 г. от Британския институт по стандартизация, описва структурата на системата за управление на бизнес приемствеността [BS259991]. Това включва, наред с другите елементи, организационната структура, изпълнението на непрекъснатостта на бизнес процесите за управление въз основа на кодексите за добрите практики и организационната концепция на гаранциите. Не са описани подробните стъпки, които трябва да се предприемат, както и конкретните предпазни мерки, които следва да бъдат изпълнени за управление на бизнес приемствеността. Читателят трябва да се отнесе към други стандарти, като например ISO 27001, ISO 20000, или PAS77 за тази цел.

Британският стандарт BS 25999-2 "Business Continuity Management - Част 2: Спецификация" определя изискванията, които трябва да бъдат изпълнени за сертифициране на бизнес система за управление на непрекъснатост [BS25999-2].

В основата на системата за управление на непрекъснатостта на бизнеса, съгласно BS 25999 за управление на програмата, която е елемент на контрол, е определянето на сферите на отговорност и осигуряването на постоянна съвместимост на бизнес процесите. Получаването на подробни знания (прозрачност) на собствената организация (например чрез извършване на BIA и анализ на риска) са нужни за успешното предотвратяване и контролиране на събития застрашаващи непрекъсваемостта на компанията.

Жизненият цикъл на BS 25999 се състои от четири фази:

1. Развитие на BCM опции за стратегия.
2. Разработване и внедряване на реакционни мерки и BCM планове.
3. Извършване на BCM упражнения, проучване и рафиниране на BCM планове и BCM гаранции.
4. Подкрепата трябва е да бъде предоставена на тези четири фази, чрез създаване на BCM култура в организацията.

Good Practice Guidelines (GPG)

Друга насока BCM е "Добри практики и насоки" (GPG) от Института Бизнес Приемственост (BCI) [GPG08]. BCI е основана през 1994 г. и има повече от 4000 членове в над 85 страни (към февруари 2008 г.). Нейната цел е да се създаде висок стандарт за управление на непрекъснатост на стопанската дейност и да се превърне в орган в тази област.

Насоките за добра практика бяха публикувани за първи път през 2002 година. Те са разработени от членовете на нашите органи и оттогава са редовно актуализирани и оптимизирани. GPG е преведена на няколко езика. Немският превод е от 2005.

BCI GPG 2008 г. е разделен на шест секции:

1. BCM политика и програмата за управление (развитие на BCM политики и управление на процесите)
2. Разбиране на организацията
3. Определяне на BCM стратегията
4. Разработване и прилагане на BCM коментара
5. Упражняване, поддържане, и преглед на BCM договореностите
6. Вграждането на BCM в културата на организацията

С повече от 120 страници, GPG от BCI, като един от малкото квази-стандарти, предлага реална помощ за изпълнение и прилагане на управлението на непрекъснатостта на дейността в една организация.

ISO / PAS 22399

Предварителната норма ISO / PAS 22399 -"Обществена сигурност - Насоки за инцидента, готовност и оперативно управление на приемствеността" е публикувана през 2007 г. [ISO22399]. Тази предварителна норма описва в 31 страници процесите и принципите на "Готовността за инцидент и оперативното управление на приемствеността" (IPOCM) в общ смисъл на общи стандарти ISO.

Животът на IPOCM цикъл е разделен на следните фази:

1. Политика
2. Планиране
3. Внедряване и функциониране
4. Оценяването на изпълнението
5. Преглед на ръководството

На IPOCM жизнен цикъл съдържа всички стъпки в BCM жизнен цикъл. Следователно терминът "IPOCM" трябва да бъде продължение на термина "BCM".

Предварителната норма се основава на NFPA 1600 [NFPA1600], HB 221:2004 HB221, BS 25999-1:2006 [BS259991], INS 24001:2007 [INS24001] стандарти и на японските разпоредби. Особеното на тази норма е целевата група. Тази целева група са компаниите, но разбира се, се фокусира специално върху частните и обществени организации, както и върху администрацията.

ISO 27001 / ISO 27002

Поради сложността на информационните технологии и търсенето на сертифициране, множество ръководства, стандарти и норми за ИТ сигурността се появиха през последните няколко години. ISO / IEC 27001 "Информационни технологии - техники за сигурност - Информационни системи за управление на сигурността, изисквания за спецификация" [ISO27001] е първият международен стандарт за управление на информационната сигурност, която също така позволява сертифициране. ISO / IEC 27001 предвижда общи препоръки на около 10 страници. Препоръки за сигурност (контрол) има и в ISO / IEC 27002. Те са посочени в нормативното приложение. Въпреки това, не се предоставя на читателя каквато и да е помощ за практическото изпълнение.

ISO / IEC 27002 (по-рано ISO / IEC 17799) стандарт "Информационни технологии - Кодекс на практиката за управление на информационната сигурност" [ISO27002] е колекция от опит, процедури и методи, придобит от практическите приложения. Нейната цел е да определи рамка за управление на информационната сигурност. Стандартът се отнася предимно към стъпките, необходими за разработване на система за управление на сигурността, както и към интегрирането на сигурност в организацията. Съответните препоръки за сигурност са скицирани накратко на около 100 страници. Глава 14 на ISO / IEC 27002 се занимава с управлението на непрекъснатостта (BCM). Пет страници в тази глава, съдържащи препоръки за BCM в рамките на управлението за сигурност, са много общи и описват най-важните етапи от процеса, които трябва да се преминат от управленското ниво.

NIST SP 800-34

NIST SP 800-34 стандарт "Ръководство за планове за извънредни ситуации за системи за информационни технологии", публикуван през 2002 г. от Националния институт за стандарти и технологии (NIST), е наръчник за планиране на непредвидени случаи за ИТ системи [NIST34].

NIST SP 800-34 стандарт описва методология за структуриране на ИТ организация, планирането при извънредни ситуации, избора и прилагането на гаранциите за ИТ планиране при извънредни ситуации. На около 60 страници се дават напътствия за справяне с извънредни ситуации. В определени пасажи се дават и специфични подходи. Шаблони могат да бъдат намерени в приложението, с документи, които трябва да бъдат създадени, например, за анализ на въздействието върху бизнеса или ИТ план за действие при извънредни ситуации.

За IT-непрекъснатост на услугата е описан жизнен цикъл в седем етапа:

1. Разработване на политика.
2. Извършване на анализ на въздействието върху бизнеса.
3. Дефиниране на профилактичния контрол.
4. Разработване на стратегии за събиране на вземания.
5. Разработване на планове за действие при извънредни ситуации.
6. Планиране, тестване, обучение и упражнение.
7. Актуализиране на ИТ планове за действие при извънредни ситуации.

Стандартът главно е насочен към правителствените агенции на САЩ, но ръководството е приложимо и за организации от всички видове и размери.

PAS 77 / BS 25777

Публично достъпна спецификация 77:2006 "IT Service Management Приемственост - Кодекс на добрите практики" от британската организация за стандарти [PAS77], която описва принципите и методите за структуриране и изпълнение на ИТ система за управление на непрекъснатостта на услугата. Този предварителен стандарт е на разположение на обществеността, но не е безплатен. PAS 77 може да се разглежда като допълнение към BS 25999 в областта на планирането на ИТ услуги. В момента може да се намери в най-новата версия на БДС 25777 "Кодекс за практика за непрекъснатост на информационните и комуникационните технологии". Първият проект е с 38 страници и е издаден през септември 2008 г. за външни коментари и може да се получи срещу заплащане. Целевата група на тази спецификация е групата от лицата, отговорни за структуриране, изпълнение и поддържане на ИТ непрекъснатост на услугата. Целта е създаването на ИТ план за извънредни ситуации за ИТ услугите, които са от критична важност. Съответните предпазни мерки и планове имат за цел да сведат до минимум прекъсванията на ИТ операциите и да се гарантира бързото възстановяване след провала на ИТ услугите.

ITIL

"IT Infrastructure Library (ITIL) са публикувани, актуализирани и рафинирани от Службата на държавния Commerce (OGC) на британската правителствена агенция. Настоящата версия на ITIL V3, се появи през 2007 година. В същото време, тя е била приета в целия свят като де-факто стандарт за проектиране, изпълнение и управление на големи ИТ процеси за контрол. Библиотеката е процесуална библиотека на най-добри практики и публикации, описващи методите за планиране и управление на ИТ услуги.

Управлението на ИТ услуги е централен организационен инструмент за съгласуването на ИТ с изискванията на бизнеса и за контролирането на ИТ услугите от

изискванията на клиента. Тези процеси за управление на услуги формират основата на ITIL.

ИТ цикълът за непрекъснатост на услугата (в съответствие с ITIL) се състои от четири фази:

1. Започване на процеса: спецификация на политиката и на обхвата / приложимост / ИТ системи;
2. Изисквания и стратегия: анализ на въздействието бизнес, анализ на риска и стратегия приемственост;
3. Изпълнение: разработване на планове за непрекъснатост, реставрация на планове и тестване на стратегии;
4. Оперативно управление: обучение и повишаване на осведомеността, одити, тестове и управление на промяната;

ISO / IEC 24762

Стандартът ISO / IEC 24762 "Информационни технологии - техники за сигурност - Насоки за информационни и комуникационни технологични услуги за възстановяване след бедствие", публикуван в началото на 2008 г., се занимава с изискванията за услугите за възстановяване на информационните и комуникационните технологии. Стандартът се отнася както за вътрешни, така и външни доставчици на услуги за информационни и комуникационни технологии (ИКТ) и на услугите за възстановяване след бедствие (DR – disaster recovery). Той описва изискванията за прилагане, експлоатация, мониторинг и поддържане на DR услуги. ИКТ услуги са част от управлението на непрекъснатостта.

4. ПРОЦЕС ЗА УПРАВЛЕНИЕ НА НЕПРЕКЪСВАЕМОСТТА

Систематичните процедури трябва да се проектират за управление на непрекъснатостта на бизнес процесите. Непрекъснатостта на бизнес процесното управление се състои от следните фази: започване на управление на бизнеса, приемственост, планове за действие при извънредни ситуации, прилагане на концепцията за планиране при извънредни ситуации, тестове и упражнения, както и поддържане и непрекъснато подобряване на бизнес процесите за управление на непрекъснатостта (фиг. 1).

Преди да може да се внедри в една организация процеса за управление на бизнес-непрекъсваемостта, трябва да бъдат определени общите условия. Политиката за управление на непрекъснатост на дейността трябва да бъде създадена и подписана от ръководството, с цел определяне на важността и на ресурсите за нейното изпълнение. В допълнение, трябва да бъдат изпълнени и организационните предпоставки за управление на непрекъснатостта. За да се направи това, ролите и отговорностите трябва да бъдат уточнени и трябва от ръководството на организацията да бъде предвиден адекватен бюджет

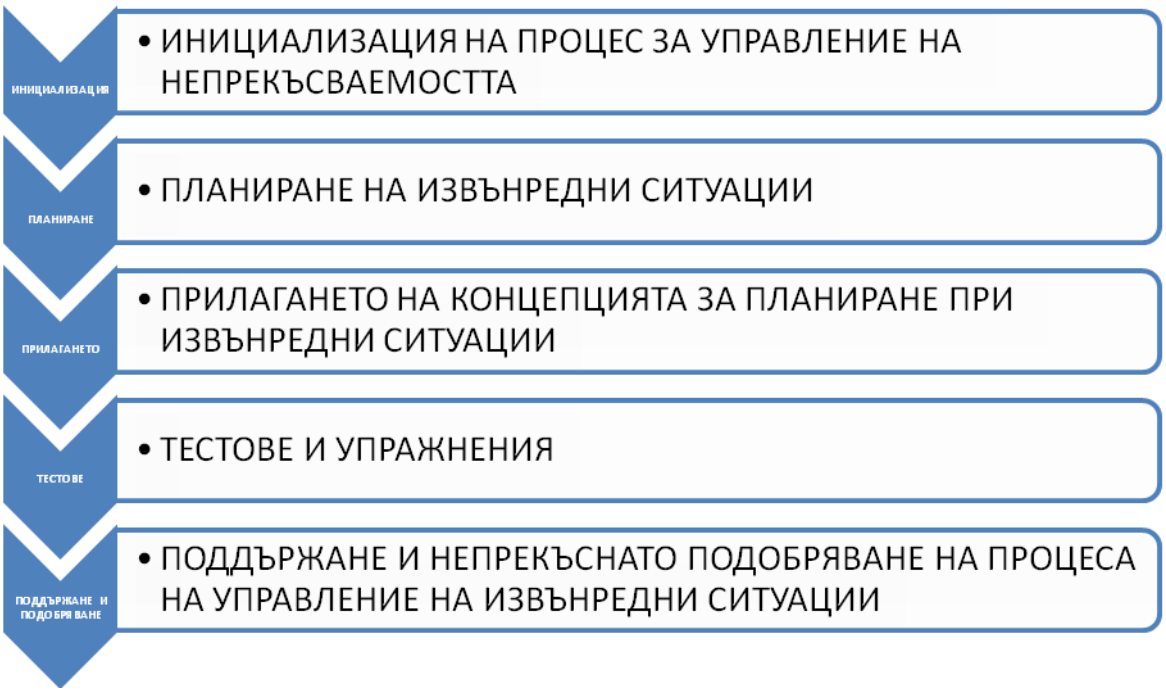
От гледна точка на ефективността, най-подходящия подход на международните компании е както следва – фиг.2.

Успешната интеграция на предмета на управление на непрекъснатостта на дейността в съществуващата правителствена агенция или корпоративната култура е от решаващо значение за успеха на бизнес процесите за управление на непрекъснатостта. За да се постигне това, служителите трябва да бъдат интегрирани в процеса и трябва да бъдат подготвени за ролите си, чрез повишаване на осведомеността и чрез програми за обучение. Трябва да бъде определен и екип за управление на кризи. За такива най-често се определят директорите на компанията (горните нива - от административно ниво М1 до М3). Също така е подходящо да се разработи матрица за ескалация на заплахите и тяхното въздействие върху оперативния бизнес.

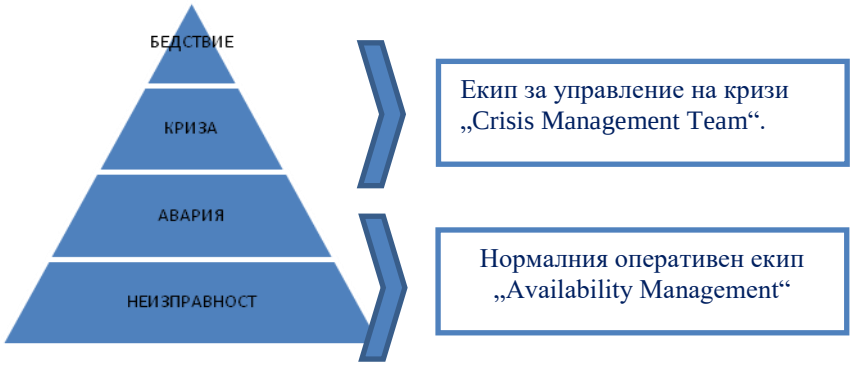
Годишник Телекомуникации 2014, том 1, с. 109 - 118

Yearbook Telecommunications 2014, vol. 1, p. 109 - 118

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii



Фиг. 1. Стъпки на процеса за управление на непрекъсваемостта.



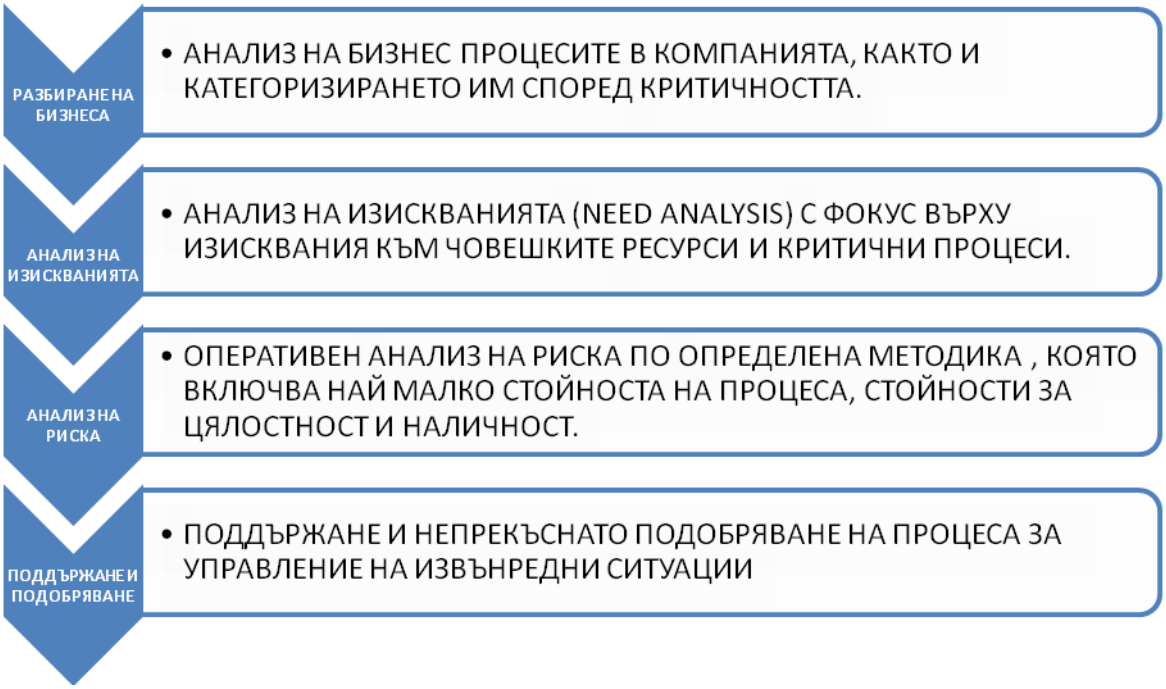
Фиг. 2. Схема за реакция спрямо вид инциденти.

Информацията, придобита чрез анализ на въздействието върху бизнеса (Business Impact Analyse - BIA) формира основата на концепцията за управление на непрекъснатостта на бизнеса (фиг. 3). В контекста на BIA, са определени както критичните бизнес процеси на организацията, така и приоритетите за възстановяване. В допълнение са идентифицирани ресурсите и подкрепящите бизнес процеси, както и минималните изисквания за потенциални аварийни действия.

Анализ на риска се извършва, за да се определят критичните процеси и ресурси. Анализът дава отговор на въпроса "Какво заплашва процесите и ресурсите ми?". Тази информация може да е вече на разположение в друга система за управление.

Въз основата на информацията от BIA и на анализа на риска, се разработват различни варианти и стратегии (сценарии). От тези опции се избират подходящи стратегии за непрекъсваемост (BCPs - business continuity plans). Тези стратегии определят рамката за избор на превантивни мерки, а следователно и за свързаните с тях инвестиции. Посочват се и извънредните мерки (концепция за планиране на непредвидени ситуации) и тяхото прилагане. Това включва също и разработването на наръчник за непрекъснатост на

стопанската дейност, който формира основата за реагиране при извънредни ситуации и се използва като помощно средство по време на такива събития.



Фиг. 3. Подход за анализ на въздействие върху бизнеса.

При разработка на такъв план и сценарий може да се зададат следните въпроси:

- Нужно е да се приеме възможността за най-лошото, за загубата на корпоративна локация, предизвикана от международно бедствие. Какви са ефектите и отговорностите върху компанията и човешките ресурси.
- Идентифициране на взаимозависимостите = на пазара, от географски характер, сред бизнес участниците в еко-системата на компанията, както и на доставчиците на инфраструктурни услуги.
- Определяне на Recovery Point Objective (RPO) и Recovery Time Objective (RTO) (уточнение за документиране, в точка 6 на документа), на апликации и на нужни инфраструктурни системи.
- Създаване на смесени технически среди, където са налице различни бази данни. Трябва де се подготвят решения и софтуер за възстановяване след инциденти/бедствия и „high availability“.

При технологичните компании е смислено да се изградят планове за непрекъсване на дейността не само на база процес, а и на база технология и платформа.

За поддържане и подобряване на бизнес процесите за управление на непрекъснатост трябва да се извършват тестове, упражнения на методите и процедурите, описани в различни документи за непрекъсваемост на бизнеса, оценки на отговорите на предишните извънредни ситуации, както и редовни прегледи. Промени и оптимизирането на вътрешната контролна система за управление на непрекъсваемостта са нужни като част на процеса за непрекъснато подобрение.

5.ДОКУМЕНТАЦИЯ

В различните фази на управление на непрекъснатостта на бизнес процесите се създава разнообразие от концепции, проверки и протоколи от изпитания и допълнителни документи за управление на непрекъснатостта на дейността в организацията. Документация на решенията е много важна.

Годишник Телекомуникации 2014, том 1, с. 109 - 118

Yearbook Telecommunications 2014, vol. 1, p. 109 - 118

eISSN 2534-854X https://telecommunications.nbu.bg/bg/godishnik-telekomunikacii

Бързата и ефективна способност да се справяме с извънредни ситуации зависи преди всичко от наличната документация. Наличието на тези документи играе решаваща роля. Те са допълнение на тяхното качество и показват как са те до момента. Служителите в бизнес екипа, отговарящи за приемствеността, се нуждаят от бърз достъп до документите, които трябва да са достъпни във всеки един момент.

Примери на документите, които трябва да бъдат създадени, включват следното:

1. Политика за управление на непрекъснатостта,
2. Концепция за планиране на непредвидени случаи с анализ на въздействието върху бизнеса и доклади за анализ на риска,
3. Наръчник за непрекъсваемост на бизнеса с актуални данни за контакти, инструкции за реакция и план за провеждане на тренировки,
4. Концепции за провеждане на тренировки и бланки за записи, документация на обучения,
5. Оценки на реакцията и адекватността на отговорниците по време на извънредни ситуации,
6. Одитните доклади и други доклади,
7. Решения на управлението на компанията за непрекъсваемостта на бизнеса.

6. РАЗВИТИЕ НА КРИЗА

Диаграмата на фиг. 4 показва класически случай на инцидент (бедствие, криза). Тя показва подходящ модел за структуриране на кризисните фази и възстановяването на бизнес операциите.

Recovery Point Objective (RPO) - Определя се максимално допустимата загуба на данни в случай на криза.

Recovery Time Objective (RTO) - Определен период от време, в рамките на който критичните бизнес процеси трябва да се възстановят.

Фиг. 4. Модел за развитие на криза и възстановяване на бизнес операциите.

7. ЗАКЛЮЧЕНИЕ

В работата е направен анализ на характерни инциденти, който е подкрепен с примери на съществуващи стандарти, от гледна точка на най-съществените модели и процедури за осигуряване на непрекъсваемост на бизнес процесите.

Въз основа на направения анализ е представена последователността от стъпки на процеса за управление на непрекъсваемостта, дадена е схема за реакция спрямо вид инциденти, подход за анализ на въздействие върху бизнеса, както и модел за развитие на криза и възстановяване на бизнес операциите.

Възможна бъдеща работа е сравнение в реални условия и създаване на модел за определяне на ефективността.

ЛИТЕРАТУРНИ ИЗТОЧНИЦИ:

[1] BS 25999-1:2006 - Business continuity management Part 1: Code of practice. *ENISA* [online]. [viewed 13 April 2013]. Available from: https://www.enisa.europa.eu
[2] *Good Practice Guidelines (GPG)* [online]. 2008 [viewed 13 April 2013]. Available from: https://www.thebci.org
[3] *ISO/PAS 22399: 2007. Societal security-Guideline for incident preparedness and operational continuity management* [online]. [viewed 16 April 2013]. International Organization for Standardization. Available from: https://www.iso.org
[4] ISO 27001/ISO 27002. *Information technology-Security techniques – Information security management systems* [online]. [viewed 16 April 2013]. International Organization for Standardization. Available from: https://www.iso.org
[5] SWANSON, Marianne, Pauline BOWEN, Amy WOHL PHILLIPS, Dean GALLUP, David LYNES. NIST SP 800-34 – Special publication. Contingency Planning Guide for Federal Information Systems. *National Institute of Standards and Technology* [online]. 2010 [viewed 16 April 2013]. Available from: https://www.nist.gov/
[6] PAS 77 / BS 25777 - IT Service continuity Management - Code of Practice. *BSI shop* [online]. [viewed 16 April 2013]. Available from: https://shop.bsigroup.com
[7] *ITIL - IT Infrastructure Library* [online]. [viewed 16 April 2013]. Available from: https://www.itlibrary.org/
[8] ISO/IEC 24762 Information technology -- Security techniques -- Guidelines for information and communications technology disaster recovery services. *International Organization for Standardization*. [online]. 2010 [viewed 16 April 2013]. Available from: https://www.iso.org
[9] Basel Committee on Banking Supervision: High-Level Principles for Business Continuity, Bank for International Settlements. *BIS* [online]. August 2006 [viewed 16 April 2013]. Available from: www.bis.org
[10] Financial Services Authority (FSA): Business Continuity Management - Practice Guide. *FSA* [online] 2006. [viewed 16 April 2013]. Available from: www.fsa.gov.uk
[11] Australian Prudential Regulatory Authority (APRA): Prudential Standard APS 232 „Business Continuity Management" und Guidance Note 232.1. *APRA* [online] April 2005 [viewed 16 April 2013]. Available from: www.apra.gov.au
[12] British Standards Organization: The Guide to Business Continuity Management, Publicly Available Specification PAS 56:2003. *Automataservices* [online]. 2003 [viewed 16 April 2013]. Available from: www.automataservices.com
[13] Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System. *Federal Reserve* [online]. [viewed 16 April 2013]. Available from: www.federalreserve.gov
[14] Aligning Business Continuity and Information Security. *Information Security Forum* [online]. March 2006. [viewed 16 April 2013]. Available from: www.securityforum.org
[15] Pandemie-Handbuch. *Staatsekretariat für Wirtschaft* [online]. March 2006. [viewed 16 April 2013]. Available from: www.seco.admin.ch
[16] Influenza-Pandemieplan Schweiz. Bundesamt für Gesundheit[online]. March 2006. [viewed 16 April 2013]. Available from: www.bag.admin.ch/influenza

Информация за автора:
Кристиан Томов, докторант, Департамент "Телекомуникации" на НБУ, ул. Монтевидео № 21, 2-609, Тел.: 359 2 8110609, e-mail: kristiantomov@yahoo.com

Contacts:
MSc Kristian Tomov, Postgraduate, Department Telecommunications, 21 Montevideo St., 2-609, Tel: 359 2 8110609, e-mail: kristiantomov@yahoo.com.

Дата на постъпване на ръкописа (Date of receipt of the manuscript): 18.07.2014
Дата на приемане за публикуване (Date of adoption for publication): 02.09.2014