# ЗА ВАЖНОСТТА НА ВЪЗСТАНОВЯВАНЕТО ОТ ИТ БЕДСТВИЯ И АВАРИИ И ВРЪЗКАТА С ПОСТАВЕНИТЕ БИЗНЕС ЦЕЛИ

**Ас. Асен Божиков, СА „Д. А. Ценов" - Свищов**

***Резюме**: Ролята на информационните и комуникационни технологии за осъществяване на бизнес през XXI век е безспорна, но в същото време те могат да се превърнат и в сериозна точка на слабост за бизнес организациите. Широкият спектър от заплахи за сигурността на информационните системи, както и традиционните проблеми, свързани с нефункционалните атрибути на тези системи предполагат необходимостта от съществуване на план за възстановяване от ИТ бедствия и аварии в бизнес организацията. Неговата цел е да осигури подход за справяне със събития, които биха довели до срив в някои от ИТ компонентите, но въпреки това критичните за бизнес дейността системи да продължат да функционират. В същото време този план не трябва да съществува самоцелно, а трябва да е обвързван с бизнес целите, които си е поставила организацията.*

***Ключови думи**: възстановяване от ИТ бедствия и аварии, бизнес цели, защита на данните.*

## 1. Нарастващата роля на информационните технологии за бизнеса

Съвременните информационни технологии (ИТ) се докосват до всяка една сфера на бизнеса. Ръководството на бизнес организациите разчита все повече на ИТ не толкова от гледна точка на това какво правят, а по-скоро на това какво може да се промени или подобри с внедряването им. Още в края на 90-те години на миналия век се посочва, че ролята на ИТ се променя в посока от поддържаща бизнеса към стратегическа за неговото съществуване [8, 4]. Според проучване на IDC световният пазар на ИТ (включват се хардуер, софтуер, услуги и телекомуникации) през 2016 година ще достигне 3.8 трилиона щатски долара [7]. За една съвременна бизнес организация е немислимо осъществяването на точно планиране, ефективен маркетинг, наблюдение на ключови показатели в реално време, незабавно обслужване на клиенти и растеж в дългосрочен план без да се използват съвремен-

ните ИТ. Те се явяват конкурентно предимство за бизнес организацията.

В същото време обаче се наблюдава и непрекъснато нарастване на видовете заплахи, насочени към преодоляване на сигурността на ИТ. Това предполага създаването и поддържане на политика по информационна сигурност във всяка една бизнес организация, която да гарантира защита на корпоративните данни и да обезпечи непрекъснатата работа на най-важните информационни системи. Част от тази политика е свързана със създаването и поддържането на план за възстановяване от ИТ бедствия и аварии. Той се свързва с възстановяне на най-важните информационни системи и приложения, които обслужват критичните бизнес процеси в организацията при възникване на някакви непредвидени събития. Въпреки, че името на плана поскоро предполага възникването на екологични катастрофи или природни бедствия, всъщност по-често причините за прекъсванията в работата на приложенията са породени от повреда в хардуерен компонент, човешка грешка, срив в самото приложение и други [9].

В ерата на дигиталната икономика се наложи стандартът 24x7, което означава, че и най-малкото прекъсване в работата на компютърните системи може да доведе до негативен резултат под различна форма за бизнес организацията. Осигуряването на висока достъпност до информационната система и възстановяването от ИТ бедствия и аварии са едни от движещите сили за ИТ инвестиции. В тази връзка, в България изследването за информационна сигурност на списание CIO за 2016 г. отчита, че 74% от анкетираните организации са включили плановете за възстановяване като организационна мярка за защита на информацията [1].

**2. Предизвикателства пред обвързването на плана за възстановяване от ИТ бедствия и аварии с поставените бизнес цели**

Разработването на план за възстановяване от ИТ бедствия и аварии предполага обвързване на функциониращите ИТ системи с целите на бизнес организацията. Този план не трябва да съществува самоцелно, а трябва да гарантира възстановяването на критичните за бизнеса ИТ системи. Това от своя страна изисква определяне на критичните бизнес процеси и свързаните с тях информационни системи, както и непрекъсната комуникация между ръководството и ИТ отдела. Често пъти обаче се наблюдават сценарии като посочените по-долу [2], които затрудняват поддържането на актуален и ефективен план за възстановяване:

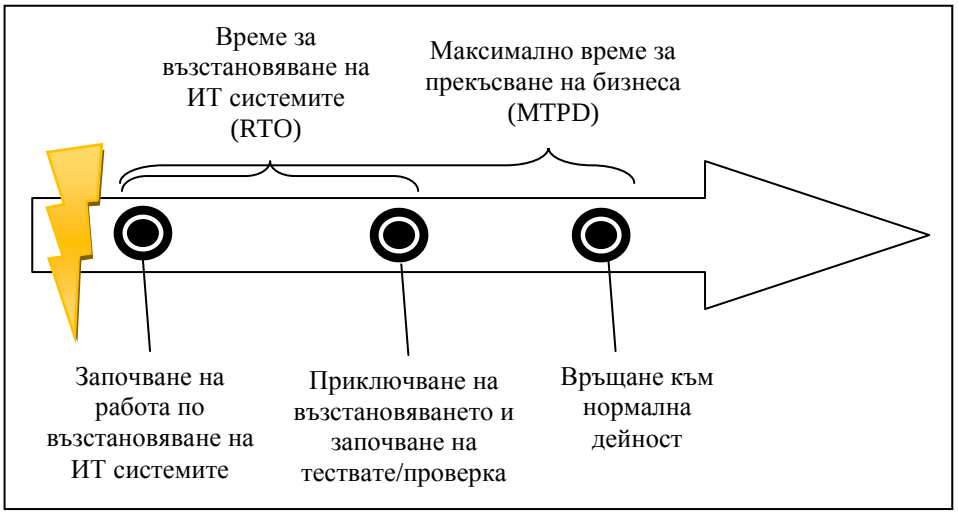
- ✓ ръководството на бизнес организацията взема решение за внедряване на нова система без да е ясно кой ще я поддържа;
- ✓ ръководството на бизнес организацията взема решение за внедряване на нова система без да се съобразява с изискванията от гледна точка на сигурност;
- ✓ ръководството на бизнес организацията взема решение за разглеждане на всички системи като критични;
- ✓ ИТ отделът поддържа системи, които не се използват изобщо за нуждите на организацията.

В резултат на това може да се достигне до: невъзможност за бързо възстановяване на най-важните системи, инвестиции в твърде голям размер или в неправилната технология, неприемливо ниво на загуба на данните и др. Като основна причина за очертаните проблеми може да се посочи разминаването между очакванията на ръководството и възможностите на ИТ системите. Важна предпоставка за преодоляването на този проблем според Чан е стратегическото обвързване между дейността на различните отдели в бизнес организацията и внедрените ИТ системи [3].

Липсата на точно дефинирани изисквания от ръководството за възстановяване на ИТ системите е друг проблем, на който трябва да се отдели внимание. За да могат да се определят критичните бизнес процеси е необходимо извършването на анализ за въздействие върху дейността (Business Impact Analysis, BIA), а така също и анализ и оценка на рисковете (Risk Assessment), които могат да доведат до прекъсване в изпълнението на съответните процеси. На база на резултатите от направените анализи се дефинират и критичните ИТ системи и приложения, без които е невъзможно осъществяването на бизнес дейността. Заедно с това трябва да се вземат под внимание връзките и зависимостите между отделните системи и приложения. Те трябва да се ревизират непрекъснато, тъй като всяка една промяна в бизнес средата или ИТ инфраструктурата оказва влияние върху дейността на организацията.

Полезен инструмент в това отношение е съставянето на каталог на ИТ услугите, в който се посочва тяхната критичност, връзката им с конкретен бизнес процес, както и нужното време за възстановяване. По този начин отделните системи се категоризират по важност и за всяка една група може да се определят очакваното време за възстановяване и технологиите, които ще се имплементират. Необходимостта от такъв каталог се обуславя и от факта, че непрекъснато нараства броят на използваните ИТ услуги в бизнес организациите, а заедно с

това се увеличава и процентът на критичните за бизнеса системи [6]. В същото време някои бизнес организации възприемат подхода за възстановяване “one size fits all” за всички бизнес процеси и осигуряват едно и също ниво на показателите за време на възстановяване и точка на възстановяване [5]. Това е погрешно и не бива да се допуска.




**Фиг. 1**. Показатели, свързани с възстановяването на ИТ системите.

Разминаване се наблюдава и в разбиранията на ръководството и ИТ отдела по отношение на конкретните показатели, свързани с възстановяването на ИТ системите (фиг. 1). ИТ отделът разглежда възстановяването на дадена система или приложение от гледна точка на необходимото време това да стане и възможността за минимална загуба на данни (RTO и RPO). От друга страна за ръководството най-важно е връщането към нормално функциониране на засегнатия бизнес процес като това се свързва с максимално толерираното време за прекъсване (MTPD) т.е. то не се интересува от възстановяване на самото приложение, а на целия бизнес процес. Само по себе си това поражда различно разбиране за зададените времеви стойности за възстановяване. В резултат на несъответствието може да възникнат катастрофални за дейността на бизнес организацията последици – пропуснати ползи или бизнес възможности, накърняване на репутацията й, отлив на клиенти, спад в продуктивността и морала на служителите и др.

Важен момент, който също трябва да се вземе под внимание е осъществяването на тестване на плана за възстановяване. Колкото и добре да си сътрудничат хората от екипа, зает с неговото изготвяна и

колкото и ефективни технологии да са използвани за реализацията му ако той не се тества поне веднъж годишно няма гаранция, че ще проработи, когато е необходимо.

**Заключение**

Информационните технологии се превръщат в стратегически приоритет в икономиката на знанието, което е предпоставка за засиленото им използване в бизнес организациите. В същото време гарантирането на сигурността на ИТ се превръща в сериозно предизвикателство. Вече всяка организация, която използва ИТ е необходимо да разполага с план за възстановяване от ИТ бедствия и аварии. Неговото изготвяне е свързано с редица предизвикателства, сред които са дефинирането на ключови бизнес процеси и системи, обвързването им с бизнес целите и непрекъсната комуникация между отделните участници/отдели.

**ЛИТЕРАТУРА**

1. Кръстева, Н. Българските организации обогатяват арсенала за защита. // CIO, 2016, N 6, с. 12.
2. Aligning Business & Technology Strategies, http://www.datacenterknowledge.com/archives/2014/09/16/aligning-business-technology-strategies/, <18.9.2016>
3. Chan Y. E. Why Haven't We Mastered Alignment? The Importance of the Informal Organization Structure. // MIS Quarterly Executive, 2002, June, Vol. 1 N 2, p. 97-112
4. Elmorshidy. A. Aligning IT with Business Objectives: A Critical Survival and Success Factor in Today's Business. //The Journal of Applied Business Research, 2013, Vol. 29, N 3, p. 819-828
5. Gow Jr., G. Addressing Business Interruption Exposures. // Risk Management, 2016, N 5, p. 18-19
6. IBM Survey 2016. Masters of Disaster Recovery, http://www.ibm.com/thought-leadership/technology-market-research/business-continuity-report.html, <16.9.2016>
7. IT Industry Outlook 2016, https://www.comptia.org/resources/it-industry-outlook-2016-final,<15.9.2016>
8. Sheth, J. Strategic Importance of Information Technologies. //Strategic Perspective on the Marketing of Information Technologies, 1994, Vol. 4, p. 3-16

9. Snedaker, S, Rima, C. Business Continuity and Disaster Recovery Planning for IT Professionals. Waltham, 2014.