OCENA DOSTĘPNOŚCI INFORMACJI W ORGANIZACJI GOSPODARCZEJ

Andrzej M. Michalski

Wprowadzenie

W organizacjach gospodarczych informacja należy do najważniejszych zasobów. Bezpieczeństwo posiadanej i wymienianej informacji ma bezpośredni wpływ na osiąganie przychodu z prowadzonej działalności, zachowanie płynności finansowej oraz kreowanie pozytywnego wizerunku marketingowego (pozycji na rynku) [Certyf07]. Wynika z tego, że niezbędna jest właściwa polityka ochrony informacji. Opublikowana w 2005 roku norma ISO 27001, dotycząca zarządzania bezpieczeństwem informacji [Inform05], wyróżnia trzy podstawowe obszary (płaszczyzny), które składają się na bezpieczeństwo informacji, a mianowicie poufność, integralność i dostępność. Każdy z tych obszarów wymaga stosowania odpowiednich metod i technologii. W niniejszym opracowaniu autor postanowił skupić się na zagadnieniu dostępności informacji. Równocześnie zwiększający się udział informacji jako składnika kosztów produktu finalnego oraz duża dynamika procesów produkcyjnych [Michal98], [Siejac98] stanowią obiektywne przesłanki wykorzystania w działalności przedsiębiorstwa systemu informatycznego zarządzania [Damgaa02], ponieważ przetwarzanie znacznych ilości informacji jest możliwe do osiągnięcia jedynie poprzez wspomaganie komputerowe.

1. Informacja i jej dostępność

We współczesnych warunkach zarządzania organizacją gospodarczą dostępność informacji (zasobów informacyjnych) nabiera kluczowego znaczenia i podstawowym sposobem, mającym ją zapewnić, jest wdrożenie systemu informatycznego [Callag02], [Wykorz02]. Wtedy dostępność informacji traktować możemy zarówno jako stan, jak i cechę systemu informatycznego organizacji. Pod pojęciem dostępności informacji w niniejszym opracowaniu rozumie się taki stan (taka cechę) systemu informatycznego organizacji, który (która) zapewnia uprawnionemu użytkownikowi zaspokojenie każdego poprawnie sformułowanego żądania dostępu do informacji w czasie, wynikającym z realizowanych procesów biznesowych. Na rozwiązania, związane z zapewnieniem dostępności informacji w organizacji mają wpływ cele i potrzeby tej organizacji, wymagania bezpieczeństwa, realizowane procesy biznesowe, wielkość i struktura samej organizacji a także wdrożony system informatyczny.

Uwarunkowania, związane z systemem informatycznym przedsiębiorstwa, to projekt i realizacja sieci komputerowej, wybór metod i narzędzi zdalnego dostępu do zasobów informacyjnych, zapewnienie nieprzerwanego przetwarzania danych, zabezpieczenie zasobów informacyjnych przed wpływem czynników zewnętrznych, działania organizacyjne, związane z zapewnieniem ciągłości procesów biznesowych po awarii lub katastrofie, i wreszcie wykorzystanie nowych technologii sprzętowych i programowych, ułatwiających zapewnienie dostępności informacji.

Dostępność informacji można rozpatrywać na dwóch poziomach: ogólnym i szczegółowym. Poziom ogólny dotyczy analizy dwóch zagadnień:

1. Przygotowanie środowiska sprzętowego i programowego, umożliwiającego realizację czterech podstawowych procesów informacyjnych (pozyskiwania, przechowywania, przetwarzania i udostępniania informacji).
2. Zapewnienie zabezpieczenia tego środowiska przed skutkami złych działań (na poziomie sprzętowym, programowym i organizacyjnym).

Poziom szczegółowy związany jest z przeanalizowaniem konkretnej aplikacji w świetle określonych procesów biznesowych. Do tego etapu odnieść możemy ustalenie:

- jakie będą potrzebne informacje, wymagane przez procesy, (czy zaprojektowane struktury danych zapewniają możliwość uzyskania potrzebnej informacji);
- kto z tych informacji będzie korzystał (czy przygotowane są profile użytkowników, posiadających stosowne uprawnienia);
- czy dostępność informacji skorelowana jest z procesami biznesowymi (czyli analiza czasowa dostępności informacji na żądanie).

Zwykle ostatni z wymienionych punktów jest najbardziej krytyczny.

Z powyższego wywodu wynika, że móc aby odpowiedzieć menedżerowi na temat dostępności konkretnej informacji w konkretnym systemie obsługującym konkretne procesy należy dokonać analizy konkretnego przypadku (w rzeczywistym czasie i środowisku).

I jeszcze jedna istotna kwestia - zależność pomiędzy danymi i informacją. W [Managi96] możemy znaleźć, że informacja, to zestrukturyzowane dane, czyli dane, które zostały uporządkowane: zdefiniowano kategorie informacji i każdy fakt został odniesiony do odpowiedniej kategorii. Z tego wynika, że wystarczającym procesem, umożliwiającym prze-

kształcenie danych w informację jest porządkowanie (bez konieczności ich przetworzenia). Takie podejście zostało wybrane przez autora pracy do prowadzenia dalszych rozważań. Jest to o tyle istotne, że zarówno z punktu widzenia bezpieczeństwa, jak i dostępności, pojęcia danych i informacji możemy traktować ekwiwalentnie, tzn. bezpieczeństwo informacji zapewnimy, gwarantując bezpieczeństwo danych i ich spójność, a dostępność informacji jest zagwarantowana przez dostępność odpowiednich danych, przechowywanych we właściwej bazie danych.

2. Sposoby oceny dostępności

W wielu publikacjach technicznych, jak np. [Bezpie06], [Kobyli05], [Reliab06], [System06], [Wielka05], oraz w materiałach normatywnych, jak to ma miejsce np. w omawianej już normie ISO 27001 [Inform05], dostępności informacji traktowana jest jako jeden z elementów bezpieczeństwa lub niezawodności systemu, stąd też potrzeba posiadania jakiegoś mierzalnego kryterium do jej wyrażenia. Gdyby za [Kobyli05] przyjąć, że dostępność (gotowość) jest atrybutem przybliżonym do niezawodności i określenia te bywają używane wymiennie, wówczas w oparciu o [Albins03], [Bascle98] i [Fenpfl97] dostępność można wyrazić jako procent czasu, w którym system jest sprawny, w postaci następującej zależności:

$$A = \frac{MTTF}{MTTF + MTTR} \times 100\%$$

gdzie A - dostępność (*Availability*),

MTTF - średni czas pomiędzy rozpoczęciem pracy a chwilą utraty przez system sprawności (*Mean Time To Failure*),

MTTR - czas niedostępności, związany z czasem, niezbędnym na naprawę i przywróceniem stanu gotowości (*Mean Time To Repair*).

I chociaż tak zdefiniowany miernik dostępności uwzględnia różne czynniki zewnętrzne, jak np. konsekwencje awarii, jednakże brakuje mu istotnej cechy - nie uwzględnia powiązania z realizowanymi procesami biznesowymi, jak np. wymagany czas reakcji.

W dostępnej literaturze trudno jest znaleźć informacje o kryteriach dostępności. Najczęściej charakterystyka sprowadza się do określenia, że informacja jest mniej czy też bardziej dostępna (lub niedostępna). Jednakże w czasie analizy literatury autor zauważył dwa podejścia, które w tym aspekcie mogą być interesujące. Pierwsze z nich znalazło się w artykule, poświęconym tendencji tworzenia mierzalnych kryteriów [Syskae03]. Otóż w tym artykule proponuje się mierzyć dostępność informacji poprzez efekty, które dzięki tej dostępności osiągamy, lub wyrażone poprzez koszty, których nie ponosimy. Jako przykład wykorzystano dostępności informacji w systemie zarządzania dokumentami organizacji i przeciwstawiane jest podejście jakościowe (gdy przyjmiemy, że dostępność informacji jest aktywem niemierzalnym) podejściu ilościowemu, opierającemu się o mierniki liczbowe. Punktem wyjściowym jest odpowiedź na pytanie "Co jest rozumiane pod hasłem dostępności informacji?" I następnie próba znalezienia ocen mierzalnych przy znalezieniu odpowiedzi, jak np. dostępnością może być skrócenie czasu dostępu do informacji, a wtedy już same różnice czasowe są mierzalną ilością dla której możemy przypisać wartość ekonomiczną. Może się okazać, że dostępność w tym systemie oznacza również, że informacja rzadziej ulega zagubieniu. To także jest mierzalne; np. wtedy gdy ta informacja wpływa na rutynowe

decyzje podejmowane w firmie. Potrafimy wówczas znaleźć ekonomiczną wartość tego usprawnienia poprzez pomiar efektów zredukowania kosztownych błędów utraty tej informacji. Lepsza dostępność informacji skutkuje tym, że mniej jest sytuacji, kiedy utrata informacji powoduje dodatkowe koszty związane z jej odtworzeniem (jak na przykład: powtórne wykonanie rysunków inżynierskich, ponieważ oryginały zaginęły). Czyli zawsze możemy sprowadzić to pojęcie do czegoś konkretniejszego, a przez to mierzalnego.

Drugim podejściem jest ocena parametryczna, zaproponowana przez firmę Hewlett-Packard i wykorzystywana w narzędziu, służącym do oceny stanu bezpieczeństwa i dostępności informacji w przedsiębiorstwie i pozwalającym planować działania, zmierzające do poprawy tego stanu.

3. Parametryczny sposób oceny dostępności informacji

Omawiany sposób wykorzystuje kryteria, opracowane w formie ankiety przez firmę Hewlett-Packard jako Business Continuity and Availability Self-Assessment Tool [Busine06], uzupełnione i uporządkowane przez autora, które z kolei stanowią podstawę zaproponowanej przez autora integralnej oceny stanu dostępności w organizacji. Na każde z pytań należy udzielić jednej z odpowiedzi: "tak/nie/częściowo/nie wiem".

Wymieńmy zatem te najistotniejsze kryteria, które decydują o dostępności:

1. Czy zidentyfikowano, które z procesów biznesowych są najważniejsze i przez jakie zasoby infrastruktury informatycznej są wspierane?
2. Czy zostały określone zagrożenia i niebezpieczeństwa zagrażające krytycznym procesom i zasobom informatycznym?

3. Czy zostały określone parametry ilościowe wpływu awarii lub zniszczenia krytycznych elementów infrastruktury informatycznej na prowadzoną działalność biznesową?
4. Czy zostały zdefiniowane parametry, związane z odtwarzaniem systemu po katastrofie, a mianowicie czas, niezbędny na odtworzenie systemu (RTO) i dopuszczalny poziom utraty aktualnych danych (RPO)?
5. Czy zostały określone poziomy dostępności krytycznych usług infrastruktury informatycznej, które są niezbędne do zapewnienia właściwej realizacji procesów biznesowych?
6. Czy zostały przygotowane plany działań w sytuacjach nagłych zagrożeń (kryzysowych), których celem jest zarządzanie w takich sytuacjach i wznowienie procesów biznesowych?
7. Cy przeprowadzane są regularnie weryfikacje planów działań w sytuacjach kryzysowych, związane ze wszystkimi obszarami działalności przedsiębiorstwa (a nie np. tylko z zasobami informatycznymi)?
8. Czy istnieje udokumentowany plan zapewnienia ciągłości usług informatycznych?
9. Czy plan zapewnienia ciągłości usług informatycznych uwzględnia obsługę systemów i urządzeń zabezpieczeń?
10. Czy istnieje regularnie weryfikowana jasna umowa serwisowa, gwarantująca odpowiedni poziom obsługi?
11. Czy realizowane są pełne zabezpieczenia danych wszystkich krytycznych zasobów informatycznych systemu jako część zdefiniowanej strategii zabezpieczenia i odtwarzania danych?
12. Czy pomieszczenie komputerowe jest zabezpieczone przed fluktuacjami lub zanikiem napięć zasilających, np. przez UPS?

13. Czy wykorzystuje się strukturę klastra lub inne formy redundancji w celu zapewnienia odporności na zagrożenia i awarie, na poziomie, gwarantującym realizację procesów biznesowych?
14. Czy infrastruktura przechowywania danych i wykonywania ich zabezpieczeń spełnia wymagania odnośnie dostępności informacji, uwarunkowanej procesami biznesowymi, a także wymogami RTO/RPO odtwarzania po katastrofie?
15. Czy plan zapewnienia ciągłości usług informatycznych przewiduje procedury, które winny być podjęte w przypadku dużych zniszczeń (np. gdy pomieszczenia nie będą mogły być dostępne przez czas dłuższy niż np. 45 dni)?
16. Czy odpowiednie umowy zapewniają wsparcie najważniejszych kooperantów w przypadku korzystania z nowej lokalizacji, w której odtwarzany jest system po katastrofie?
17. Czy posiadane plany zapewnienia ciągłości usług informatycznych są na bieżąco aktualizowane w celu uwzględnienia zmian i aktualizacji wprowadzanych do infrastruktury czy też instalacji nowych aplikacji w wyniku ich włączenia do ogólnych procedur zarządzania zmianami?
18. Czy wszystkie krytyczne dane są dublowane np. w zapasowym systemie, np. drogą zdalnej replikacji?
19. Czy realizowane są zabezpieczenia danych na taśmach magnetycznych i czy te zabezpieczenia przechowuje się w oddalonych lokalizacjach?
20. Czy są regularnie realizowane testy posiadanych w oddalonych lokalizacjach zabezpieczeń danych drogą ich odtwarzania w systemie?

21. Czy istnieje udokumentowana procedura zgłaszania awarii i problemów do dostawców usług serwisowych, w odniesieniu do zasobów krytycznych także poza normalnymi godzinami pracy?
22. Czy istnieje rezerwowa infrastruktura (np. linie analogowe), zapewniająca łączność w przypadku awarii krytycznych linii lub urządzeń komunikacyjnych?
23. Czy przeprowadzane są regularne testy macierzy dyskowych i przechowywanych na nich danych w celu upewnienia się, że urządzenia pracują właściwie?
24. Czy są zdefiniowane w sposób jasny i jednoznaczny procedury wsparcia w przypadku sytuacji awaryjnych (ang. helpdesk), ukierunkowane na konkretne działania zmierzające do rozwiązania problemu?
25. Czy istnieje i działa zautomatyzowany system, wykrywający stany odbiegające od normy i pojawiające się stany zagrożeń bezpieczeństwa, w celu alarmowania obsługi?
26. Czy zostało zaimplementowane pełne monitorowanie środowiska pracy serwerów (pomieszczenia komputerowego)?
27. Czy istnieje udokumentowany proces eskalacji problemów w przypadku sytuacji trudnych i kryzysowych, kiedy nie można na miejscu znaleźć rozwiązania?

Jeżeli przeanalizujemy powyższe kryteria, to możemy zauważyć, że po pierwsze określają one bezpośrednio zespół metod i środków zapewnienia bezpieczeństwa informacji w przypadku awarii lub katastrofy. Po drugie, podlegające ocenie przedsięwzięcia mogą zostać sklasyfikowane pod względem ważności. Autor proponuje wydzielenie trzech obszarów: konieczne (poz. 1-14), pożądane (poz. 15-23) i wspomagające (24-27). Ta

parametryczna ocena stanowi punkt wyjściowy do zintegrowanej oceny dostępności informacji.

4. Zintegrowana ocena dostępności

Udzielenie rzetelnych odpowiedzi na sformułowane pytania to dopiero początek procesu. W dalszej kolejności należy dokonać oceny stopnia przygotowania organizacji (a przede wszystkim działu IT) do zapewnienia dostępności informacji, najlepiej mając do dyspozycji w miarę obiektywną metodę nie tylko jakościową, ale i ilościową. W tym celu autor proponuje wykorzystać zintegrowaną metodę oceny stanu przygotowania do zapewnienia dostępności informacji, niezbędnej do realizacji procesów biznesowych. Proponowana metoda oceny opiera się o punktowany system odpowiedzi. W pierwszej kolejności odpowiedziom należy przyporządkować określone wartości punktowe (na podstawie wiedzy eksperckiej). Dobrym odwzorowaniem rzeczywistości wydaje się być następująca struktura punktów (Tabela 1):

Tabela 1

Wartości punktowe odpowiedzi

Odpowiedzi	Punkty
Tak	1
Częściowo	0,5
Nie	0,2
Nie wiem	0

Źródło: Opracowanie własne

Kolejny etap związany jest z wprowadzeniem w każdym obszarze funkcjonalnym odpowiednich wag, które wyrażają ważność określonego

kryterium. Na podstawie posiadanego doświadczenia autor proponuje następujący układ (Tabela 2):

Tabela 2

Wagi grup kryteriów

Grupa ważności	Waga
Konieczne	0,5
Pożądane	0,3
Wspomagające	0,2

Źródło: Opracowanie własne

Przeprowadzone ustalenia pozwalają uzyskać wyrażoną liczbowo ocenę (miarę) dostępności informacji w realnych warunkach w odniesieniu do realizowanych procesów biznesowych. Taka ocena uzyskiwana jest w dwóch krokach. Krok pierwszy to wyliczenie rzeczywistej wartości dostępności (kryterium dostępności) według wzoru:

$$A = \sum_{j} (w_j \times \sum_{i} p_{ij})$$

gdzie A - wyliczona dostępność, p_{ij} - wartość punktowa odpowiedzi, dotycząca konkretnego kryterium i w_j - waga określonego poziomu ważności.

Krok drugi służy do oceny, jak bardzo stan aktualny odbiega od stanu, w którym zrealizowane są wszystkie niezbędne przedsięwzięcia, zapewniające dostępność informacji. Ocena ta realizowana jest w odniesieniu do maksymalnej wartości, którą można uzyskać przy przyjętym systemie wartości punktów i wag. Wykorzystywana jest w tym celu następująca zależność:

$$P = \frac{A_{rzecz}}{A_{\max}} \times 100\%$$

gdzie P - aktualny poziom dostępności, A_{rzecz} - rzeczywista wartość wyliczonej dostępności i $A_{\max}$ - maksymalna wartość dostępności przy przyjętych kryteriach.

Podsumowanie

Zaproponowana integralna miara dostępności informacji może być wykorzystywana jako jeden z elementów oceny przygotowania infrastruktury informatycznej organizacji gospodarczej do wymagań, związanych ze skutecznym procesem wspomagania procesu decyzyjnego i jego odporności na szkodliwe oddziaływania zewnętrzne.

Należy podkreślić, że zarówno zaproponowany sposób oceny dostępności, jak i otrzymane z jego pomocą konkretne wartości mają charakter bardzo przybliżony i w praktyce winny być wykorzystywane przez menedżerów służb informatycznych jedynie do oceny przygotowania infrastruktury informatycznej organizacji do zapewnienia dostępności informacji w ramach realizowanych procesów biznesowych i identyfikacji obszarów, wymagających poprawy.

Literatura

[Albins03] Albin S. T.: The Art of Software Architecture - Design Methods and Techniques, Wiley Publishing, Indianapolis 2003.

[Bascle98] Bass L., Clements P., Kazman R.: Software Architecture in Practice, Addison-Wesley, 1998.

[Bezpie06] Bezpieczeństwo informacji, Jason MacKenzie, 2006, http://jmk.pl/jmk/u9.html.

[Busine06] Business Continuity and Availability Self-Assessment Tool, Hewlett-Packard Company, http://h30328.www3.hp.com/ui/forms/Default.aspx, 2006.

[Callag02] Callaghan J.: Inside Intranets & Extranets: Knowledge Management and the Struggle for Power, Palgrave Macmillan, UK 2002.

[Certyf07] Certyfikacja ISO 27001 - Zarządzanie bezpieczeństwem informacji, ISOQUAR CEE Sp. z o.o., portal www.isoquar.pl, Warszawa 2007.

[Damgaa02] Damgaard J.: IT On the Fast Track, Optimize Magazine, September 2002.

[Fenpfl97] Fenton N.E., Pfleeger S.L.: Software Metrics. A Rigorous and Practical Approach, 2nd ed., PWS Publishing Company, Boston 1997.

[Inform05] Information technology - Security techniques - Information security management systems - Requirements, International Standard ISO/IEC 27001, ISO/IEC 2005.

[Kobyli05] Kobyliński A.: Modele jakości produktów i procesów programowych, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2005.

[Managi96] Managing Information, "Color In Color Out" CD, Epson, 1996.

[Michal98] Michalski A.: Uwarunkowania stosowania systemów informatycznych w przedsiębiorstwie, Materiały Konferencyjne Katedry Informatyki i Ekonometrii, Politechnika Śląska, Gliwice 1998.

[Reliab06] Reliability and Availability Basics, EventHelix.com, http://www.eventhelix.com/RealtimeMantra/FaultHandling/reliability_availability_basics.htm, 2006.

[Siejac98] Sierpińska M., Jachna T.: Ocena przedsiębiorstwa według standardów światowych, wydanie drugie, Wydawnictwo Naukowe PWN, Warszawa 1998.

[Syskae03] Syska E.: ROI: Wszystko jest mierzalne, IT Investment Consulting, http://www.it-invest ment.com.pl/index.php?option=com_content&task=view&id=84&Itemid=109, 2003.

[System06] System pojąć a ludzi zrozumieć - recepta na udane wdrożenie, Portal rozwiązań IT w biznesie ERP-view.pl, www.erp-view.pl/ERP/system_poj_a_ludzi_zrozumie_-_recepta_na_udane_wdro_enie__2.html, sierpień 2006.

[Wielka05] Wielka Internetowa Encyklopedia Multimedialna 2006, Onet.pl. 2005.

[Wykorz02] Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych, praca zbiorowa pod red. Andrzeja Michalskiego, Wydawnictwo Politechniki Śląskiej, Gliwice 2002.

Informacje o autorze

Dr inż. Andrzej M. Michalski
Wydział Organizacji i Zarządzania Politechniki Śląskiej
ul. Roosevelta 26-28
41-800 Zabrze - Polska
Numer telefonu +48/32/2777352
e-mail: andrzej.m.michalski@polsl.pl