dr inż. ANDRZEJ MICHALSKI
Centrum Elektryfikacji i Automatyzacji Górnictwa EMAG

Ocena dostępności informacji

Information availability assessment

W artykule przeanalizowano pojęcie i znaczenie dostępności informacji w organizacji gospodarczej oraz zaproponowano zintegrowane kryterium do oceny aktualnej dostępności informacji. Przedstawiono także sposób wykorzystania zaproponowanej oceny w oparciu o realne scenariusze, które dotyczą organizacji, podchodzących w różny sposób do zagadnień zapewnienia dostępności informacji. Podane zostały uzyskane wartości zintegrowanej oceny dla poszczególnych scenariuszy.

In the article the author analyzed the concept and significance of information availability in an organization and proposed an integrated criterion for assessing the current availability of information. Additionally, the article presents the method to use the proposed assessment on the basis of real scenarios with respect to organizations where the issues of information availability are approached in different ways. Finally, the integrated assessment values for particular scenarios are given.

1. WPROWADZENIE

W dzisiejszych czasach w większości organizacji gospodarczych informacja należy do najważniejszych zasobów. Bezpieczeństwo posiadanej i wymienianej informacji ma bezpośredni wpływ na realizację celu organizacji, w tym osiąganie przychodu z prowadzonej działalności, zachowanie płynności finansowej oraz kreowanie pozytywnego wizerunku marketingowego (pozycji na rynku) [7]. Wynika z tego, że niezbędna jest właściwa polityka ochrony informacji oraz zapewnienia jej dostępności, którą obecnie wyznacza norma ISO 27001. Norma ta należy do grupy standardów[1], wywodzących się z brytyjskiego standardu bezpieczeństwa BS 7799. W szczególności Polska przyjęła w roku 2003 normę ISO/IEC 17799 jako PN-ISO/IEC 1799:2003. Zawiera ona techniczne aspekty implementacji systemów bezpieczeństwa. W styczniu 2007 dokument ten został znowelizowany jako PN-ISO/IEC 17799:2007. Aby umożliwić audytowanie

[1] Wywód o historii normy pochodzi z materiałów dr. hab. inż. S. Stanka, prof. AE, dotąd niepublikowanych, wykorzystany w [16] za zgodą autora i tu ponownie przytoczony.

1. INTRODUCTION

The majority of today's organizations treat information as their most important asset. The security of information, both possessed and exchanged, directly influences the level of the organization's income, financial liquidity, and development of the organization's positive image on the market (position on the market) [7]. For this reason, it is indispensable to have a proper information security policy and to provide the availability of information, just as it is stipulated by the current ISO 27001 standard. This standard belongs to a group of standards[1], originating from the British standard BS 7799. In 2003 Poland adopted the ISO/IEC 17799 standard as PN-ISO/IEC 1799:2003. This standard contains technical aspects of security systems implementation. In January 2007 the document was updated as PN-ISO/IEC 17799:2007. In order to enable to audit the systems in compliance with PN-ISO/IEC 17799:2003,

[1] The presentation of the standard history was taken from the yet unpublished materials of S. Stanek, Senior D Sc, professor of the Academy of Economics. The presentation had been previously used in [16], after the author's consent, and quoted again in the present article.

systemów na zgodność z PN-ISO/IEC 17799:2003, została wprowadzona norma PN-I 07799-2:2005, będąca tłumaczeniem oryginalnego standardu BS 7799-2, zaadaptowanego w roku 2005 jako ISO/IEC 27001. Obecnie, po przetłumaczeniu na język polski, obowiązuje jako PN-ISO/IEC 27001:2007 [22] oraz zastępuje PN-I 07799-2:2005 [12]. Drugi ważny dla problematyki informacji zestaw norm ISO/IEC 13335 przyjęto nazywać skrótem GMITS (*Guidelines for Management of IT Security*) [11].

2. POJĘCIE DOSTĘPNOŚCI INFORMACJI

W dokumentach normalizacyjnych pojęcie dostępności (ang. *availability*), z jednej strony, definiowane jest na poziomie funkcjonalnym. Możemy zatem spotkać takie określenia:

- zapewnienie, że osoby upoważnione mają dostęp do informacji i związanych z nią aktywów wtedy, gdy jest to potrzebne [12], [21];
- właściwość bycia dostępnym i możliwym do wykorzystania na żądanie w założonym czasie przez autoryzowany podmiot [11].

Określenia te związane są bezpośrednio z pojęciem zapewnienia ciągłości biznesowej (ang. *BCM - Business Continuity Management*). Działania w tym zakresie regulowane są głównie przez normy [5], [13] i [18].

Z drugiej strony, pojęcie dostępności traktowane jest jako składowa systemu bezpieczeństwa informacji, np. norma ISO 27001:2007 ([22] wraz materiałami dodatkowymi [23]) wyróżnia trzy podstawowe obszary (płaszczyzny), które składają się na bezpieczeństwo informacji:

- poufność – gwarantująca, że dostęp do informacji posiadają tylko osoby upoważnione,
- integralność – czyli dokładność i kompletność informacji, z uwzględnieniem metody jej przetwarzania,
- dostępność – która zapewnia, że upoważnione osoby mają dostęp do potrzebnej im informacji (por. także w [11]).

Każdy z tych obszarów wymaga stosowania odpowiednich metod i technologii. W niniejszym artykule autor postanowił skupić się na zagadnieniu dostępności informacji. Bezpośrednim impulsem napisania pracy stała się chęć pogłębienia zagadnienia dostępności informacji w organizacji, który to obszar został w normie – zdaniem autora – potraktowany zbyt pobieżnie, i to zarówno w zakresie podanej definicji, jak i w warstwie treściowej. Otóż stwierdzenie, że z dostępnością informacji mamy do czynienia wtedy, gdy „uprawnione osoby mają do niej dostęp", nie

the PN-I 07799-2:2005 standard was implemented which is the translation of the original BS 7799-2, adopted in 2005 as ISO/IEC 27001. Now, after having been translated into Polish, the standard is valid as PN-ISO/IEC 27001:2007 [22] and has replaced PN-I 07799-2:2005 [12]. The second group of standards which are important with respect to information security are GMITS (*Guidelines for Management of IT Security*) [11].

2. INFORMATION AVAILABILITY CONCEPT

Some standards define availability on a functional level. Thus it is possible to find the following definitions of the concept:

- the assurance that authorized persons have access to information and related assets at the time when it is needed [12], [21];
- the quality of being available and possible to use on demand at the given time by an authorized subject [11].

These definitions are directly related to the concept of business continuity management (BCM). The issues of BCM are stipulated by the standards [5], [13] and [18].

On the other hand, the concept of availability can be defined as an element of an information security system. Such a definition is provided, for example, by ISO 27001:2007 ([22] with related documents [23]) which identifies three basic areas (levels) making up information security:

- confidentiality – which guarantees that only authorized persons have access to information,
- integrity – understood as accuracy and completeness, including the method of information processing,
- availability – which ensures that only authorized persons have access to the information they need (see also [11]).

Each of these areas requires that suitable methods and technologies should be applied. In this article the author decided to focus on the issue of information availability. The direct motivation to write the article was the desire to extend the issue of information availability in the organization as, in the author's opinion, the standard presents this concept in a slightly superficial manner, with respect to both the definition and the contents. Thus, the statement that we deal with information availability when "authorized persons have access to information" does not take into account, for example, the fact that the infor-

uwzględnia np. faktu, że informacja musi być dostępna w czasie, zdefiniowanym przez realizowane procesy biznesowe. Trzeba także zauważyć, że obiektywnie istniejąca informacja może się okazać niedostępna w wyniku niepoprawnie sformułowanego żądania dostępu.

We współczesnych warunkach zarządzania organizacją gospodarczą dostępność informacji (zasobów informacyjnych) nabiera kluczowego znaczenia i podstawowym sposobem, mającym ją zapewnić, jest wdrożenie systemu informatycznego [5], [25]. Wtedy dostępność informacji traktować możemy zarówno jako stan, jak i cechę systemu informatycznego organizacji.

3. OCENA DOSTĘPNOŚCI INFORMACJI

Ponieważ system informatyczny powinien zapewniać dostęp do właściwej informacji przez właściwą osobę we właściwym czasie, przyjęto, że dostępność informacji ma miejsce wówczas, gdy zostaje zaspokojone każde poprawnie sformułowane przez uprawnionego użytkownika żądanie dostępu do informacji, związanej z działalnością organizacji w czasie, wynikającym z realizacji procesów biznesowych[2] [16]. Jak widać, problem ten nie sprowadza się wyłącznie do zabezpieczenia przed utratą informacji. Mając to na uwadze możemy wydzielić dwa etapy (tryby działania):

1. Dostęp do informacji, gdy wszystko postępuje zgodnie z planem i nie występują żadne przeszkody czy też zagrożenia zewnętrzne (odpowiada to minimalnym nakładom, które zapewniają realizację procesów biznesowych).
2. Dostęp do informacji w przypadku wystąpienia awarii, zagrożeń zewnętrznych lub innych działań, mogących uniemożliwić realizację głównego postulatu – dostępności informacji (związane jest to z dodatkowymi przedsięwzięciami organizacyjnymi i nakładami na infrastrukturę).

Aby organizacja mogła poprawnie funkcjonować, niezbędne jest zidentyfikowanie wielu działań i zarządzanie nimi w sposób właściwy, przy czym u podstaw tych wszystkich przedsięwzięć leży ocena aktualnej dostępności informacji w organizacji. I tu pojawia się problem – jak oceniać tę dostępność?

W publikacjach technicznych, jak np. [3], [14], [17], [20] i [24] oraz w materiałach normatywnych,

[2] Przez pojęcie proces biznesowy rozumieć tu będziemy serię kroków (najczęściej powtarzalnych) wykonywanych przez organizację w celu uzyskania pożądanego efektu, związanego z celami biznesowymi organizacji [8], które mogą zostać wyodrębnione np. w oparciu o model Zachmanna [26].

mation has to be available at certain duration of time defined by the conducted business processes. It is also important to note that the objectively existing information may prove to be unavailable due to improperly formulated access demand.

In modern conditions of organization management the availability of information (information assets) acquires key significance and the basic way to ensure it is to implement an IT system [5], [25]. Then information availability can be treated both as a condition and a quality of the organization's IT system.

3. INFORMATION AVAILABILITY ASSESSMENT

The IT system should ensure access to proper information by a proper person and at a proper time. Therefore, it was assumed that information availability occurs when each properly formulated request, issued by an authorized user, to access the information related to the organization's operations at a certain time resulting from the execution of business processes is satisfied.[2] [16]. Obviously, this issue is not limited to the protection against information loss. Having this in mind, it is possible to define two stages (operation modes):

1. Access to information when all processes run according to the plan and there are no obstacles or external threats (this corresponds to minimum expenditure which ensures that business processes are fulfilled).
2. Access to information in the case of breakdowns, external threats or other activities which may disable the fulfillment of the main requirement – information availability (this is related to additional organizational undertakings and expenditure on infrastructure).

In order that the organization could function properly, it is necessary to identify many operations and to manage them in a suitable manner. Still, all these undertakings have at their basis the assessment of the current availability of information in the organization. And here an issue arises – how this availability can be assessed.

In technical publications, e.g. [3], [14], [17], [20], [24], and in standards, as in the ISO 27001 [12] and

[2] Business process is understood here as a series of steps (most frequently repeated) taken by the organization to achieve the desired effect with respect to its business goals [8] which can be identified, for example, on the basis of the Zachmann model [26].

jak to ma miejsce np. w omawianej już normie ISO 27001 [12] i [22], dostępność informacji traktowana jest jako jeden z elementów bezpieczeństwa lub niezawodności systemu, stąd też potrzeba posiadania jakiegoś mierzalnego kryterium do jej wyrażenia. Gdyby za [14] przyjąć, że dostępność (gotowość) jest atrybutem przybliżonym do niezawodności i określenia te bywają używane wymiennie, wówczas w oparciu o [1], [2] i [9] dostępność można wyrazić jako procent czasu, w którym system jest sprawny, w postaci następującej zależności (1):

$$A = \frac{MTTF}{MTTF + MTTR} \times 100\% \qquad (1)$$

gdzie:

A – dostępność,
MTTF – średni czas pomiędzy rozpoczęciem pracy a chwilą utraty przez system sprawności,
MTTR – czas niedostępności, związany z czasem, niezbędnym na naprawę i przywróceniem stanu gotowości.

I chociaż tak zdefiniowana miara dostępności uwzględnia różne czynniki zewnętrzne, jak np. konsekwencje awarii, jednakże brakuje jej istotnej cechy – nie uwzględnia powiązania z realizowanymi procesami biznesowymi, jak np. wymagany czas reakcji. Dlatego też w dalszej części artykułu zostanie zaproponowana metoda oceny dostępności informacji w oparciu o zintegrowaną miarę, wykorzystującą wskaźniki parametryczne.

4. KRYTERIA DOSTĘPNOŚCI

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 [19]. Otóż proponuje się w nim mierzyć dostępność informacji poprzez efekty, które dzięki tej dostępności osiągamy, lub poprzez koszty, których nie ponosimy.

[22] mentioned above, information availability is defined as one of the elements of the system security or reliability. Thus there is a need for a measurable criterion to express it. If, following [14], we assume that availability (readiness) is an attribute close to reliability and these concepts are used interchangeably, then, based on [1], [2] and [9], availability can be expressed as the percentage of time in which the system remains efficient, in the form of the following dependence (1):

$$A = \frac{MTTF}{MTTF + MTTR} \times 100\% \qquad (1)$$

where:

A – availability,
MTTF – mean time to failure,
MTTR – mean time to repair.

Although the availability measure defined in such a manner takes into account different external factors, such as, for example, the consequences of a breakdown, it lacks one important quality – it does not take into account the relations with the conducted business processes, e.g. the required time of reaction. Therefore, further in this article, there will be a method proposed to assess the availability of information with the use of parametric indicators.

4. AVAILABILITY CRITERIA

In the publications available on the subject it is difficult to find information about availability criteria. Most frequently, the characteristics is limited to the description that certain information is more or less available (or unavailable). However, while analyzing the literature, the author observed two approaches which might be interesting in this aspect. The first one was found in an article devoted to the tendency to create measurable criteria [19]. The approach presented in that article proposes to measure information availability through the effects which can be achieved due to this availability or through the costs which are not borne thanks to it.

Tabela 1

Kryteria dostępności informacji

Nr	Opis kryterium
1.	Identyfikacja, które z procesów biznesowych są najważniejsze i przez jakie zasoby infrastruktury informatycznej są wspierane.
2.	Określenie niebezpieczeństw, zagrażających krytycznym procesom i zasobom informatycznym.
3.	Określenie parametrów ilościowych wpływu awarii lub zniszczenia krytycznych elementów infrastruktury informatycznej na prowadzoną działalność biznesową. Uwzględnić należy zarówno koszty bezpośrednie, jak utrata zamówień czy przestoje pracowników, jak i koszty pośrednie: reputacja na rynku, zdolność kredytowa, kurs akcji na giełdzie.
4.	Zdefiniowanie parametrów, związanych z odtwarzaniem systemu po katastrofie, a mianowicie czasu, niezbędnego na odtworzenie systemu (RTO) i dopuszczalnego poziomu utraty aktualnych danych (RPO).
5.	Określenie poziomów dostępności krytycznych usług infrastruktury informatycznej, które są niezbędne do zapewnienia właściwej realizacji procesów biznesowych.
6.	Przygotowanie planów działań w sytuacjach nagłych zagrożeń (kryzysowych), których celem jest zarządzanie w takich sytuacjach i wznowienie procesów biznesowych.
7.	Regularna weryfikacja planów działań w sytuacjach kryzysowych, związana ze wszystkimi obszarami działalności przedsiębiorstwa (a nie tylko z zasobami informatycznymi).
8.	Udokumentowany plan zapewnienia ciągłości usług informatycznych (odtwarzania systemu po katastrofie).
9.	Uwzględnienie obsługi systemów i urządzeń zabezpieczeń w planie zapewnienia ciągłości usług informatycznych.
10.	Uwzględnienie w planie zapewnienia ciągłości usług informatycznych procedur, które winny być podjęte w przypadku dużych zniszczeń (np. gdy pomieszczenia nie będą mogły być dostępne przez czas dłuższy niż 45 dni).
11.	Istnienie umów, zapewniających wsparcie najważniejszych kooperantów w przypadku korzystania z nowej lokalizacji, w której odtwarzany jest system po katastrofie.
12.	Zawarcie regularnie weryfikowanej jasnej umowy serwisowej, gwarantującej odpowiedni poziom obsługi.
13.	Wykonywanie pełnego zabezpieczenia (ang. *backup*) danych wszystkich krytycznych zasobów informatycznych systemu jako części zdefiniowanej strategii zabezpieczenia i odtwarzania danych.
14.	Dublowanie wszystkich krytycznych danych np. w zapasowym systemie, czy to drogą zdalnej replikacji, czy też wykorzystując nośniki taśmowe.
15.	Realizacja zabezpieczeń danych na taśmach magnetycznych i przechowywanie zabezpieczeń w oddalonych lokalizacjach.
16.	Realizacja regularnych testów posiadanych w oddalonych lokalizacjach zabezpieczeń danych drogą ich odtwarzania w systemie.
17.	Aktualizacja na bieżąco posiadanych planów zapewnienia ciągłości usług informatycznych w celu uwzględnienia zmian i aktualizacji wprowadzanych do infrastruktury czy też instalacji nowych aplikacji w wyniku ich włączenia do ogólnych procedur zarządzania zmianami.
18.	Zdefiniowanie w sposób jasny i jednoznaczny procedury wsparcia w przypadku sytuacji awaryjnych (ang. *helpdesk*), ukierunkowanej na konkretne działania zmierzające do rozwiązania problemu.
19.	Udokumentowana procedura zgłaszania awarii i problemów do dostawców usług serwisowych, w odniesieniu do zasobów krytycznych, także poza normalnymi godzinami pracy.
20.	Zaimplementowanie pełnego monitorowania środowiska pracy serwerów (pomieszczenia komputerowego).
21.	Zabezpieczenie pomieszczenia komputerowego przed fluktuacjami lub zanikiem napięć zasilających (np. przez UPS).
22.	Przygotowanie rezerwowej infrastruktury (np. linii analogowych), zapewniającej łączność w przypadku awarii krytycznych linii lub urządzeń komunikacyjnych.
23.	Wykorzystanie struktury klastra lub innych form redundancji w celu zapewnienia odporności na zagrożenia i awarie, na poziomie, gwarantującym realizację procesów biznesowych.
24.	Zapewnienie, aby infrastruktura przechowywania danych i wykonywania ich zabezpieczeń spełniała wymagania dotyczące dostępności informacji, uwarunkowanej procesami biznesowymi, a także wymogami RTO/RPO odtwarzania po katastrofie.
25.	Przeprowadzanie regularnych testów macierzy dyskowych i danych, które są w nich przechowywane w celu upewnienia się, że urządzenia pracują właściwie.
26.	Wdrożenie sprawnego zautomatyzowanego systemu, wykrywającego stany odbiegające od normy i pojawiające się stany zagrożeń bezpieczeństwa, w celu alarmowania obsługi.
27.	Opracowanie udokumentowanego procesu eskalacji problemów w przypadku sytuacji trudnych i kryzysowych, kiedy nie można na miejscu znaleźć rozwiązania.

Źródło: Opracowanie własne na podstawie [15] i [16]

Table 1

Information availability criteria

No	Criterion description
1.	Identification which business processes are the most important and which IT assets they are supported by.
2.	Determining the threats to critical processes and IT assets.
3.	Determining quantity parameters of the influence of breakdowns or damages done to critical elements of IT infrastructure on the organization's business operations. It is necessary to take into account both direct costs, such as the loss of business orders or the occurrence of work standstills, and indirect costs, such as the loss of good reputation on the market, creditworthiness, and share price at a stock exchange.
4.	Defining parameters related to the system recovery after a disaster, i.e. the Recovery Time Objective (RTO) – the duration of time in which the system must be restored, and the Recovery Point Objective (RPO) – the acceptable amount of data loss.
5.	Determining availability levels of these IT infrastructure critical services which are indispensable to ensure proper fulfillment of business processes.
6.	Preparing operation plans in emergency (crisis) situations in order to provide proper management in such situations and to resume business processes.
7.	Regular verification of emergency plans with respect to all operations of the organization (not only with respect to IT assets).
8.	A documented plan of business continuity assurance of IT services (system recovery after a disaster).
9.	Including the operation of security systems and devices in the IT services business continuity plan.
10.	Including in the IT services business continuity plan the procedures which should be undertaken in the case of big disasters (e.g. when certain rooms are not available for more than 45 days).
11.	Agreements which support the key partners in the case of using a new location where the system is recovered after the disaster.
12.	A clear and regularly verified service agreement which guarantees a suitable service level.
13.	Providing full data backup of all critical IT assets of the system as a part of the defined strategy of data protection and recovery.
14.	Replication of all critical data, for example in a spare system, either by remote replication or with the use of tape data carriers.
15.	Data protection by backup on magnetic tapes and storage in remote locations.
16.	Regular tests of data protection in remote locations through backup recovery procedures in the system.
17.	Update of IT services business continuity plans in order to take into account changes and upgrades to the infrastructure, or installation of new applications which have been included into the overall change management procedures.
18.	Defining clearly help desk procedures in the form of concrete operations aimed at solving a problem.
19.	A documented procedure of reporting breakdowns and problems to maintenance service providers with respect to critical assets, also after regular working hours.
20.	Full monitoring of the servers working environment (computer room).
21.	Protection of the computer room against power supply fluctuations or shutdowns (e.g. by a UPS).
22.	Preparing spare infrastructure (e.g. analogue lines) to ensure communication in the case of a breakdown of critical telecommunications lines or equipment.
23.	Using the cluster structure or other redundant forms to provide resistance to threats and breakdowns at a level which will guarantee the fulfillment of business processes.
24.	Ensuring that the data storage and protection infrastructure meets the requirements of information availability with respect to business processes and RTO/RPO requirements of recovery after a disaster.
25.	Carrying out regular tests of disk arrays and data which are stored on them in order to ensure that the equipment works properly.
26.	Implementation of an efficient automated system to detect abnormal states and threats to security in order to alert the servicing personnel.
27.	Preparing and documenting a problem escalation process to be used in difficult and crisis situations when a solution cannot be found on the spot.

Source: Author's own study based on [15] and [16]

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. Narzędzie w formie ankiety nosi nazwę *Business Continuity and Availability Self-Assessment Tool* [3]. Ankieta zawiera szereg pytań; na każde z nich należy udzielić jednej z odpowiedzi: [tak | nie | częściowo | nie wiem] i ich celem jest ustalenie aktualnego stanu bezpieczeństwa i dostępności zasobów informacyjnych firmy. W dalszej części artykułu autor oparł się na tej właśnie parametrycznej ocenie, która abstrahuje od rodzaju realizowanych procesów biznesowych, a przez to może być szeroko stosowana. Jako podstawę przyjęto zbiór pytań wspomnianego narzędzia Hewlett-Packard, który został przez autora rozszerzony i uporządkowany (tab. 1) [15], [16].

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, mogą one być sklasyfikowane zarówno pod kątem obszaru funkcjonalnego, jak i znaczenia (ważności) dla zapewnienia dostępności. W zakresie funkcjonalności można wydzielić np. następujące obszary:

- identyfikacja czynników,
- przedsięwzięcia, zapewniające bezpieczeństwo informacji,
- procedury awaryjne.

5. ZINTEGROWANA METODA OCENY DOSTĘPNOŚCI INFORMACJI

Udzielenie rzetelnych odpowiedzi na pytania, dotyczące spełnienia kryteriów, 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 na systemie punktowym, związanym z odpowiedziami, w jakim stopniu zrealizowane są kryteria, które zostały podane w poprzednim punkcie. W pierwszej kolejności tym odpowiedziom należy przy-

The second approach is parametric assessment proposed by Hewlett-Packard and applied in the tool which evaluates the state of information security and availability in the organization and allows to plan operations to improve this state. The tool has a form of a questionnaire and is called *Business Continuity and Availability Self-Assessment Tool* [3]. The questionnaire contains a number of questions which should be answered with one answer only [yes | no | partially | don't know]. The questions are to determine the current state of security and availability of the organization's information assets. In the further part of the present article the author based his reasoning on this parametric evaluation which disregards the types of conducted business process and, for this reason, can be widely applied. The set of questions of the above mentioned tool by Hewlett-Packard was adopted as the basis, still it was extended and organized by the author (table 1) [15], [16].

If we analyze the above criteria we can observe that, firstly, they determine directly the set of methods and means to ensure information security in the case of a breakdown or disaster. Secondly, they can be classified in terms of both their functional area and significance (importance) for availability assurance. In terms of functionality it is possible to define, for example, the following areas:

- identification of factors,
- undertakings which ensure information security,
- emergency procedures.

5. INTEGRATED METHOD OF INFORMATION AVAILABILITY ASSESSMENT

To give fair answers to the questions about the requirements fulfillment is just the beginning of the process. Next, it is necessary to assess the level of the organization's (especially its IT department's) preparation to information availability assurance. Here, an objective method should be at hand, not only a qualitative method but also a quantitative one. To achieve this, the author proposes to use an integrated method to assess how the organization is prepared to ensure the availability of information indispensable to run its business processes.

The proposed method is based on a system of scores granted for particular answers which show to what extent the criteria described in the previous section are fulfilled. First, it is necessary to assign certain scores to the answers (based on the expert's

porządkować określone wartości punktowe (na podstawie wiedzy eksperckiej). Dobrym odwzorowaniem rzeczywistości wydaje się być następująca struktura punktów (tab. 2):

Tabela 2

Wartości punktowe odpowiedzi

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

Źródło: [16]

Kolejny etap związany jest z wprowadzeniem w każdym obszarze funkcjonalnym odpowiednich wag, które wyrażają ważność danego kryterium. I chociaż wagi mają charakter subiektywny, zależny od oceny menedżera – jak określony poziom wpływa na całość przedsięwzięć zapewnienia dostępności informacji, należy zauważyć, że zarówno zbytnie spłaszczenie, jak i przesadne rozróżnienie poziomów ważności jest niepożądane. Na podstawie posiadanego doświadczenia autor proponuje następujący układ (tab. 3):

Tabela 3

Wagi grup kryteriów

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

Źródło: [16]

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 (2):

$$A = \sum_j (w_j \times \sum_i p_{ij}) \qquad (2)$$

gdzie
A – wyliczona dostępność,
p_{ij} – wartość punktowa odpowiedzi, dotycząca konkretnego kryterium,
w_j – waga określonego poziomu ważności,
i – kolejne kryterium w ramach poziomu ważności j,
j – grupa kryteriów o określonym poziomie ważności.

knowledge). The following structure of scores seems to be a good representation of reality (table 2):

Table 2

Scores for particular answers

Answer	Score
Yes	1
Partially	0.5
No	0.2
Don't know	0

Source: [16]

The next stage is to introduce into each functional area a suitable weight which expresses the importance of a given criterion. Though the weights have
a subjective character, depending on how the manager evaluates the influence of a certain level on the whole of undertakings aimed at providing information availability, it is important to note that neither too much flattening nor too much differentiation of levels is desirable. Based on his experience, the author proposes the following (table 3):

Table 3

Weights of criteria groups

Group of importance	Significance
Necessary	0.5
Desirable	0.3
Supporting	0.2

Source: [16]

The established results allow to obtain a numerically expressed assessment (measure) of information availability in real conditions with respect to conducted business processes. Such assessment is obtained in two steps. The first step is to calculate the real value of availability (availability criterion) according to the following formula (2):

$$A = \sum_j (w_j \times \sum_i p_{ij}) \qquad (2)$$

where
A – calculated availability,
p_{ij} – score value of the answer with respect to a particular criterion,
w_j – weight of a particular importance level,
i – successive criterion within an importance level j,
j – group of criteria with a determined importance level.

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. Może być wykorzystywana w tym celu ocena procentowa (3):

$$P = \frac{A_{rzecz}}{A_{\max}} \times 100\% \qquad (3)$$

gdzie
P – aktualny poziom dostępności,
A_{rzecz} – rzeczywista wartość wyliczonej dostępności,
A_{max} – maksymalna wartość dostępności przy przyjętych kryteriach.

Należy tu z całą mocą podkreślić, że zarówno zaproponowany sposób oceny dostępności, jak i otrzymane konkretne wartości mają charakter bardzo przybliżony i w praktyce winny być wykorzystywane jedynie do oceny przygotowania infrastruktury informatycznej organizacji do zapewnienia dostępności informacji i identyfikacji obszarów, wymagających poprawy.

6. PRZYKŁAD WYKORZYSTANIA W PRAKTYCE

Ilustracją wykorzystania zaproponowanej metody niech będzie symulacja kilku konkretnych sytuacji, w jakiej może znajdować się infrastruktura informatyczna organizacji. Po pierwsze, na podstawie oceny eksperckiej, dokonano klasyfikacji poszczególnych kryteriów (tab. 4).

Tabela 4

Klasyfikacja kryteriów dostępności informacji

Ważność	Kryteria
Konieczne	1,2,3,4,5,6,7,8,9,12,13,21,23,24
Pożądane	10,11,14,15,16,17,19,22,25
Wspomagające	18,20,26,27

Źródło: [Opracowanie własne]

Następnie każdą sytuację ujęto w tzw. scenariusz, określający określony stan przygotowania organizacji do zapewnienia dostępności informacji (tab. 5), po czym na podstawie wzoru (2) wyliczono wartość dostępności informacji A_{rzecz} w każdym z przypadków.

The second step is to evaluate how the current state differs from the state in which all indispensable undertakings are conducted to ensure information availability. This assessment is carried out with respect to the maximum value which can be achieved at an adopted system of scores and significances. To achieve this, it is possible to use percentage assessment (3):

$$P = \frac{A_{rzecz}}{A_{\max}} \times 100\% \qquad (3)$$

where:
P – current level of availability,
A_{rzecz} – real value of calculated availability,
A_{max} – maximum value of calculated availability at the used criteria.

Here it is necessary to state clearly that both the proposed manner of availability assessment and the obtained concrete values are approximate. Thus, in practice, they should be used only to assess how the organization's IT infrastructure is prepared to ensure information availability and to identify areas which need improvement.

6. APPLICATION IN PRACTICE – CASE STUDY

To illustrate the use of the proposed method let us simulate several concrete situations in which the organization's IT infrastructure can be. First, based on the expert's evaluation, the classification of particular criteria was carried out (table 4).

Table 4

Importance groups of criteria

Importance	Criteria
Necessary	1,2,3,4,5,6,7,8,9,12,13,21,23,24
Desirable	10,11,14,15,16,17,19,22,25
Supporting	18,20,26,27

Source: [Author's own study]

Then each situation was expressed by the so called scenario which determines a particular state of the organization's preparation for information availability assurance (table 5). Finally, based on the formula (2) the value of information availability A_{rzecz} was calculated in each case.

Tabela 5/Table 5

Praktyczne scenariusze
Practical scenarios

Nr kryterium / No of criterion	Scen1	Scen2	Scen3	Scen4	Scen5	Scen6
1	t	n	t	t	t	t
2	t	n	t	t	t	t
3	t	n	t	t	t	n
4	t	n	t	t	t	?
5	t	n	t	t	t	n
6	t	t	t	t	t	t
7	n	t	t	t	t	?
8	t	t	t	t	t	t
9	t	t	t	t	t	t
10	t	n	n	t	t	c
11	?	n	n	t	t	t
12	?	t	t	t	t	t
13	t	t	t	t	t	c
14	t	t	n	t	t	?
15	t	t	n	t	t	c
16	t	t	n	t	t	n
17	n	t	n	t	t	t
18	t	n	n	n	t	t
19	t	n	n	t	t	c
20	t	t	n	n	t	n
21	t	t	t	t	t	t
22	t	t	n	t	t	?
23	t	t	t	t	t	t
24	t	t	t	t	t	c
25	t	n	n	t	t	c
26	?	n	n	n	t	c
27	?	n	n	n	t	t
A_{rzecz}	**8,66**	**7,06**	**7,70**	**9,86**	**10,50**	**6,50**
P	**82,48%**	**67,24%**	**73,33%**	**93,90%**	**100,00%**	**61,90%**

Źródło: [Opracowanie własne]
Source: [Author's own study]

Wykorzystane w tabeli symbole oznaczają: t – kryterium jest spełnione w pełni, c – kryterium jest spełnione częściowo, n – kryterium nie jest spełnione, ? – brak wiedzy na ten temat. Natomiast kolejne scenariusze odpowiadają następującym sytuacjom:

Scen1 Organizacja wdrożyła bardzo dobrze przygotowane przedsięwzięcia i procedury, które jednakże uległy skostnieniu (nie są aktualizowane).).

Scen2 Sytuacja, w której skupiono się na zapewnieniu bezpieczeństwa informacji w oparciu o typowe metody, bez przeprowadzania rozeznania procesów biznesowych oraz bez wprowadzania rozbudowanych procedur awaryjnych.

Scen3 Ze względów ekonomicznych (minimalizacja kosztów) zrealizowano jedynie niezbędne przedsięwzięcia, związane z dostępnością informacji.

The symbols in the table stand for: t – criterion fully fulfilled, c – criterion partly fulfilled, n – criterion not fulfilled, ? – no information on the subject. The successive scenarios correspond to the following situations:

Scen1 The organization implemented very well prepared undertakings and procedures but they are now outdated (have not bee updated).

Scen2 The organization focused on information security based on typical methods with no research of business processes and without any extended emergency procedures.

Scen3 Due to economic reasons (costs minimization) only indispensable undertakings to ensure information availability were carried out.

Scen4 Sytuacja jak w Scen3, gdzie wraz z poprawą sytuacji finansowej wdrożono przedsięwzięcia pożądane.

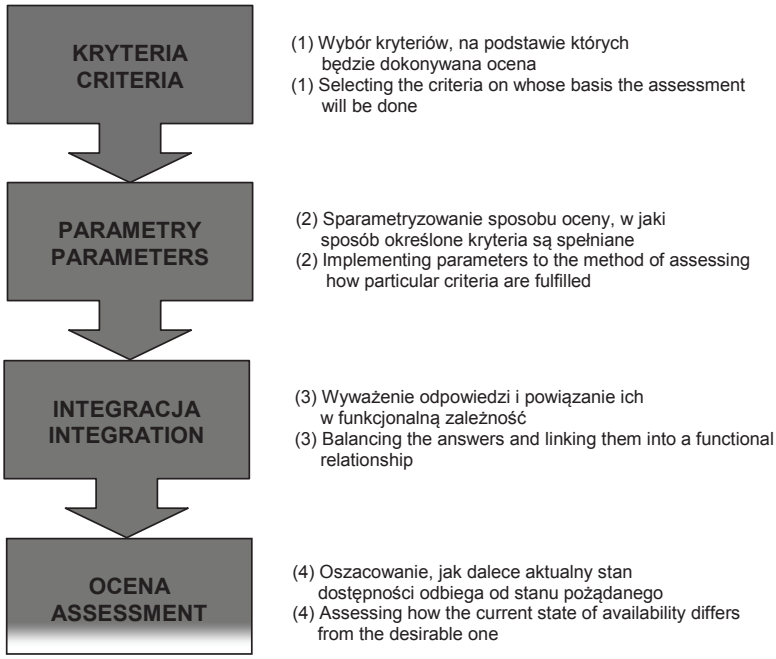
Scen5 Sytuacja najbardziej pożądana, gdy zrealizowane są wszystkie przedsięwzięcia, zapewniające dostępność informacji (maksymalna wartość oceny dostępności).

Scen6 Sytuacja typowa w przeciętnym przedsiębiorstwie, gdzie stosuje się tradycyjne podejście do zagadnień bezpieczeństwa.

Scen4 A situation like in Scen3 where with better financial standing the desirable undertakings were implemented.

Scen5 The most desirable situation when all undertakings to ensure information availability are fulfilled (maximum value of availability assessment).

Scen6 A typical situation in a typical organization where a traditional approach to security issues is used.



Rys. 1. Parametryczna metoda ocena dostępności informacji [16]
Fig. 1. Parametric method of information availability assessment [16]

Pozycja tabeli „P", wyliczona w oparciu o zależność (3) określa, jak znacznie dany scenariusz odbiega od sytuacji, w której wszystkie przedsięwzięcia, związane z zapewnieniem dostępności informacji zostały zrealizowane, czyli od scenariusza, który w danych warunkach posiada największą wartość oceny dostępności. Jest to zarazem wskazówka, ile jeszcze pozostało do zrobienia w tej kwestii.

The "P" position in the table, calculated on the basis of the equation (3), determines how much the given scenario differs from the situation in which all undertakings related to information availability assurance have been fulfilled, i.e. from the scenario which, in the given conditions, has the highest value of availability assessment. This also indicates how much there is to be done in this matter.

7. PODSUMOWANIE

Na dostępność informacji w organizacji możemy wpływać poprzez mechanizmy techniczne (sprzęt i oprogramowanie) oraz organizacyjne (planowanie i procedury). W celu identyfikacji niezbędnych działań zaproponowano ekspercką parametryczną ocenę

7. CONCLUSIONS

The information availability in an organization can be influenced by technical (hardware and software) and organizational (plans and procedures) mechanisms. In order to identify indispensable operations, the expert parametric assessment of information

dostępności informacji na podstawie zintegrowanego kryterium ilościowego. Metoda ta posiada strukturę modułową (rys. 1), co pozwala w łatwy sposób dostosowywać ją do konkretnych okoliczności i rozwijać w miarę potrzeb. Każdy z modułów, będący kolejnym etapem przeprowadzanej oceny, wykorzystuje wyniki uzyskane wcześniej, ale nie zależy funkcjonalnie od poprzednika.

I tak np. wybrany w pracy zmodyfikowany zestaw kryteriów (etap 1) na podstawie [3] może zostać rozszerzony do zbioru, o którym mowa w [10]. Zmianie może ulec także sposób ustalenia miar wybranych parametrów (etap 2). Autor zauważa także celowość dalszych prac nad rozwojem funkcji integrującej (etap 3) oraz wykorzystaniem mechanizmów logiki rozmytej do oceny odchylenia aktualnego poziomu dostępności od wartości pożądanej (etap 4).

availability was proposed, based on the integrated quantity criterion. This method has a modular structure (Fig. 1) which allows to adapt it easily to particular circumstances and to extend when necessary. Each module, being a successive stage of the assessment process, uses previously obtained results but does not depend functionally on the previous one.

Thus, for example, the modified set of criteria selected in this article (stage 1) on the basis of [3] can be extended into the set mentioned in [10]. Additionally, it is possible to change the manner of fixing the measures of selected parameters (stage 2). The author stresses the importance of further work to develop the integrating function (stage 3) and to use the mechanisms of fuzzy logic for assessing the deviation of the current availability level from the desirable value (stage 4).

Literatura

1. *Albin S.T.*: The Art of Software Architecture - Design Methods and Techniques, Wiley Publishing, Indianapolis 2003.
2. *Bass L., Clements P., Kazman R.*: Software Architecture in Practice, Addison-Wesley, 1998.
3. Bezpieczeństwo informacji, Jason MacKenzie, 2006, http://jmk.pl/jmk/u9.html.
4. Business Continuity and Availability Self-Assessment Tool, Hewlett-Packard Company, http://h30328.www3.hp.com/ui/forms/Default.aspx, 2006.
5. Business Continuity Management Code of Practice, standard BS 25999-1:2006, 2006.
6. *Callaghan J.*: Inside Intranets & Extranets: Knowledge Management and the Struggle for Power, Palgrave Macmillan, UK 2002.
7. Certyfikacja ISO 27001 - Zarządzanie bezpieczeństwem informacji, ISOQUAR CEE Sp. z o.o., portal www.isoquar.pl, Warszawa 2007.
8. Definicja BPM, DSA – Dokumenty w zasięgu ręki, dostępne pod adresem www.dsa.com.pl/index.php?id=222&lang=pl, październik 2007.
9. *Fenton N.E., Pfleeger S.L.*: Software Metrics. A Rigorous and Practical Approach, 2nd ed., PWS Publishing Company, Boston 1997.
10. *Gałach A.*: Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna, Ośrodek Doradztwa i Doskonalenia Kadr Sp. z o.o., Gdańsk 2005.
11. Information technology – Security techniques – Management of information and communications technology security, International Standard ISO/IEC 13335-1, 2004.
12. Information technology – Security techniques, International Standard ISO/IEC FDIS 17799, 2005.
13. IT Service Continuity Management. Code of Practice, Standard PAS77:2006, 2006.
14. *Kobyliński A.*: Modele jakości produktów i procesów programowych, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2005.
15. *Michalski A.*: Information Availability As a Component of the Information Security System, rozdział w monografii "Richnest and Diversity of GIS", Hrvatski Informaticki Zbor - GIS Forum, University of Silesia, Zagreb 2007.
16. *Michalski A.*: Dostępność informacji w organizacji gospodarczej, monografia, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
17. Reliability and Availability Basics, EventHelix.com, http://www.eventhelix.com/Realtime Mantra/FaultHandling/reliabilityavailability_basics.htm, 2006.
18. Specification for Business Continuity Management, Standard BS 25999:2007, 2007.
19. *Syska E.*: ROI: Wszystko jest mierzalne, IT Investment Consulting, http://www.it- investment.com.pl/index.php?option=com_content&task=view&id=84&Itemid=109, 2003.

References

1. *Albin S.T.*: The Art of Software Architecture - Design Methods and Techniques, Wiley Publishing, Indianapolis 2003.
2. *Bass L., Clements P., Kazman R.*: Software Architecture in Practice, Addison-Wesley, 1998.
3. Bezpieczeństwo informacji, Jason MacKenzie, 2006, http://jmk.pl/jmk/u9.html.
4. Business Continuity and Availability Self-Assessment Tool, Hewlett-Packard Company, http://h30328.www3.hp.com/ui/forms/Default.aspx, 2006.
5. Business Continuity Management Code of Practice, standard BS 25999-1:2006, 2006.
6. *Callaghan J.*: Inside Intranets & Extranets: Knowledge Management and the Struggle for Power, Palgrave Macmillan, UK 2002.
7. Certyfikacja ISO 27001 - Zarządzanie bezpieczeństwem informacji, ISOQUAR CEE Sp. z o.o., portal www.isoquar.pl, Warszawa 2007.
8. Definicja BPM, DSA – Dokumenty w zasięgu ręki, available at www.dsa.com.pl/index.php?id=222&lang=pl, October 2007.
9. *Fenton N.E., Pfleeger S.L.*: Software Metrics. A Rigorous and Practical Approach, 2nd ed., PWS Publishing Company, Boston 1997.
10. *Gałach A.*: Zarządzanie bezpieczeństwem systemu informatycznego – uniwersalna lista kontrolna, Ośrodek Doradztwa i Doskonalenia Kadr Sp. z o.o., Gdańsk 2005.
11. Information technology – Security techniques – Management of information and communications technology security, International Standard ISO/IEC 13335-1, 2004.
12. Information technology – Security techniques, International Standard ISO/IEC FDIS 17799, 2005.
13. IT Service Continuity Management. Code of Practice, Standard PAS77:2006, 2006.
14. *Kobyliński A.*: Modele jakości produktów i procesów programowych, Oficyna Wydawnicza Szkoły Głównej Handlowej w Warszawie, Warszawa 2005.
15. *Michalski A.*: Information Availability As a Component of the Information Security System, rozdział w monografii "Richnest and Diversity of GIS", Hrvatski Informaticki Zbor - GIS Forum, University of Silesia, Zagreb 2007.
16. *Michalski A.*: Dostępność informacji w organizacji gospodarczej, a monograph, Wydawnictwo Politechniki Śląskiej, Gliwice 2007.
17. Reliability and Availability Basics, EventHelix.com, http://www.eventhelix.com/Realtime Mantra/FaultHandling/reliabilityavailability_basics.htm, 2006.
18. Specification for Business Continuity Management, Standard BS 25999:2007, 2007.
19. *Syska E.*: ROI: Wszystko jest mierzalne, IT Investment Consulting, http://www.it- investment.com.pl/index.php?option=com_content&task=view&id=84&Itemid=109, 2003.

20. System pojąć, a ludzi zrozumieć - recepta na udane wdrożenie, Portal of business IT solutions ERP-view.pl, www.erp-view.pl/ERP/system_poj_a_ludzi_zrozumie_-_recepta_na_udane_wdro_enie__2.html, sierpień 2006.
21. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, ISO 27001, PN-ISO/IEC 27001:2005, 2005.
22. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, Standard PN-ISO/IEC 27001:2007, 2007.
23. Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji, Standard PN-ISO/IEC 17799:2007, 2007.
24. Wielka Internetowa Encyklopedia Multimedialna 2006, Onet.pl, 2005.
25. Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych, joint paper edited by Andrzej Michalski, Wydawnictwo Politechniki Śląskiej, Gliwice 2002.
26. *Zachman J.A.*: Enterprise Architecture: a Framework, ZIFA – Zachman Institute for Framework Advancement, Pinckney MI, available at www.zifa.com, September 2007.

20. System pojąć, a ludzi zrozumieć - recepta na udane wdrożenie, Portal of business IT solutions ERP-view.pl, www.erp-view.pl/ERP/system_poj_a_ludzi_zrozumie_-_recepta_na_udane_wdro_enie__2.html, sierpień 2006.
21. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, ISO 27001, PN-ISO/IEC 27001:2005, 2005.
22. Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania, Standard PN-ISO/IEC 27001:2007, 2007.
23. Technika informatyczna – Praktyczne zasady zarządzania bezpieczeństwem informacji, Standard PN-ISO/IEC 17799:2007, 2007.
24. Wielka Internetowa Encyklopedia Multimedialna 2006, Onet.pl, 2005.
25. Wykorzystanie technologii i systemów informatycznych w procesach decyzyjnych, joint paper edited by Andrzej Michalski, Wydawnictwo Politechniki Śląskiej, Gliwice 2002.
26. *Zachman J.A.*: Enterprise Architecture: a Framework, ZIFA – Zachman Institute for Framework Advancement, Pinckney MI, available at www.zifa.com, September 2007.

Recenzent: dr inż. Andrzej Białas

ОЦЕНКА ДОСТУПНОСТИ ИНФОРМАЦИИ

В статье проанализировано понятие и значение доступности информации в экономической организации и предложен интегрированный критерий для оценки актуальной доступности информации. Представлен также способ использования предложенной оценки на основании реальных сценариев, касающихся организации, подходящих различными способами к вопросам доступности информации. Указаны полученные данные интегрированной оценки для отдельных сценариев.