Zeszyty Naukowe Warszawskiej Wyższej Szkoły Informatyki Nr 9, Rok 7, 2013, s. 37-52

Bezpieczeństwo zasobów informacyjnych determinantą informatycznych technologii zarządzania

Piotr Zaskórski[*], Krzysztof Szwarc[**]

Streszczenie

W artykule przedstawiono problem bezpieczeństwa zasobów informacyjnych w kontekście wykorzystania informatycznych systemów wspomagających zarządzanie. Skoncentrowano się na metodach i technikach zapewniania ciągłości działania w aspekcie bezpieczeństwa informacyjnego współczesnych organizacji. Przywołano podstawowe dokumenty, standardy i procedury zapewniania bezpieczeństwa informacji w organizacji.

Słowa kluczowe: *zintegrowane systemy informatyczne zarządzania, zasoby informacyjne, bezpieczeństwo, ciągłość działania*

1 Wprowadzenie

Miejsce i rola technologii informatycznych w zarządzaniu organizacją XXI wieku warunkowana jest przede wszystkim ich użytecznością. Jednym z aspektów tej użyteczności jest poziom bezpieczeństwa zasobów informacyjnych gromadzonych i eksploatowanych przez różnego typu podmioty. Ma to szczególne znaczenie dla tzw. organizacji rozproszonych, a dziś coraz częściej określanych jako organizacje procesowe z dynamiczną strukturą działania.

Niezależnie od typu podmiotu[1] w gospodarce rynkowej standardem jest tworzenie takich organizacji na bazie infrastruktury sieciowej z dostępem do odpowiednio zorganizowanych zasobów informacji, umożliwiających komunikację, a tym samym nawiązywanie relacji między

[*] Warszawska Wyższa Szkoła Informatyki.
[**] Wojskowa Akademia Techniczna.
[1] Gospodarstwo domowe, przedsiębiorstwo, państwo.

wskazanymi grupami podmiotów. Można zatem mówić o informatycznej infrastrukturze zarządzania (**IIZ**), widocznej na każdym kroku ludzkiej aktywności [6].

Stąd jedną z płaszczyzn wykorzystania tego typu technologii jest tworzenie więzi gospodarczych, które zarówno na poziomie strategicznym, jak i operacyjnym mogą sprowadzać się do generowania decyzji o tym, z kim warto współdziałać przy realizacji określonych procesów oraz jaki system wartości ekonomicznych, społecznych i technicznych preferować. W szczególności może to być związane z poszukiwaniem odpowiedzi na pytania: gdzie, za ile, kiedy czy ile warto pozyskiwać określonych zasobów i za jaką cenę? Wykorzystanie do celów planistycznych określonych grup informacji musi być związane z odpowiednią wiarygodnością danych i poziomem ich bezpieczeństwa.

2 Rola technologii informatycznych w zarządzaniu

Podejmowanie decyzji przez różne podmioty działające w rozproszeniu i koordynujące swoją działalność przez dostęp do wspólnych zasobów informacyjnych o wybranym procesie lub określonych zadaniach − przy założeniu racjonalności gospodarowania − wymaga zatem dostępu do informacji (rysunek 1) o odpowiedniej wartości, determinującej jakość podejmowanych decyzji. Tak rozumiana rola informacji w organizacji każe interpretować zasoby informacyjne jako strategiczny komponent infrastruktury krytycznej[2]. W praktyce konieczne jest zatem wyodrębnienie zorganizowanego zbioru elementów powiązanych siecią dedykowanych relacji, umożliwiających pozyskiwanie i gromadzenie danych o środowisku i otoczeniu organizacji oraz selektywne ich przetwarzanie i udostępnianie uprawnionym podmiotom. Znaczący wzrost liczby danych implikuje automatyzację procesów informacyjnych, wprowadzanie odpowiednich mechanizmów ochrony oraz ściśle dedykowany dostęp do poszczególnych grup informacji w użytkowanych systemach informatycznych.

Postrzeganie systemów informatycznych przez pryzmat użyteczności, kieruje szczególną uwagę na podmiot działania[3] i jego potrzeby informacyjne. Ich spełnienie warunkowane jest poziomem bezpieczeństwa informacyjnego jednostki i całych współczesnych organizacji, a co za tym idzie zdolność do skutecznego i efektywnego działania oraz rozwoju. Jednym z dominujących tu zjawisk jest asymetria w dostępie do informacji, determinująca m.in. miejsce w strukturze organizacji (hierarchię) oraz bezpieczeństwo zasobów informacyjnych (czyt. w [18]).

[2] Zaliczanie zasobów oraz infrastruktury teleinformatycznej do infrastruktury krytycznej wydaje się w pełni uzasadnione w świetle Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 ze zm.) oraz Decyzji Rady Unii Europejskiej z dnia 12 lutego 2007 r., ustanawiającej na lata 2007-2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program: „Zapobieganie, gotowość
i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" (Dz.U. UE. L. 07.58.1).

[3] Użytkowników, administratorów, konserwatorów, twórców − systemu informatycznego.

Rysunek 1. Determinanty jakości decyzji
Źródło: opracowanie własne na podstawie [5].

Rozwój nauki i technologii IT determinowały ewolucję systemów informatycznych zarządzania. Widoczne to jest począwszy od systemów pasywnych (dziedzinowych), wpisujących się w strategię tzw. wysp informacyjnych, przez systemy wspomagania decyzji i systemy ekspertowe, po zintegrowane systemy informatyczne zarządzania. Zmienia się w ten sposób i zakres i poziom wspomagania organizacji. Można więc zauważyć, jak przeobraża się strategia (czyt. w [20]) wykorzystania informacji w organizacji – także z punktu widzenia potrzeby komunikacji i dzielenia się informacją (w tym również z otoczeniem organizacji).

Z perspektywy czasu przyjmuje się, że **jakość systemu informacyjnego determinuje skalę efektu synergii**, a tym samym pozycję konkurencyjną organizacji. Ze względu na potrzeby informacyjne zarządzania, zwłaszcza przy uwzględnieniu podejścia procesowego (tworzenie organizacji sieciowych/ wirtualnych, sieciocentrycznych z ekspozycją kompetencji) na szczególną uwagę zasługują zarówno systemy transakcyjne [4] jako narzędzie do opisu stanu procesów, jak również informacyjno-raportujące – wykorzystywane do monitorowania przebiegu realizacji procesów. Coraz częściej organizacje wspierane są całą rodziną systemów wspomagania decyzji (w tym systemów ekspertowych) i systemów tzw. sztucznej inteligencji, połączonych z koncepcją organizacji „uczących się". Współczesność to jednak próba integracji nie tylko danych, ale i usług. Platformą realizacji tej wizji stają się systemy zintegrowane

będące syntezą funkcjonalną i techniczno-organizacyjną wybranych lub wszystkich elementów wymienionych systemów dla potrzeb wsparcia organizacji procesowych.

Otwartym pozostaje uzyskanie odpowiedzi na pytanie o sposób wykorzystania dostępnych technologii informatycznych w zarządzaniu. „Przeniesienie" mocy obliczeniowej ze specjalnie przygotowanego pomieszczenia do „kieszeni" wydaje się tego najlepszym przykładem. Inną dominującą już dziś koncepcją jest technologia chmury obliczeniowej (ang. *cloud computing*) – zwłaszcza w kontekście wirtualizacji struktur działania. Z jednej strony można bowiem mówić o integracji i wirtualizacji zasobów informacyjnych, możliwości elastycznego i dynamicznego dopasowania do potrzeb użytkownika oferowanych usług oraz efektywności gospodarowania[4], ale z drugiej strony pozostaje istotne pytanie o dostępność, integralność czy poufność (bezpieczeństwo) informacji. Ten drugi kontekst eksponuje ważny atrybut determinujący skuteczność ochrony zasobów informacyjnych. Z przeprowadzonych przez firmę IDC badań wynika, że to właśnie obawa o bezpieczeństwo zasobów informacyjnych negatywnie wpływa na powszechność zastosowania tej technologii [9].

Niezależnie od dalszych modeli rozwoju usług informatycznych można stwierdzić, że rola informacji oraz systemów i zasobów informacyjnych jest coraz ważniejsza, a te stały się składnikiem aktywów organizacji determinującym jej pozycję i zdolność do konkurowania (w tym na globalnym rynku), a także efektywność działania (płynność finansową) oraz wiarygodność i pozycję rynkową [13].

3 Funkcjonalność zasobów informacyjnych

W każdym systemie działania zarówno na wejściu, jak i na wyjściu różnych procesów transformacji (produkcji, usługi, przetwarzania itp.) można zidentyfikować określone kategorie zasobów informacyjnych, co oznacza, że informacja jest zasobem:

- koniecznym do wytworzenia określonej wartości wyjściowej (produkt);
- powstającym w wyniku realizacji procesów transformacji, w tym procesów informacyjnych;
- posiadającym swoją wartość;
- determinującym sprawność całego systemu działania.

Tak więc informację należy interpretować jako kategorię ekonomiczną – i jako taka może być dobrem publicznym bądź towarem o cenie determinowanej mechanizmami rynkowymi. Stąd procesy informacyjne różnicowane mogą być pod względem nakładów, co ilustruje tzw. siodło kosztów informacji [11]. Można więc stwierdzić, że zasoby informacyjne są zarówno istotnym czynnikiem wytwórczym, jak i wynikiem (wartością wyjściową) systemu działania. Dlatego też na zasoby informacyjne należy spojrzeć przez pryzmat funkcji [2]:

[4] Naliczaniu opłat wyłącznie za wykorzystane zasoby/ usługi.

- **informacyjnej**, związanej z właściwym rozpoznaniem bieżącego potencjału wiedzy i potrzeb informacyjnych odbiorcy według wykorzystywanego przez niego języka oraz formy przekazu;
- **decyzyjnej**, jako zasilenie procesu decyzyjnego według właściwej percepcji problemu decyzyjnego, a w tym wariantowanie, szacowanie ryzyka wariantów decyzyjnych oraz dokonywanie racjonalnego wyboru;
- **motywująco-sterującej**, związanej z wywołaniem określonej reakcji u odbiorcy, a przez to zmianę stanu systemu i/lub otoczenia. Funkcja ta jest szczególnie widoczna w aspekcie automatyzacji procesów wytwórczych i usługowych z wykorzystaniem tzw. systemów CAx[5];
- **modelującej**, czyli umożliwiającej odzwierciedlenie przepływów informacyjnych w ramach całego systemu informacyjnego organizacji.

Wypełnianie wskazanych funkcji wymaga dostępu do informacji o pożądanym poziomie jakości. Wciąż otwartym problemem jest definiowanie pojęcia jakości informacji, a zwłaszcza czynników i kryteriów oceny. Można tu wskazać takie atrybuty jakości, jak istotność i relewancja, kompletność, aktualność, dokładność, spójność, a także adekwatność pod względem formy czy też bezpieczeństwo. Ocena jakości informacji w znacznej mierze ma często charakter subiektywny i trudno mierzalny.

4 Bezpieczeństwo zasobów informacyjnych

Analiza miejsca i roli zasobów informacyjnych przez pryzmat [7]: zarówno postrzegania ich jako strategicznego zasobu organizacji, jak i czynnika warunkującego sprawność i skuteczność procesów biznesowych, a także jako medium koniecznego do sterowania (zautomatyzowanymi systemami/ podsystemami wykonawczymi), kierowania (jednostkami lub grupami ludzi), zarządzania (instytucjami, przedsiębiorstwami), czy też w procesach dowodzenia (np. system bezpieczeństwa państwa) − wymaga zapewnienia odpowiedniego poziomu bezpieczeństwa. Co więcej, coraz częściej potrzeba ochrony określonych kategorii informacji wynika z przepisów prawa oraz ogólnych zaleceń formułowanych w formie strategii [16] i programów [15]. Stąd konieczne jest rozróżnienie pojęć: bezpieczeństwo informacyjne oraz bezpieczeństwo informacji.

Bezpieczeństwo informacyjne jest rozumiane zwykle jako stan zaufania (poparty odpowiednimi analizami, procesem myślowym) jednostki, grupy społecznej, całego społeczeństwa co do dostępności i jakości pozyskiwanej, przechowywanej, wykorzystywanej i przekazywanej informacji. Podmiotem bezpieczeństwa informacyjnego jest zatem pośrednio (w przypadku systemów sterowania) lub bezpośrednio człowiek, którego potrzeba (dostępu do informacji) może być w takim przypadku spełniona.

[5] CAx – Computer Aided: Planning, Manufacturing, Quality Assurance, Design, Engineering.

Węższym pojęciem jest **bezpieczeństwo informacji**, rozumiane jako poczucie zaufania (poparte analizą ryzyka, wynikami audytów bezpieczeństwa teleinformatycznego), że przechowywane informacje spełniają kryteria *poufności* (nie będą ujawnione i wykorzystywane przez nieuprawnione osoby), *integralności* (poprawne, nienaruszone i niemodyfikowane) i *dostępności* (dla uprawnionych użytkowników zgodnie z warunkami/ wymaganiami danego systemu) [14, p. 3.4]. Warto tu zwrócić uwagę na następujące cechy:

- autentyczność, czyli możliwość jednoznacznej identyfikacji podmiotów dostarczających informacje;
- rozliczalność, czyli możliwość jednoznacznej identyfikacji użytkowników oraz wykorzystywanych przez nich zasobów;
- niezaprzeczalność rozumianą jako pewność przypisania/adnotacji uczestnictwa użytkownika procesu informacyjnego (uniemożliwienie wyparcia się takiego działania);
- niezawodność postrzeganą jako zdolność systemu informacyjnego do bezawaryjnego działania w określonym przedziale czasu.

Zgodnie z normą: *bezpieczeństwo informacji oznacza jej ochronę przed szerokim spektrum zagrożeń w celu zapewnienia ciągłości działania, minimalizacji ryzyka i maksymalizacji zwrotu z inwestycji oraz możliwości biznesowych* [13]. Zatem ochrona informacji wymaga podejścia systemowego.

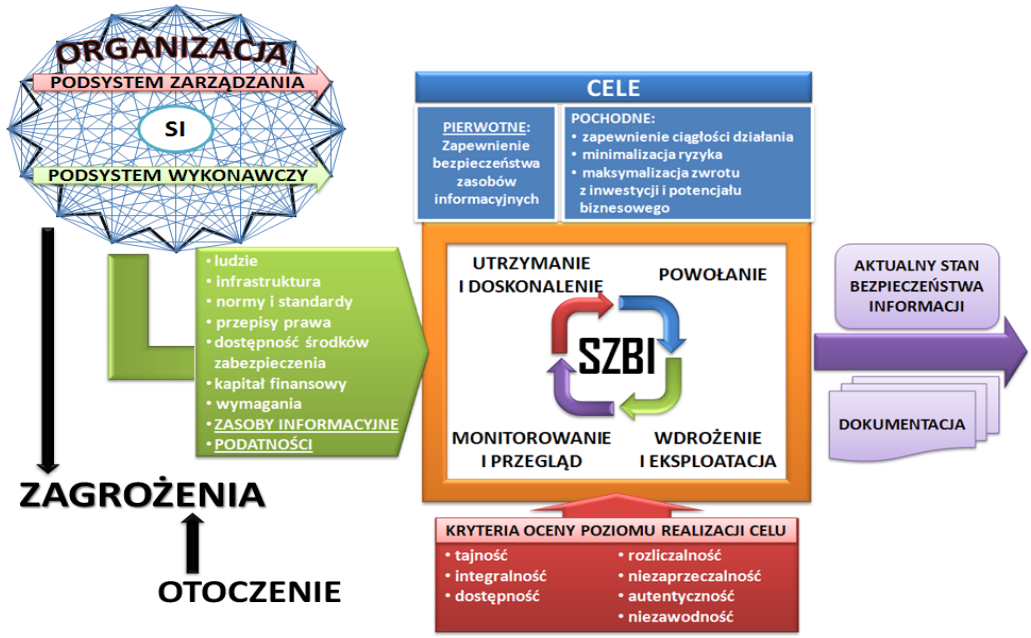
System zarządzania bezpieczeństwem informacji w organizacji (rysunek 2) uwarunkowany jest środowiskiem systemu działania (organizacji). Należy więc mieć świadomość podatności (luk), będących konsekwencją błędów na etapie projektowania systemu oraz niedostatecznych narzędzi (środków) zabezpieczenia. Jak w każdym modelu związanym z bezpieczeństwem, można mówić o **zagrożeniach**, które w tym kontekście należy rozumieć jako wszystkie możliwe działania skierowane na elementy systemu informacyjnego (SI), które mogą spowodować szkody – w przypadku istnienia określonej podatności [7]. Generalnie zagrożenia można podzielić na:

- celowe działania człowieka o charakterze terrorystycznym, przestępczym, dywersyjnym lub sabotażu;
- nieświadome, błędne wykorzystywanie elementów systemu, w tym wywołane niewłaściwie sformułowanymi procedurami;
- szkodliwe oddziaływanie sił natury, zwłaszcza w przypadku klęsk żywiołowych;
- awarie sprzętowe i błędy (wady) oprogramowania.

Dynamika systemu oraz zagrożeń implikuje konieczność tworzenia elastycznych systemów zabezpieczeń (rysunek 2), umożliwiających ich modyfikację, w przypadku zmiany środowiska/otoczenia działania. Dlatego w tym modelu, bazującym na wytycznych normy [14, pkt. 4] zaleca się ciągłe doskonalenie zgodnie z koncepcją PDCA. Stąd szczególna rola ewidencjonowania i dokumentowania w ramach systemu, w tym również w aspekcie ochrony i nadzoru sporządzanych zapisów i dokumentacji.

Warto tu również zaznaczyć, że problem bezpieczeństwa informacji, zwłaszcza systemów teleinformatycznych znajduje obszerne odzwierciedlenie w zbiorze międzynarodowych i krajowych norm. Obok cytowanych do tej pory norm PN-ISO/IEC 17799:2007 oraz PN-ISO/

IEC 27001:2007, na szczególną uwagę zasługuje standard Common Criteria, mający swoje odzwierciedlenie w postaci normy PN-ISO/IEC 15408 – części 1 i 3, a także publikacje NIST[6] – seria 800, czy standardy COBIT[7] i ITIL[8]. Dość wnikliwą analizę tych oraz innych istotnych dokumentów można znaleźć w literaturze przedmiotu [8].



Rysunek 2. Model systemu zarządzania bezpieczeństwem informacji w organizacji

5 Ryzyko obniżenia wartości zasobów informacyjnych

Przedstawione we wcześniejszej części rozważania na temat pojęć „zagrożenie" i „podatność" w kontekście możliwych strat prowadzą do konstatacji, że zagrożenie jest zjawiskiem naturalnym lub wywołanym przez człowieka, które nie musi się zrealizować i na które organizacja może nie mieć wpływu. Powstawanie szkód związanych z systemem informacyjnym jest wynikiem wykorzystania jego podatności, a poziom ich realizacji jest zależny od istniejących zabezpieczeń. Można zatem mówić o **ryzyku** utraty wartości zasobów informacyjnych, przede wszystkim ze względu na zagrożenie atrybutów poufności, integralności i dostępności tych zasobów. Poziom ryzyka będzie w takich warunkach determinowany prawdopodobieństwem

[6] NIST – National Institute of Standards and Technology.
[7] COBIT – Control Objectives for Information and Related Technology.
[8] ITIL – Information Technology Infrastructure Library.

realizacji zagrożenia oraz stopniem szkodliwości. Dlatego zarządzanie ryzykiem organizacji, jako proces holistyczny, dotyczy także bezpieczeństwa informacyjnego. Ważne tu staje się więc przygotowanie i stosowanie odpowiedniej polityki, formalnych procedur działania oraz dobrych praktyk menadżerskich dla realizacji procesów zarządzania ryzykiem (rysunek 3) [12]. Zarządzanie ryzykiem w kontekście sytemu informacyjnego wiąże się z:

1) Ustaleniem miejsca i roli systemu informacyjnego w organizacji, a dokładniej − w jaki sposób zasoby informacyjne warunkują możliwość osiągnięcia zakładanych (statutowych) celów;
2) Identyfikacją potencjalnych zagrożeń oraz podatności systemu informacyjnego wpływających na prawdopodobieństwo utraty atrybutów poufności, integralności i dostępności informacji;
3) Oceną stopnia dotkliwości zjawiska poprzez:
    - analizę prawdopodobieństwa realizacji zagrożenia w zależności od podatności systemu oraz oszacowaniem potencjalnych skutków takiego zdarzenia w odniesieniu do celów systemu informacyjnego oraz szerzej celów podmiotu gospodarczego (organizacji);
    - przyporządkowanie i ewaluację (nadanie rangi) opisywanego (ocenianego) zjawiska i podjęcie decyzji o zasadności przeciwdziałania/ reagowania;
4) Podjęciem stosownych działań w zakresie:
    - akceptacji możliwości występowania określonego rodzaju ryzyka, opisanego jako mało istotne (niskiej rangi), co jednak wymaga dokonania stosownej dokumentacji oraz wyznaczenia wartości progowych, których przekroczenie wpływa na zmianę postrzegania i konieczność podjęcia działań[9];
    - określenia sposobu postępowania z ryzykiem:
        - unikanie – wykluczenie elementów systemu z którymi wiąże się wysokie ryzyko, a ich usunięcie nie przeszkodzi realizacji celów[10];
        - ograniczanie – poprzez podejmowanie działań o charakterze prewencyjnym (stosowanie zabezpieczeń) oraz działań po realizacji zagrożenia, zmierzających do minimalizacji strat;
        - transfer – przekazanie całości lub części ryzyka na podmioty, które zarządzają tym zjawiskiem lepiej oraz skłonne są podjąć je za określoną opłatą;
        - retencja – gromadzenie środków niezbędnych do odtworzenia właściwego funkcjonowania systemu po incydencie, którego ryzyko jest wysokie, a których transfer jest niemożliwy lub nieuzasadniony z przyczyn ekonomicznych.

[9] W takim przypadku z oceny ryzyka wynika, że ze względu na prawdopodobieństwo i potencjalne skutki wystąpienia zjawiska są marginalne dla realizacji zakładanych celów.
[10] W praktyce takie działanie może polegać np. na wyborze sprawdzonego dostawcy, odebraniu prawa dostępu i modyfikacji określonych kategorii informacji.

Rysunek 3. Procesy zarządzania ryzykiem w organizacji
Źródło: opracowanie własne na podstawie [12].

Dynamika każdego systemu wymaga zwrócenia szczególnej uwagi na procesy monitorowania i komunikowania tak, by podejmowane działania odpowiadały rzeczywistości. Warto zaznaczyć, że gromadzone, generowane i przekazywane w ten sposób informacje zasilają pozostałe, opisane wcześniej procesy. Zakres i złożoność działań w tym obszarze determinowany jest bezpośrednio wynikami procesów ustalania kontekstu, identyfikacji oraz oceny ryzyka.

6 Postępowanie z ryzykiem utraty bezpieczeństwa informacji

Postępowanie z ryzykiem to ogół działań (zaprezentowanych na rysunku 3) ukierunkowanych na obniżenie jego poziomu do wartości tolerowanej [12, pkt. 3.6, pkt. 6.4]. Ich dobór jest nieprzypadkowy i powinien być konsekwencją pozostałych procesów składających się na zarządzanie ryzykiem przedsięwzięcia. Można zatem mówić przede wszystkim o unikaniu ryzyka. Podstawową cechą takiego działania jest zapewnienie braku realizacji danego typu ryzyka w stosunku do zasobów informacji lub procesów informacyjnych. Czynnikiem ograniczającym możliwość stosowania tego typu rozwiązania jest jego wpływ na zdolność osiągnięcia

celu. Dla przykładu, wyłączenie pracownika o wymaganych umiejętnościach od realizacji procesu technologicznego, ze względu na zagrożenie utraty tajności receptury, może prowadzić do braku możliwości jej praktycznego wykorzystania. Częściej spotykana jednak będzie sytuacja, gdy wyłączenie określonego elementu wiąże się z obniżeniem efektywności finansowej, wydłużeniem czasu realizacji, czy obniżeniem wybranych kryteriów jakościowych.

Różne organizacje biznesowe dążąc do realizacji swoich celów, a w tym maksymalizacji zysków, podejmują ryzyko, stosując przy tym określone mechanizmy ochronne. Działania w tym zakresie polegają na ograniczaniu prawdopodobieństwa realizacji zagrożenia poprzez zastosowanie określonych zabezpieczeń oraz zapewnieniu ciągłości działania w sytuacjach kryzysowych, ukierunkowanych na zmniejszenie potencjalnych skutków zjawiska (rysunek 4). Minimalizacja prawdopodobieństwa realizacji zagrożeń dla bezpieczeństwa informacji wymaga wykorzystania różnych zabezpieczeń, które można identyfikować w trzech kategoriach:

1) Zabezpieczenia **fizyczne**, których stosowanie ma na celu niedopuszczenie do fizycznego dostępu przez nieuprawnione podmioty oraz zabezpieczenie przed skutkami pożarów, zalania czy awarii/ katastrofy budowlanej. W praktyce zabezpieczenia fizyczne realizowane są poprzez zaangażowanie służb ochrony, zintegrowane systemy monitoringu, informowania o włamaniach, pożarach, a także wykorzystanie rozwiązań technicznych typu wzmocnione drzwi z zamkiem szyfrowanym, sejfy, klatki Faradaya i inne.
2) Zabezpieczenia **systemowe i programowe** wiążą się zwykle z systemami logicznej kontroli dostępu (zastosowanie uwierzytelniania i weryfikacji autoryzacji), z zabezpieczeniami kryptograficznymi, monitorowaniem ruchu w sieciach, systemami antywirusowymi i ścianami ogniowymi, tworzeniem kopii zapasowych, zapewnieniem właściwej eksploatacji i konserwacji wykorzystywanych systemów informatycznych oraz elementów infrastruktury technicznej. Można do tego obszaru zaliczyć także nadzór nad usługami sieciowymi (w tym przez podmioty zewnętrzne) i samą obsługę nośników danych. Celem stosowania tej grupy zabezpieczeń jest zapewnienie bezpieczeństwa eksploatacji systemów informatycznych wspomagających zarządzanie i dostęp do określonej kategorii zasobów przez uprawnione do tego podmioty.
3) Zabezpieczenia natury **organizacyjnej** związane są zwykle z przygotowaniem i utrzymaniem odpowiedniej dokumentacji (w tym odzwierciedlającej odpowiedzialność za dany zasób), opracowaniem i doskonaleniem norm i standardów postępowania z zasobami informacyjnymi (np. zasada czystego biurka i ekranu, zasady niszczenia dokumentów, normy etyczne), opracowaniem zasad reagowania na incydenty, organizacją i nadzorem bezpieczeństwa informacji (w tym przy wykorzystaniu podmiotów zewnętrznych), a także zasad rekrutacji, doskonalenia (szkolenia) i zasad zachowania po zakończeniu pracy lub zmianie miejsca zatrudnienia [13, pkt. 8-13].

Rysunek 4. Metody ograniczania ryzyka zagrożenia informacji

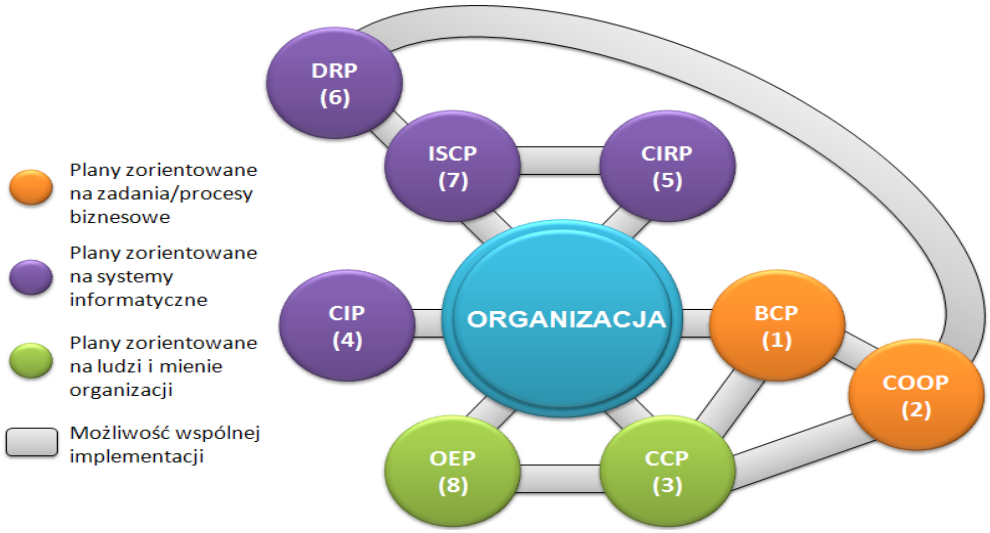
Wszelkie zabezpieczenia należy postrzegać jako spójny system ukierunkowany na obniżenie prawdopodobieństwa realizacji zagrożenia w wyniku wykorzystania podatności systemu informacyjnego. Innym sposobem ograniczania ryzyka jest dążenie do minimalizacji strat wynikających z wystąpienia incydentu.

Jednym z ważnych uregulowań proceduralnych w obszarze stosowania informatycznych technologii zarządzania jest przygotowanie i wdrażanie **planów ciągłości działania IT,** a w tym [10]:

1) **Planów zapewnienia ciągłości działania (BCP)**, które powinny zawierać kompleksowe założenia w zakresie zarządzania ciągłością działania w skali stanowiska, zespołu, organizacji czy całej korporacji. Plan powinien uwzględniać potrzeby i możliwości systemu informacyjnego organizacji ze względu na ich role we wspomaganiu zadań i funkcji realizowanych przez organizację;
2) **Planów reagowania na incydenty cybernetyczne (CIRP)**, w których ustanawia się procedury dotyczące działania w przypadku ataku na system informatyczny organizacji, a zwłaszcza działania związane z nieautoryzowanym dostępem do danych (poufność), odmowy dostępu do danych lub usług informacyjnych (dostępność), nieuprawnionej

ingerencji w sprzęt, oprogramowanie, dane systemu (integralność) np. poprzez wykorzystanie szkodliwego oprogramowania jak wirusy, robaki czy konie trojańskie;

3) **Planów odtwarzania funkcji systemów po katastrofie (DRP)**, które dotyczą bezpieczeństwa systemów informatycznych, przywracania ich zdolności w odniesieniu do aplikacji oraz sprzętu w zapasowej lokalizacji. Ich tematyka często pokrywa się z planami zapewnienia ciągłości działania systemów IT;
4) **Planów zapewnienia ciągłości działania systemów IT (ISCP)**, które powinny umożliwiać ocenę oraz sposoby przywracania zdolności systemu wraz ze zdefiniowaniem ról i odpowiedzialności, spisem inwentaryzacyjnym, procedurami oceny, szczegółowymi procedurami odtwarzania i testowania systemu. Podstawową różnicą między ISCP i DRP jest miejsce działania, które w przypadku planów ISCP może oznaczać zarówno miejsca awarii, jak i działania w wyznaczonym miejscu zapasowym, ponieważ plany DRP określają zasady przeniesienia elementów systemu do zapasowej lokalizacji oraz przywracania ich zdolności;
5) **Planu (krajowego) ochrony infrastruktury krytycznej (CIP)**, który jest opracowywany na szczeblu krajowym (RCB) i dotyczy ochrony infrastruktury krytycznej kraju. Określa się tutaj zasady ochrony elementów kluczowych dla zachowania ciągłości działania państwa, jego instytucji oraz przedsiębiorstw o znaczeniu strategicznym. Zawarte w tym planie wytyczne mają wpływ na działanie organizacji/ podmiotu dysponującego elementami infrastruktury krytycznej państwa.



Rysunek 5. Metody ograniczania ryzyka zagrożenia informacji

Na rysunku 5 zaprezentowano powiązania między planami w aspekcie ich implementacji. Najbardziej kompleksowymi rozwiązaniami odnoszącymi się do utrzymania ciągłości systemu działania są: plan ciągłości działania (BCP) oraz plan utrzymania ciągłości operacyjnej (COOP).

Dość ważnym sposobem postępowania z ryzykiem jest **transfer.** Oznacza to, że jest realizowany wtedy, gdy pomimo podjętych działań (unikania i ograniczania) poziom ryzyka jest nadal wysoki. Generalnie transfer ryzyka odbywa się przez jego podział i przekazanie podmiotom, które ze względu na ich umiejętności są w stanie skutecznie sobie z nim radzić. Przykładowymi formami transferu ryzyka informacyjnego może być ubezpieczenie (np. sprzętu, od strat wynikających z przerw w dostawach usług) lub outsourcing (np. obsługa portalu internetowego organizacji). Szczególnie ciekawe wydaje się wykorzystanie w tym aspekcie technologii chmury [21], której wariantem może być np. usługa IaaS[11].

Świadomość istnienia poważnego rodzaju ryzyka, którego organizacja nie jest w stanie uniknąć, zmniejszyć jego rozmiarów lub przekazać innym podmiotom, determinuje obowiązek zatrzymania (retencji), a tym samym poniesienia wszelkich konsekwencji w przypadku jego realizacji. Rozpoznanie ryzyka umożliwia wydzielenie określonej ilości środków, gromadzonych na wypadek takiego zdarzenia.

7 Bezpieczeństwo informacji determinantą ciągłości procesów zarządzania

Zarządzanie to ogół działań ukierunkowanych na zasoby organizacji, w wyniku których możliwe jest sprawne i skuteczne osiąganie zakładanych celów [3]. Można zatem powiedzieć, że procesy zarządzania będą oceniane przede wszystkim według kryterium sprawności i skuteczności działania. W powyższych rozważaniach skoncentrowano się na mechanizmach zapobiegania ryzyku obniżania wartości zasobów informacyjnych. Można zatem powiedzieć, że wartość informatycznych technologii zarządzania jest determinowana bezpieczeństwem tych zasobów, utrzymywanych zarówno w systemach klasy OLTP, jak i w systemach BI.

Bez wiarygodnej informacji trudno jest mówić o spełnianiu kryteriów systemowych (np. efektywność, jakość) przez całą organizację i dlatego warunkiem skutecznego działania jest ciągłość procesów informacyjno-decyzyjnych, ponieważ:

a. informacja stanowi często nie tylko zasób operacyjny, ale i strategiczny bezpośrednio związany z procesami prognozowania, planowania i podejmowania decyzji, a także organizowania, normowania, nadzorowania, sprawozdawczości oraz kontroli i oceny,
b. każdy proces/ przedsięwzięcie może być postrzegany jako sprawny (efektywny i jakościowo dobry) oraz skuteczny (zapewniający realizację zakładanych celów), jeżeli jest m.in. informacyjnie bezpieczny.

[11] IaaS – Infrastructure as a Service.

Ciągłość procesów zarządzania determinowana jest dostępem do informacji o wymaganej wartości, czyli do informacji adekwatnej do potrzeb decydenta, przedstawionej w odpowiedniej formie, wewnętrznie spójnej, kompletnej, wiarygodnej i aktualnej. Uświadomienie sobie takiej zależności powoduje, że zalecenia norm [14] tutaj przywoływanych jest odzwierciedleniem ich znaczenia, ale również zagwarantowania niezbędnych środków oraz umocowania stosownych założeń w kulturze organizacji.

Można przy tym wskazać na zestaw działań natury organizacyjnej i technicznej ograniczających negatywne skutki utraty ciągłości działania wywołane zagrożeniami bezpieczeństwa informacyjnego (tabela 1).

Zapewnienie stałego dostępu do krytycznych zasobów organizacji wiąże się z zaangażowaniem określonego potencjału ludzkiego, infrastrukturalnego, intelektualnego i finansowego, będącego w zasadzie odzwierciedleniem możliwości organizacji. Zawsze bowiem konieczna będzie odpowiedź na pytanie, czy inwestować w wybrane elementy infrastruktury o określonym czasie amortyzacji, czy zasadnym jest poniesienie ryzyka – a jeżeli tak, to jakiego?

Tabela 1. Działania w sferze organizacyjnej i technicznej związane z zapewnieniem „informacyjnej" ciągłości działania

Przedsięwzięcia organizacyjne	**Przedsięwzięcia techniczne**
Identyfikacja krytycznych procesów i zasobów organizacji oraz dopuszczalnego czasu przerw w dostępie do informacji niepowodującego zakłóceń w ciągłości działania	Dokonywanie przeglądów oraz formułowanie wniosków i zaleceń na potrzeby działań organizacyjnych
Opracowanie i wdrożenie planów zapewnienia ciągłości działania (ogólnoorganizacyjnych i procesowych/ funkcjonalnych)	Utrzymanie i pielęgnacja elementów sprzętowych, oprogramowania i sieci (w tym zapasowych)
Organizacja ćwiczeń/ szkoleń w zakresie działania w przypadku zakłócenia ciągłości działania	Określanie potrzeb i zakup urządzeń zasilania zastępczego
Zakup i eksploatacja sprzętu zgodnie ze standardami jakościowymi	Zabezpieczenie przed nieuprawnionym dostępem do zasobów systemu
Zawarcie porozumień na potrzeby wykorzystania zapasowych ośrodków pracy	Wykorzystanie wyników działań organizacyjnych do dublowania zasobów krytycznych
Kształtowanie norm i standardów związanych z zapewnieniem ciągłości działania w kulturze organizacji	Okresowe wykonywanie kopii zapasowych oraz weryfikacja ich jakości

Źródło: opracowanie własne na podstawie [7].

8 Podsumowanie

Celem tego opracowania z całą pewnością nie jest próba eksponowania określonego rozwiązania, ani też tworzenia rankingu i oceniania poszczególnych metod i technik zapewniania informacyjnej ciągłości działania [19]. W organizacjach XXI wieku technologie informatyczne wspomagają całą gamę procesów wytwórczych i usługowych. Powstają organizacje rozproszone, wirtualne. Ich sprawność determinowana jest szybkim i pewnym dostępem do żądanej informacji. Stąd zasoby informacyjne − szczególnie te współdzielone − wymagają odpowiednich mechanizmów ochrony. Zwraca się więc uwagę na problemy, których rozwiązanie może decydować o przetrwaniu organizacji w turbulentnym otoczeniu. Bezsprzecznie jednym z nich jest odpowiednie wykorzystanie i zapewnienie bezpieczeństwa informacji – jako kluczowego zasobu współczesnych organizacji.

Bibliografia

[1] Decyzja Rady Unii Europejskiej z dnia 12 lutego 2007 r., ustanawiająca na lata 2007-2013, jako część ogólnego programu w sprawie bezpieczeństwa i ochrony wolności, szczegółowy program: „Zapobieganie, gotowość i zarządzanie skutkami terroryzmu i innymi rodzajami ryzyka dla bezpieczeństwa" (Dz.U. UE. L. 07.58.1)

[2] Flakiewicz W., *Systemy informacyjne w zarządzaniu. Uwarunkowania, technologie, rodzaje*, Wyd. C.H. Beck, Warszawa 2002

[3] Griffin R.W., *Podstawy zarządzania organizacjami*, Wyd. Nauk. PWN, Warszawa 2008

[4] Januszewski A., *Funkcjonalność informatycznych systemów zarządzania. Tom 1 Zintegrowane systemy transakcyjne*, Wyd. Nauk. PWN, Warszawa 2011

[5] Kisielnicki J., Turyna J., (red. nauk), *Decyzyjne systemy zarządzania*, Difin, Warszawa 2012

[6] Kisielnicki J., *Zarządzanie: jak zarządzać i być zarządzanym*, PWE, Warszawa 2008

[7] Liderman K., *Bezpieczeństwo informacyjne*, Wyd. Nauk. PWN, Warszawa 2012

[8] Liderman K., *Normy i standardy z zakresu bezpieczeństwa informacyjnego i teleinformatycznego*, „Biuletyn Instytutu Automatyki i Robotyki", nr 26, WAT, Warszawa 2009

[9] Mateos A., Rosenberg J., *Chmura obliczeniowa. Rozwiązania dla biznesu*, Helion, Gliwice 2011

[10] Swanson M., Bowen P., Wohl Phillips A., Gallup D., Lynes D., *Contingency Planning Guide for Information Technology Systems*, NIST Special Publication 800-34, May 2010, http://csrc.nist.gov/publications/nistpubs/800-34-rev1/sp800-34-rev1_errata-Nov11-2010.pdf

[11] Oleński J., *Ekonomika informacji. Metody*, PWE, Warszawa 2003

[12] PN-IEC 62198:2005 *Zarządzanie ryzykiem przedsięwzięcia. Wytyczne stosowania*, PKN, Warszawa 2005

[13] PN-ISO/IEC 17799: 2007 *Technika informatyczna. Techniki bezpieczeństwa. Praktyczne zasady zarządzania bezpieczeństwem informacji*, PKN, Warszawa 2007
[14] PN-ISO/IEC 27001:2007 *Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania*, PKN, Warszawa 2007
[15] *Rządowy program ochrony cyberprzestrzeni RP na lata 2011-2016. Wersja 1.1*, MSW, Warszawa 2010
[16] *Strategia Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2007, http://www.bbn.gov.pl/portal/pl/475/1144/Strategia_Bezpieczenstwa_Narodowego_RP.html
[17] Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz.U. z 2007 r. Nr 89, poz. 590 ze zm.)
[18] Zaskórski P., *Asymetria informacyjna w zarządzaniu procesami*, WAT, Warszawa 2012
[19] Zaskórski P., *Zarządzanie organizacją w warunkach ryzyka utraty informacyjnej ciągłości działania*, WAT, Warszawa 2011
[20] Zaskórski P., *Strategie informacyjne w zarządzaniu organizacjami gospodarczymi*, WAT, Warszawa 2005
[21] Zaskórski P., *Wirtualizacja organizacji w „chmurze" obliczeniowej*, „Ekonomika i Organizacja Przedsiębiorstwa", Wyd. ORGMASZ, nr 3/2012, Warszawa 2012

Information resources security as determinant of IT management

Abstract

In this article we have tried to identify security problem for information resources in using aspect of Integrated Management Information Systems. We presented possibility of adaptation some of the methods and techniques of continuity functioning of organization in information security aspects. The main goal of our concept is connected with documents, standards and procedures management of information security.

***Keywords**: integrated management information systems, information resources, security, continuity*