Barbara Biszewska

AUDYT INFORMATYCZNY W INSTYTUCJACH SKARBOWYCH

Wprowadzenie

W instytucjach publicznych, w przeciwieństwie do sektora biznesu, zarządzanie ryzykiem, jego analiza, identyfikacja, pomiar i kontrola są względnie nowym zjawiskiem. Zarządzanie ryzykiem jest obecnie procesem usprawniającym funkcjonowanie organizacji. Przyczynia się do poprawy jakości zarządzania organizacją, poprzez lepsze świadczenie usług, szybsze wprowadzanie innowacji organizacyjnych, jak też lepsze wykorzystanie jej zasobów. Prowadzenie analizy ryzyka pozwala na obiektywną realizację i uzasadnienie wyboru zadania w audycie wewnętrznym, do którego prowadzenia zobowiązane są ustawowo jednostki sektora finansów publicznych.

Celem analizy ryzyka jest wskazanie tych obszarów audytu, gdzie ryzyko jest największe. W artykule przedstawiono zagadnienie analizy ryzyka w obszarze systemu informatycznego POLTAX, głównego systemu funkcjonującego w jednostkach sektora finansów publicznych, jakimi są urzędy i izby skarbowe.

1. Pojęcie i klasyfikacja ryzyka

Terminu **ryzyko** nie da się jednoznacznie zdefiniować. Zarówno w literaturze ekonomicznej jak i innych specjalistycznych dziedzinach i obszarach istnieje wie-

le pojęć ryzyka. Według Słownika współczesnego języka polskiego słowo **ryzyko**[1] oznacza przedsięwzięcie, czyn, którego wynik jest niepewny, wątpliwy; możliwość niepowodzenia, porażki, straty. Specjalistyczna literatura, na przykład Międzynarodowe Standardy Profesjonalnej Praktyki Audytu Wewnętrznego[2] określają **ryzyko** – jako możliwość zaistnienia zdarzenia, które będzie miało wpływ na realizację założonych celów.

Ryzyko jest mierzone wpływem (wielkością skutków) oraz prawdopodobieństwem jego wystąpienia. Ryzyko można też przedstawić w skrócie za pomocą wzoru: **R = P * S**, gdzie **R** – oznacza ryzyko, **P** – prawdopodobieństwo jego wystąpienia, a **S** – określony skutek. Niezmiernie ważne według R. Rudnickiego[3] jest to, że skutek i prawdopodobieństwo to dwie całkowicie od siebie niezależne wielkości, w żaden sposób na siebie nie wpływające, tym samym wymagające odrębnej analizy. Ryzyko jest koncepcją związaną z pomiarem niepewności (prawdopodobieństwa)[4]. W procesie niepewność dotyczy możliwości osiągnięcia celów organizacyjnych. Ryzyko może dotyczyć zarówno pozytywnych jak i negatywnych skutków. Większość pozytywnych konsekwencji określana jest mianem możliwości, a negatywnych nazywana jest zagrożeniami bądź ryzykiem. Skutki to materialne efekty ryzyka związanego z decyzją, wydarzeniem lub procesem. Dotkliwość skutków zależy od wielu czynników, między innymi od: zasobów ryzyka, rodzaju zagrożenia, czasu trwania konsekwencji oraz efektywności funkcjonujących kontroli.

Najczęściej jednak ryzyko kojarzone jest z aspektem negatywnym[5]. Oznacza niebezpieczeństwo nieosiągnięcia założonych celów i efektów finansowych, a nawet poniesienie straty. Ryzyko może mieć również aspekt pozytywny. Jest szansą na osiągnięcie celu i uzyskanie zysku. Podobnie opisuje ryzyko K. Czerwiński[6] jako możliwość wystąpienia zdarzenia, które będzie miało wpływ na organizację. Według

[1] *Słownik współczesnego języka polskiego*, Wilga, Warszawa 1998, s. 283.

[2] Komunikat Nr 1 Ministra Finansów z dnia 19 lutego 2009 r. w sprawie standardów audytu wewnętrznego w jednostkach sektora finansów publicznych, Dz. Urz. MF nr 2, poz. 12.

[3] R. Rudnicki, *Zarządzanie ryzykiem dla członków zarządu*, www.rudnicki.com.pl/ artykuły i publikacje.

[4] D. McNamee, *Oszacowanie ryzyka w audycie wewnętrznym i zarządzaniu*, Fundacja Rozwoju Rachunkowości w Polsce, Warszawa 2004, s. 14.

[5] T.T. Kaczmarek, *Ryzyko i zarządzanie ryzykiem. Ujęcie interdyscyplinarne*, Difin, Warszawa 2006, s. 54.

[6] K. Czerwiński, H. Grocholski, *Podstawy audytu wewnętrznego*, LINK, Szczecin 2003, s. 53.

niego istnieją dwa źródła ryzyka: zagrożenia bezpośrednie – zdarzenia szkodliwe, które powodują, że cele nie zostaną osiągnięte oraz szanse – zdarzenia korzystne, które dają możliwość skuteczniejszego osiągnięcia celów. Zagrożenie jest połączeniem ryzyka, skutków tego ryzyka i prawdopodobieństwa, że negatywne zdarzenie nastąpi.

Kiedy kierownictwo rozważa ryzyko, z reguły myśli o jego oszacowaniu i zarządzaniu ryzykiem. Oszacowanie ryzyka to metoda identyfikacji i pomiaru ryzyka. Zarządzanie ryzykiem to podejmowanie czynności w celu minimalizacji ryzyka. W ramach szacowania ryzyka dokonuje się ilościowego i jakościowego szacunku zagrożenia powstałego z jakiejkolwiek działalności. Identyfikuje się i klasyfikuje co jest ryzykiem, dokonuje się jego charakterystyki oraz ustala hierarchie ryzyka. Ponadto określa się jak poszczególne ryzyka są powiązane między sobą.

W praktyce występują trzy główne podejścia do identyfikacji ryzyka:

1) analiza zagrożenia, czyli identyfikacja ryzyka, która może oddziaływać na zasoby (aktywa). Podejście to ma najlepsze zastosowanie w procesach, w których osiągnięcie ich celów uzależnione jest mocno od zasobów, między innymi w rozwoju systemów informatycznych,
2) analiza środowiskowa, polegająca na identyfikacji ryzyka, które może wpływać na działania operacyjne. Działa ona najlepiej w procesach związanych z działalnością usługową dla klientów oraz działalnością rządu i instytucji użyteczności publicznej,
3) scenariusze zagrożenia to specjalistyczna metoda identyfikacji ryzyka wystąpienia oszustwa, zagrożenia, katastrofy. Jest najbardziej skuteczna w zakresie oszustw. Wykorzystanie tego podejścia wymaga jednak kogoś biegłego, zaangażowanego w proces, względnie doświadczonego audytora. Wybór, który z powyższych sposobów jest najwłaściwszy zależy od istoty organizacji.

Najczęściej identyfikacja ryzyka jest dokonywana przy wykorzystaniu wszystkich trzech sposobów. Na pojęcie ryzyka składają się elementy obiektywne i subiektywne. Do obiektywnych należy zaliczyć przeszkody w działalności gospodarczej, zdarzenia powodujące niebezpieczeństwa oraz możliwość ich wystąpienia. Subiektywnym elementem jest świadomość niebezpieczeństwa, decyzja wzięcia na siebie odpowiedzialności, postawa człowieka, jego umiejętności oraz cechy osobowości.

W definicji pojęcia ryzyka należy uwypuklić elementy obiektywne, stanowiące podstawowe jego składniki. Podkreślenie rangi i kwantyfikacji elementów subiek-

tywnych jest konieczne dla ich obiektywizacji i niedopuszczenia do pomniejszania ich roli.

Etapy rozwoju naukowej definicji ryzyka są w dużej mierze zgodne z ewaluowaniem rozróżnienia określeń ryzyko i niepewność z nim związana. Dyskusje nad tymi definicjami doprowadziły do czterech zasadniczych wniosków dotyczących natury ryzyka[7]:

1) ryzyko jest czymś jednorodnym, a zatem nie jest możliwe podanie jednej uniwersalnej i jednoznacznej definicji tego pojęcia,
2) ryzyko występuje w co najmniej dwóch aspektach: obiektywnym i subiektywnym,
3) ryzyko może być badane w różnych kontekstach, jako niebezpieczeństwo, hazard, niepewność, prawdopodobieństwo,
4) ryzyko jest czymś zmiennym i stadialnym, czyli jest raczej procesem niż stanem.

Wiele jest zatem definicji przedmiotu ryzyka i wiele znaleźć można różnych klasyfikacji ryzyka. Najczęściej wyróżnia się:

– ryzyko właściwe – związane z prawem wielkich liczb i odnoszące się do zjawisk o charakterze katastroficznym (pożar, powódź),
– ryzyko subiektywne – związane z niedoskonałością człowieka, który subiektywnie ocenia prawdopodobieństwo wystąpienia pewnych zjawisk w przyszłości,
– ryzyko obiektywne – forma absolutna niepewności, która jest związana z niemożliwością przewidzenia rozwoju niektórych zjawisk.

Kolejna klasyfikacja pozwala wyróżnić dwa rodzaje ryzyka związanego z funkcjonowaniem przedsiębiorstwa:

– ryzyko stałe (niezmienne) – dotyczy całego systemu gospodarczego,
– ryzyko niestałe (zmienne) – dotyczy danego przedsiębiorstwa.

Ryzyko koreluje ze wszystkimi naszymi działaniami, lecz niektóre spośród nich zwiększają ryzyko, a inne zmniejszają. W teorii ekonomii ryzykowne działania charakteryzują się:

– prawdopodobieństwem wystąpienia określonego wyniku,
– pewnym podziałem zmienności wszystkich możliwych wyników[8].

[7] K. Czerwonka, M. Cież, *Zarządzanie ryzykiem*, Encyklopedia Zarządzania, strona internetowa.

[8] D. Begg, S. Fischer, R. Dornbusch, *Mikroekonomia*, PWE, Warszawa 2003, s. 398.

Można stwierdzić, że obecnie mamy do czynienia ze swoistym trendem na widzenie wszystkich aspektów działalności biznesowej firmy przez pryzmat ryzyka. Ograniczanie ryzyka w zakresie działalności jednostki jest podstawowym celem audytu wewnętrznego. Wyboru zadań audytowych do zrealizowania w organizacji, obiektywnie przeprowadzonego i uzasadnionego dokonuje się dzięki analizie ryzyka. Ma to przełożenie między innymi, również na problematykę bezpieczeństwa teleinformatycznego, niezmiernie istotną we współczesnych, wysoko zinformatyzowanych organizacjach.

2. Istota ryzyka informatycznego

W dzisiejszych czasach organizacje dokonują ogromnych inwestycji w automatyzację wewnętrznych procesów w nich zachodzących i nabierają wartości w wyniku gromadzenia olbrzymiej ilości danych, pochodzących z różnych źródeł. Zgromadzone informacje stają się obecnie najważniejszym aktywem organizacji i dlatego trzeba jej i narzędziom przetwarzającym te informacje zapewnić odpowiednie bezpieczeństwo. Jednym z elementów bezpieczeństwa informacji jest bezpieczeństwo systemów informatycznych, służących do przetwarzania informacji. Jak powiedział E.H. Spafford[9]: „Jeśli systemy byłyby budowane z zachowaniem ostrożności i dobrej praktyki w dziedzinie inżynierii oprogramowania, to mielibyśmy o wiele mniej problemów z bezpieczeństwem informacji".

Zapewnienie bezpieczeństwa systemom przetwarzającym informacje jest procesem ograniczania ryzyka lub prawdopodobieństwa szkody. W obszarze systemów informatycznych najczęściej wykorzystywana i powszechnie znana jest definicja ryzyka przyjęta przez ISO[10]. Ryzyko to prawdopodobieństwo, że określone zagrożenie może wykorzystać słabość zasobów lub grup zasobów powodując ich utratę lub zniszczenie. Wpływ lub relatywne narażenie na ryzyko jest proporcjonalne do wartości biznesowej utraty lub zniszczenia i oszacowanej częstotliwości wystąpienia zagrożenia. Zagrożenia mogą pochodzić od błędów, wad stosowanych rozwiązań i urządzeń, sił natury lub celowych działań człowieka. Dla potrzeb bezpieczeństwa

[9] E.H. Spafford, *Reexamining Instrusion Detection* zaprezentowany na University of Virginia 1999, przytoczone za D.L. Pipkin, *Bezpieczeństwo informacji*, WNT, Warszawa 2002, s. 23.

[10] *Guidelines for the Management of IT Cecurity, International Organization for Standardization (ISO)*, przytoczone za M. Forystek, *Audyt informatyczny*, Info-Audit, Warszawa 2005, s. 13.

informacji definicję podaną w normach przystosował K. Lidermann[11]. **Ryzyko** oznacza według niego miarę stopnia zagrożenia dla tajności, integralności i dostępności informacji, wyrażoną jako iloczyn prawdopodobieństwa (lub możliwości) wystąpienia sytuacji stwarzającej takie zagrożenie i stopnia szkodliwości jej skutków (strat). Do zagrożeń związanych z systemami informatycznymi można zaliczyć między innymi:

– awarie zasilania,
– zawieszanie się systemów operacyjnych,
– nieuzasadnione zajmowanie całych zasobów pamięci i mocy przetwarzania przez programy i procesy,
– pomyłki we wprowadzaniu parametrów konfiguracji,
– pomyłki w ustalaniu praw dostępu do programów i danych,
– błędy w działaniu i awarie sprzętu,
– infekowanie wirusami, celowe niszczenie danych,
– udostępnianie danych osobom nieuprawnionym,
– wykonywanie operacji bez zezwolenia itp.

W fazie badania bezpieczeństwa informatycznego poddaje się głębokiej analizie aspekty finansowe aktywów i zasobów oraz szkody, jakie mogą powstać w przypadku ich utraty, modyfikacji lub ujawnienia. Bezpieczeństwo zmniejsza ryzyko. Aby określić żądany poziom bezpieczeństwa, należy znać prawdopodobieństwo incydentu związanego z bezpieczeństwem oraz zakres szkód, jakie incydent może spowodować. Aspekty te są właśnie przedmiotem analizy ryzyka informatycznego.

Analiza ryzyka bezpieczeństwa systemów teleinformatycznych pozwala na identyfikację zasobów systemu, odpowiadających im podatności i zagrożeń, oszacowanie prawdopodobieństwa ich wystąpienia i wielkości potencjalnych strat. Analiza ryzyka powinna obejmować gruntowne zinwentaryzowanie zasobów informacyjnych oraz oszacowanie zagrożeń. Aby prawidłowo zidentyfikować zasoby podlegające ochronie, przeprowadza się ich inwentaryzację, ocenia wartość dla obszaru objętego analizą ryzyka oraz ustala:

– na jakie procesy w organizacji dany zasób ma wpływ i jaki jest to wpływ,
– z jakimi atrybutami bezpieczeństwa dany zasób jest związany (dostępność, integralność, poufność),

[11] K. Liderman, *Analiza ryzyka i ochrona informacji w systemach komputerowych*, PWN, Mikom, Warszawa 2008, s. 70.

– jaka jest wartość zasobu w zależności od danego atrybutu bezpieczeństwa,
– kto jest właścicielem zasobu.

Kolejnym krokiem jest identyfikacja zagrożeń. Zagrożeniem[12] są potencjalne działania człowieka (lub zaniechanie takich działań) albo sił wyższych, dotyczące bezpośrednio zasobu teleinformatycznego lub organizacji procesu przetwarzania informacji i mogące (po wykorzystaniu podatności, jeśli istnieje) spowodować, w zależności od konkretnego atrybutu bezpieczeństwa: tajności, integralności lub dostępności, straty proporcjonalne do wagi procesu krytycznego, wspieranego przez ten proces i wykorzystywane w nim zasoby. Krótko ujmując zagrożeniami są wszystkie możliwe działania dotyczące jakiegoś zasobu lub procesu, które mogą spowodować straty.

Zagrożenia mogą być zamierzone lub przypadkowe. Przy zagrożeniach zamierzonych należy wziąć pod uwagę motywację, wiedzę, możliwości i zasoby atakujących oraz atrakcyjność zasobów. Przy zagrożeniach przypadkowych należy zwrócić uwagę na źródła niebezpieczeństwa, położenie geograficzne, warunki pogodowe, błąd ludzi czy błąd maszyny.

Zagrożenia bezpośrednio wpływające na system informatyczny i przetwarzane w nim informacje można sklasyfikować następująco[13]:

1) **Siły wyższe** – klęski żywiołowe, katastrofy finansowe, zmiany prawa itp.,
2) **Nieuprawnione i przestępcze działania ludzi**, w tym:
   a) zagrożenia związane z kradzieżami fizycznymi i zagubieniami sprzętu, oprogramowania i dokumentów,
   b) zagrożenia związane z podsłuchami różnego typu sprzętu i oprogramowania,
   c) nieuprawnione działania personelu,
   d) nieuprawnione działania osób postronnych.
3) **Błędy personelu** obsługującego system komputerowy,
4) **Skutki złej organizacji pracy**, w tym zagrożenia związane z błędami w ochronie fizycznej i technicznej,
5) **Awarie i uszkodzenia sprzętu oraz wady oprogramowania.**

Gruntowne zinwentaryzowanie zasobów informatycznych oraz szacowanie zagrożeń należy zatem do zakresu analizy ryzyka informatycznego.

[12] *Ibidem*, s. 41.

[13] *Ibidem*, s. 42.

4. Identyfikacja i wycena ryzyka systemu informatycznego POLTAX w urzędach i izbach skarbowych

Izby i urzędy skarbowe są jednostkami budżetowymi, należącymi do sektora finansów publicznych zgodnie z przepisami ustawy o finansach publicznych[14]. Działają na podstawie statutu, określającego w szczególności nazwę, siedzibę i przedmiot działalności, w tym działalności podstawowej. Ich charakterystykę i organizację określa zarządzenie Ministra Finansów w sprawie organizacji urzędów i izb skarbowych oraz nadania im statutów[15]. Urzędy skarbowe są jednostkami organizacyjnymi obsługującymi naczelników urzędów skarbowych, a izby skarbowe obsługującymi dyrektorów izb skarbowych[16].

Głównym celem w zakresie realizacji polityki finansowej państwa dla dyrektorów izb skarbowych i naczelników urzędów skarbowych jest zapewnienie wpływu dochodów do budżetu państwa na poziomie określonym w ustawie budżetowej[17] na dany rok. Organy te mają za zadanie również osiągnięcie efektywnego i profesjonalnego poziomu działania administracji podatkowej i wysokiego poziomu dobrowolnego wypełniania obowiązków podatkowych przy jednoczesnej racjonalizacji kosztów funkcjonowania administracji.

W każdym obszarze działania komórek organizacyjnych izb i urzędów skarbowych wykorzystuje się, w celu usprawnienia i przyspieszenia prac, dostępne narzędzia informatyczne. Administracja podatkowa korzysta z wielu narzędzi informatycznych, które poprzez odpowiednie powiązania stanowią sprawny instrument gromadzenia i wykorzystywania zawartych w nich informacji. Głównym zadaniem administracji podatkowej w dziedzinie komputeryzacji, w szczególności urzędów skarbowych jest utrzymanie ciągłości działania infrastruktury i eksploatowanych systemów informatycznych. Natomiast izby skarbowe organizują nadzór nad eksploatacją wszystkich systemów informatycznych zarówno w swojej jednostce, jak i w podległych jej urzędach skarbowych oraz zapewnić prawidłowe warunki techniczne eksploatacji systemów informatycznych.

[14] Ustawa z dnia 30 czerwca 2005 r. o finansach publicznych, DzU nr 249, poz. 2104.

[15] Zarządzenie Nr 13 Ministra Finansów z dnia 20 czerwca 2006 r. w sprawie organizacji urzędów i izb skarbowych.

[16] Ustawa z dnia 21 czerwca 1996 r. o urzędach i izbach skarbowych, DzU z 2004 r., nr 121, poz. 1267.

[17] Ustawa budżetowa z dnia 23 stycznia 2009 r., DzU nr 10, poz. 58.

W ramach organizacji pracy izb i urzędów skarbowych w dziedzinie komputeryzacji szczególną uwagę zwraca się na zapewnienie bezpieczeństwa danych przetwarzanych w systemach informatycznych oraz przestrzeganie przepisów i procedur dotyczących komputerowych baz danych. Kompleksowa komputeryzacja jednostek skarbowych w kraju trwa już od początku lat dziewięćdziesiątych, ale śmiało można stwierdzić, że podstawowym, najważniejszym systemem informatycznym eksploatowanym we wszystkich urzędach i izbach skarbowych jest system POLTAX. System POLTAX został pomyślany jako długofalowe przedsięwzięcie służb podatkowych, którego celem jest zapewnienie efektywnych i skutecznych działań: poboru, dystrybucji, planowania i kontroli należności budżetowych. Jego istotną cechą jest otwartość na zmienność przepisów prawnych i jednocześnie możliwość zapewnienia jednolitości ich interpretacji i stosowania w całym kraju. System POLTAX ma za zadanie ułatwienie pracy pracownikom administracji skarbowej, zwiększenie efektywności ich pracy oraz doprowadzenie do poprawy obsługi podatników, płatników i innych klientów instytucji skarbowych oraz spowodowanie skuteczniejszej współpracy służb skarbowych zarówno w ramach poszczególnych organizacji jak też pomiędzy sobą. System POLTAX służy zwiększeniu efektywności i skuteczności systemu podatkowego. Jest jednym z podstawowych źródeł danych i informacji dla organów Państwa. Rzeczywiste bazy danych tworzone są w wyniku eksploatacji systemu POLTAX w urzędach skarbowych, natomiast w izbach skarbowych instaluje się kolejne wydania systemu i bazy dla celów szkoleniowych.

Podatkowy system informatyczny POLTAX składa się z szeregu modułów, podsystemów i innych elementów zintegrowanych ze sobą. Wszystkie z eksploatowanych modułów i podsystemów POLTAX'u oparte są na wspólnej bazie danych, są ze sobą wzajemnie powiązane, przez co zapewniają komputerowe wspomaganie pracy we wszystkich komórkach urzędu skarbowego. Dają też możliwość wykonywania różnorodnych sprawozdań, raportów i zestawień z danych przez siebie gromadzonych.

Każda jednostka skarbowa dąży do skutecznego i profesjonalnego zabezpieczenia całości swoich zasobów, w tym informacji, danych i systemów informatycznych poprzez funkcjonujący w jednostce system zapewnienia bezpieczeństwa. Naczelnik urzędu skarbowego i dyrektor izby skarbowej jest zobowiązany zastosować środki techniczne i organizacyjne zapewniające ochronę przetwarzanych danych i systemów informatycznych odpowiednio do potencjalnych zagrożeń.

System informatyczny w urzędach skarbowych narażony jest na różnego rodzaju niepożądane zdarzenia, które prowadzić mogą między innymi do:
- przerwy w pracy systemu (z powodu uszkodzenia programów, systemów operacyjnych, sprzętu),
- wykorzystania systemu do celów niezgodnych z jego przeznaczeniem,
- utraty lub zniekształcenia danych (utrata poufności i integralności),
- ujawnienia przetwarzanych informacji.

W celu wykonania optymalnej identyfikacji zagrożeń, jedną z czynności jest odpowiedni dobór zespołu identyfikującego. W przypadku systemów informatycznych powinny być to osoby, których działalność związana jest z funkcjonowaniem systemów informatycznych w jednostce. W urzędzie skarbowym mogą to być pracownicy komórek bezpieczeństwa informacji: pełnomocnik do spraw ochrony informacji niejawnych, administrator bezpieczeństwa informacji (danych osobowych), kierownicy głównych komórek organizacyjnych oraz pracownicy zajmujący się administrowaniem systemów i sieci teleinformatycznych.

Jedną z technik identyfikacji zagrożeń jest „burza mózgów". Przykładowo, w jednym z badanych urzędów skarbowych, po wygenerowaniu przypadków i sformułowaniu możliwych scenariuszy, których wystąpienie stanowić może zagrożenie dla systemu informatycznego, zidentyfikowane zagrożenia podzielono na: zewnętrzne, środowiskowe i wewnętrzne.

Zagrożenia zewnętrzne związane są z ryzykiem uszkodzenia sprzętu, sieci i utraty danych spowodowanych przerwami w dostawie energii elektrycznej, jak również zanikami napięcia. Zagrożeniami zewnętrznymi są też włamania do systemu informatycznego, fizyczne włamanie do obiektu, jak i włamanie przez sieć komputerową. Szczególne zagrożenie stanowią też komputery przenośne pracowników, które narażone są na kradzież lub zgubienie.

Zagrożenia środowiskowe związane są z klęskami żywiołowymi (pożar, powódź, huragan, opady atmosferyczne, ruchy tektoniczne), które należy rozpoznawać w zależności od podatności i warunków w jakich znajduje się jednostka (klimat, lokalizacja).

Zagrożenia wewnętrzne stanowią największy procent zdarzeń związanych z naruszeniem bezpieczeństwa systemu informatycznego. Najczęstszą przyczyną występowania tego typu zagrożeń jest nieprzestrzeganie przepisów i procedur bezpieczeństwa, zasad korzystania z systemu, brak zrozumienia wymogów bezpie-

czeństwa, niewystarczająca znajomość systemów i programów komputerowych, zaniedbania ze strony pracowników i administratorów, awarie urządzeń i instalacji. Do takich zagrożeń należą między innymi:

- pozostawianie niewyłączonych komputerów, brak profilaktyki antywirusowej,
- niewłaściwy przydział uprawnień użytkownikom,
- nieprzestrzeganie zasady ochrony haseł dostępu,
- pozostawianie osób nieuprawnionych w pomieszczeniach biurowych,
- nieuczciwość pracowników, którzy mogą przekazać dane osobom nieuprawnionym,
- nieprzestrzeganie procedury archiwizacji danych,
- błędne instalacje aplikacji i zmian do systemu operacyjnego,
- uszkodzenie sprzętu w wyniku nieprawidłowej obsługi,
- kradzież sprzętu, nieprawidłowe użytkowanie komputerów przenośnych,
- nieprawidłowe działania administracyjne związane z brakiem nadzoru nad bezpieczeństwem systemu informatycznego.

Wszystkie wymienione kategorie zagrożeń mogą wystąpić w każdym urzędzie skarbowym. Jednakże w każdym indywidualnie prawdopodobieństwo ich wystąpienia i skutki jakie mogą wywołać jest zupełnie różne. Główną i wyłączną odpowiedzialność za procesy związane z zarządzaniem ryzykiem w jednostce ponosi kierownik. Jednakże żadna osoba nie dysponuje kompletną wiedzą, umożliwiającą realizację takiego zadania, jakim jest identyfikacja ryzyka, dokonanie analizy i oceny ryzyka dla całej organizacji. Dla potrzeb opracowania autor dokonał uprzednio analizy ryzyka dla najistotniejszych, zidentyfikowanych zagrożeń systemu informatycznego POLTAX, z jakimi spotkać się można w urzędach skarbowych, korzystając z metody szacunkowej – mieszanej. Następnie dokonał oceny, które ryzyko można zaakceptować, które można ograniczać i jakie środki zaradcze i zabezpieczenia można zastosować. Jako wynik prowadzonej analizy ryzyka bezpieczeństwa systemu informatycznego POLTAX w urzędzie skarbowym, dokonał również charakterystyki działań, które można zastosować do niektórych rodzajów zagrożeń.

W przypadku analizy ryzyka prowadzonej na potrzeby systemu informatycznego środki zmniejszające ryzyko w zakresie działań związanych z kontrolowaniem ryzyka nazywa się zabezpieczeniami. Zabezpieczenia mogą być typu organizacyjnego, fizycznego (obiektów i urządzeń, w tym komputerów) lub technicznego. W jednostkach skarbowych stosowanie zabezpieczeń wynika z przepisów, między

innymi ustawy o ochronie danych osobowych[18] i przepisów wykonawczych[19] do niej. Cechą charakterystyczną zarządzania ryzykiem związanym z przetwarzaniem informacji w organizacji jest znaczenie zabezpieczeń, szczególnie zabezpieczeń sprzętowo-programowych w przypadku informacji. Wynika to z faktu, że podstawowym elementem systemu informacyjnego, dla którego prowadzona jest analiza ryzyka jest system teleinformatyczny. Problem unikania bądź ograniczania ryzyka powinien być rozwiązany na etapie projektowania systemu informatycznego.

System informatyczny POLTAX został wyposażony w odpowiednie zabezpieczenia już na etapie projektowania w Ministerstwie Finansów. Jednostki skarbowe eksploatujące ten system muszą natomiast w ramach realizacji swoich funkcji w swoistych warunkach, dokonywać analizy ryzyka i starać się minimalizować największe ryzyko (najmniejszym kosztem) związane z zabezpieczeniem tego systemu. Prowadzenie analizy ryzyka i audytu wewnętrznego w obszarze systemów informatycznym w organizacji nie jest zadaniem prostym, pozbawionym konieczności profesjonalnego podejścia, wykorzystującego odpowiednie metodyki i standardy.

Audyt wewnętrzny jest nierzadko narzędziem prewencyjnym, pozwalającym zapobiec nieprawidłowościom i udoskonalić proces zarządzania bezpieczeństwem systemów informatycznych w jednostce. Zarządzający organizacją zaczynają zauważać, że realizacja rekomendacji audytu przynosi znaczne korzyści i usprawnia działania instytucji. W urzędach skarbowych zalecenia audytu w zakresie zarządzania i bezpieczeństwa systemów informatycznych dotyczą z reguły następujących kwestii:

1. Okresowego dokonywania identyfikacji ryzyka w obszarze systemów informatycznych,
2. Dokonania odpowiednich zmian w dokumentacji systemu: politykach, procedurach, instrukcjach,
3. Usprawnienia procedur związanych z prowadzeniem dzienników systemu,
4. Wprowadzenia rozwiązań zmierzających do wykrywania włamań do danych przez nieuprawnionych użytkowników,

[18] Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, DzU nr 100 z 2004 r., poz. 1024.

[19] Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych oraz warunków technicznych..., DzU nr 100, poz. 1024.

5. Usprawnienia zabezpieczeń fizycznych obiektów i pomieszczeń informatyki,
6. Dokonywania okresowych przeglądów uprawnień użytkowników systemu.

Doskonaląc i utrzymując proces zabezpieczania systemów informatycznych, jednostki skarbowe, podobnie jak inne organizacje, mogą dążyć do wdrożenia systemu zarządzania bezpieczeństwem informacji (SZBI) i zdobyć stosowny certyfikat. Bez względu na charakter, rozmiar, typ i sektor organizacji można spełniać wymagania odpowiednich norm, dotyczących ustanawiania, wdrażania, eksploatacji, monitorowania, przeglądu utrzymywania i doskonalenia SZBI. Zaleca się, aby wprowadzenie SZBI było dla organizacji decyzją strategiczną podobnie jak wdrożenie systemu zarządzania jakością (SZJ). Na projektowanie i wdrażanie SZBI w organizacji mają wpływ potrzeby i cele biznesowe, wynikające z nich wymagania bezpieczeństwa, realizowane procesy oraz wielkość i struktura instytucji.

Uwagi końcowe

Zarządzanie ryzykiem to kwestia kluczowa dla wszystkich organizacji, zarówno w sektorze publicznym, jak i prywatnym. Proces ten jest wynikiem debaty dotyczącej *governance* (ładu organizacyjnego), która toczyła się szczególnie w ciągu ostatnich lat. Governance to kombinacja procesów oraz struktur wprowadzonych przez kierownictwo dla uzyskania przepływu informacji, zarządzania, kierowania oraz monitorowania działań w organizacji, nakierowanych na realizacje celów tej organizacji. Organizacje zwróciły uwagę na potrzebę skutecznej identyfikacji, analizy i zarządzania ryzykiem. Nie ma jednej „właściwej" metody identyfikacji ryzyka.

Każda jednostka, również jednostka sektora finansów publicznych, musi wypracować własną metodę, biorąc pod uwagę swoje doświadczenie, wielkość i charakter organizacji. Proces zarządzania ryzykiem, przeprowadzanie analizy i pomiaru ryzyka należy wdrożyć w całej organizacji. Każdy kierownik jednostki sektora finansów publicznych będzie zobowiązany wdrożyć środki odpowiednie do osiągnięcia tego celu.

Działanie jednostki (urzędu skarbowego) opiera się na informacjach do niej należących, zgromadzonych w jej bazach, na jej tajemnicach. Wszystkie te tajemnice mają ogromne znaczenie dla organizacji. Wszystkie muszą być chronione. Kierownictwo jednostki musi doceniać znaczenie przyjętych zasad, standardów i procedur służących ochronie informacji. Powinno wprowadzić efektywne środki bezpie-

czeństwa zapewniające ochronę posiadanej informacji, ciągłą dostępność systemów podtrzymujących krytyczne funkcje oraz odpowiednie mechanizmy zabezpieczenia informacji przed jej rozmyślnym lub przypadkowym ujawnieniem, manipulacją, modyfikacją, zniszczeniem lub skopiowaniem. Zadaniem środków ochronnych jest zapewnienie tajności, integralności i dostępności informacji przetwarzanej w chronionych systemach informatycznych, ponieważ ma ona wpływ na przebieg zachodzących w niej procesów.

Efektywne zarządzanie ryzykiem informatycznym w organizacji pozwoli na właściwą identyfikację zagrożeń dla bezpieczeństwa systemów informatycznych i oszacowanie ryzyka związanego z użytkowaniem systemów. Na podstawie wniosków z dostępnych statystyk wynika, że największa liczba zagrożeń związana jest z błędami w obsłudze systemu komputerowego i organizacji pracy z systemem.

Najpowszechniejsze ryzyko związane z systemem informatycznym użytkowanym w urzędzie stanowi błąd ludzki. Prawdopodobieństwo błędu może być zmniejszone poprzez szkolenia użytkowników. Ciągłe szkolenie pracowników jest najbardziej efektywnym finansowo programem bezpieczeństwa, jaki jest dostępny w jednostce. Gdy użytkownicy będą popełniać mniej błędów, lepiej zrozumieją znaczenie bezpieczeństwa, będą mieć ogromny wpływ na zmniejszenie ryzyka w obszarze informatycznym.

Literatura

Begg D., Fisher S., Dornbusch R., *Mikroekonomia*, PWE, Warszawa 2003.

Bywanis-Jodlińska M., *Kontrola i zarządzanie ryzykiem, materiały szkoleniowe służby cywilnej*, Warszawa 2005.

Czerwiński K., Grocholski H., *Podstawy audytu wewnętrznego*, Link, Szczecin 2003.

Czerwonka K., Cież M., *Zarządzanie ryzykiem*, Encyklopedia Zarządzania.

Forystek M., *Audyt informatyczny*, InfoAudit, Warszawa 2005.

Kaczmarek T.T., *Ryzyko i zarządzanie ryzykiem*. *Ujęcie interdyscyplinarne*, Difin, Warszawa 2006.

Liderman K., *Analiza ryzyka i ochrona informacji w systemach informatycznych*, PWN, Mikom, Warszawa 2008.

Liderman K., *Podręcznik administratora bezpieczeństwa teleinformatycznego*, Mikom, Warszawa 2003.

McNamee D., *Oszacowanie ryzyka w audycie wewnętrznym i zarządzaniu*, Fundacja Rozwoju Rachunkowości, Warszawa 2004.

Międzynarodowe Standardy Profesjonalnej Praktyki Audytu Wewnętrznego, IIA, Warszawa 2009.
Pipkin D.L., *Bezpieczeństwo informacji*, WNT, Warszawa 2002.
Piotrowski M., *Zarządzanie ryzykiem bezpieczeństwa informacji w systemach TI*, Prezentacja 2006, Serwis SCO.
Rozporządzenie MSWiA z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych, DzU nr 100, poz. 1024.
Rudnicki R., *Zarządzanie ryzykiem dla członków zarządu*, Artykuły i publikacje 2009.
Słownik współczesnego języka polskiego, Wilga, Warszawa 1998.
Ustawa budżetowa z dnia 23 stycznia 2009 r., DzU nr 10, poz. 58.
Ustawa z dnia 30 czerwca 2005 r. o finansach publicznych, DzU nr 249, poz. 2104.
Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych, DzU z 2002 r., nr 101, poz. 926.
Ustawa z dnia 21 czerwca 1996 r. o urzędach i izbach skarbowych, DzU z 2004 r., nr 121, poz. 1267.
Zarządzenie Nr 13 Ministra Finansów z dnia 20 czerwca 2006 r. w sprawie organizacji urzędów i izb skarbowych oraz nadania im statutów, Dz. Urz. MF nr 7, poz. 55.

INFORMATION AUDIT IN TAX INSTITUTIONS

Summary

The article presents the informations about analysis of risk on example chosen by author of area of computerized information system POLTAX, which is exploited in all tax offices in country. It explain definition of risk and classification. Author brings closer essence of risk on area of computerized information system. In the final article part author includes information of biggest threats in area of safety computerized information POLTAX. Also author presents recommendations which are recommended in revenue boards for liquidation most often and limiting of information risk and affirmation of safeties of computerized information systems in unit

Translated by Anna Zbaraszewska