Rola audytu w zarządzaniu zabezpieczeniami systemów informatycznych

Małgorzata Pańkowska

Omówiono podstawowe koncepcje analizy SWOT stosowanej w zarządzaniu zabezpieczeniami systemów informatycznych w instytucji. Zdefiniowano strategię i politykę ochrony systemów informatycznych oraz poddano analizie znaczenie audytu zabezpieczeń do skutecznej realizacji tej polityki. Przedstawiono audyt analizowany w aspekcie przeglądu zabezpieczeń i wnioskowania na podstawie śladu rewizyjnego oraz zaprezentowano nowe obszary badań audytu, tj. testowanie podatności zasobów, kształtowanie świadomości użytkowników, planowanie ciągłości funkcjonowania, licencjonowanie i rozwój oprogramowania.

zabezpieczenie systemów informatycznych, strategia zabezpieczeń, polityka zabezpieczeń, analiza SWOT, audyt systemów informatycznych, analiza ryzyka

Podstawowe koncepcje zarządzania zabezpieczeniami systemów informatycznych

Zabezpieczenie systemów informatycznych jest częścią składową zarządzania informacją w instytucji i obejmuje ochronę zarówno systemów komputerowych oraz infrastruktury, jak i informacji przed celowymi lub przypadkowymi zniszczeniami. Program zabezpieczeń, czyli całokształt działań ochrony zasobów informatycznych organizacji gospodarczej, powinien umożliwić realizację takich celów, jak: określenie procesu planowania zabezpieczeń, zdefiniowanie funkcji zarządzania zabezpieczeniami, zapewnienie rozwoju polityki zabezpieczeń, określenie procesu analizy nakładów i efektów, określenie procesu zarządzania ryzykiem, określenie formalnych procedur oceny zabezpieczeń, planowanie i realizacja działań naprawczych.

Zarządzanie zabezpieczeniami można realizować na podstawie analizy SWOT (*Strenghts Weaknesses Opportunities Threats*) (rys. 1 i tabl. 1). W pierwszym kroku analizuje się zewnętrzne aspekty działania instytucji, które mają wpływ na wybór strategii zabezpieczeń (zagrożenia, środki i sposoby zabezpieczeń). W drugim kroku należy dokonać analizy wewnętrznych mocnych (odporność zasobów) i słabych (podatność zasobów) stron instytucji oraz jej kultury pracy. Trzeci krok to wykorzystanie wyników analizy SWOT i opracowanie strategii oraz polityki zabezpieczeń.

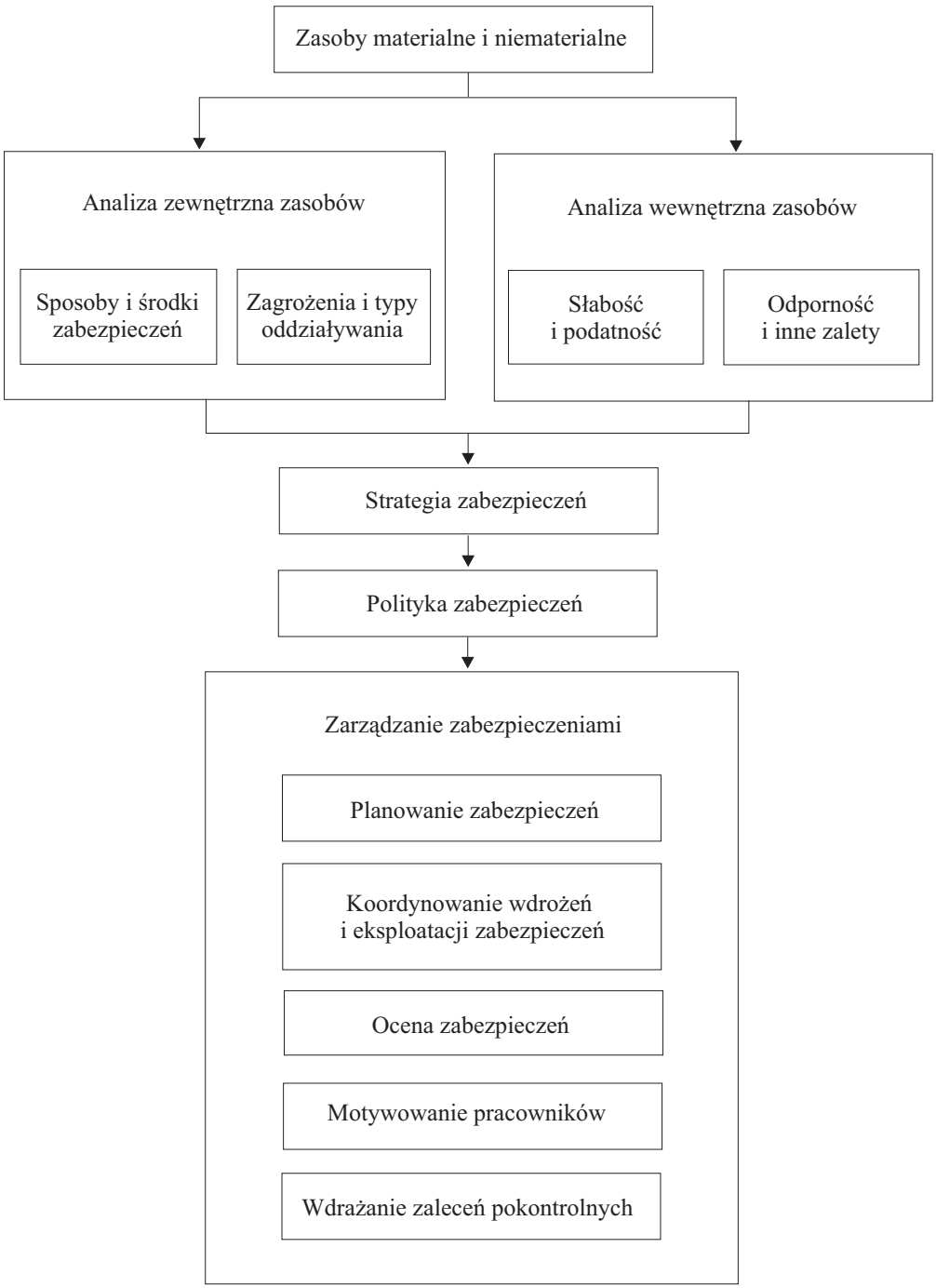
Ogólnie, wytyczne analizy SWOT są proste, ale jednocześnie trudne w realizacji: należy unikać i eliminować zagrożenia, wykorzystywać szanse obrony oraz minimalizowania strat podczas ataku, wzmacniać słabe strony i opierać się na mocnych podstawach.

Zabezpieczenie systemów informatycznych wymaga analizy zasobów instytucji, przy czym jest istotna wartość każdego zasobu, będąca jego wewnętrznym atrybutem, wyrażana w odniesieniu do zasobów materialnych jako koszt nabycia i konserwacji. W systemach informatycznych wyróżnia się cztery podstawowe kategorie zasobów: zasoby fizyczne (komputery, nośniki pamięci, urządzenia wprowadzania i wyprowadzania danych), zasoby intelektualne (oprogramowanie wraz z dokumentacją), zasoby kadrowe (użytkownicy, projektanci, programiści i administratorzy), usługi i transakcje dokonane przy użyciu oprogramowania aplikacyjnego, a także usługi operatorskie, administracji i oceny systemów

informatycznych. Zasoby wskutek oddziaływania zagrożeń są narażone na kradzież, zniszczenie lub uszkodzenie. Przykładowe zagrożenia wymieniono w tablicy 1.

Tabl. 1. Analiza SWOT – przykładowa lista problemów strategicznych

Potencjalne mocne strony *(Strengths)*	Potencjalne słabe strony *(Weaknesses)*	Potencjalne szanse *(Opportunities)*	Zagrożenia *(Threats)*
Znacząca pozycja na rynku Wystarczające zasoby finansowe na inwestycje w systemy zabezpieczeń Doświadczenie i umiejętności personelu Wysokie morale pracowników Zaangażowanie kierownictwa w opracowanie programu zabezpieczeń Zgodna współpraca wewnątrz instytucji Pomysłowość, kreatywność	Brak środków finansowych na systemy zabezpieczeń Niska rentowność Brak należytego zainteresowania kierownictwa ochroną zasobów Brak kluczowych umiejętności administrowania i obsługi systemów informatycznych Przestarzałe systemy zabezpieczeń Niemożność rozwiązania wewnętrznych problemów organizacyjnych Nienadążanie za postępem technicznym Brak odpowiedzialności za zasoby Inercja, lekceważenie obowiązków, korupcja	Dostępne na rynku środki zabezpieczeń i nowe rozwiązania techniczne Ustawodawstwo Sprawne działanie instytucji nadzoru publicznego: policja, straż pożarna Możliwość scedowania ryzyka zniszczeń na towarzystwa ubezpieczeniowe Możliwość zainstalowania analogicznego systemu komputerowego i baz danych do pracy w sytuacjach zniszczeń lub awarii	Kradzież zasobów, w tym także kopiowanie układów pamięci Niewłaściwe wykorzystanie zasobów, np. symulacja zachowań pełnoprawnego użytkownika, przekazywanie informacji utajnionymi kanałami Użycie zasobów informatycznych w innych celach niż zadeklarowano w kontrakcie (wykorzystanie systemów komputerowych do osiągania prywatnych korzyści materialnych) Bezprawne ujawnianie informacji osobom nieupoważnionym Podsłuchiwanie rozmów, bezprawne rejestrowanie przesyłanych komunikatów, nieumyślne zniszczenie zasobów, wprowadzanie bezprawnych komunikatów do ruchu sieciowego, bezprawna modyfikacja informacji, bezprawny odczyt informacji pozostawionej w dostępnym miejscu wskutek niedbalstwa pracowników, błędy w oprogramowaniu aplikacyjnym Projektowanie wadliwej infrastruktury informacji: przeładowana pamięć i przeciążone linie dostępu, utrata komunikatów w sieci, „załamanie się” usług w okresach szczytu, nieumyślne zaprzeczenie lub opóźnienie usługi, naruszenie ciągłości usługi



Rys. 1. *Analiza SWOT w procesie zarządzania zabezpieczeniami*

Nie wszystkie zagrożenia są jednakowo prawdopodobne. Według [12], najbardziej obszerną klasą zagrożeń są ludzkie błędy (35%) i pomyłki (25%), a następnie nieuczciwi pracownicy (15%), intruzi z zewnątrz (10%), ogień (7%), woda (5%) i inne niespodziewane zdarzenia (3%). Podobną strukturę zagrożeń można znaleźć w [9, 11]. Decyzja, czy dany zasób należy chronić, zależy od jego wartości oraz znaczenia dla instytucji i powinna być podejmowana przez kierownictwo. To zarząd musi zdecydować, które zasoby chronić, a które pozostawić bez ochrony, przyjmując ryzyko ich uszkodzenia lub zniszczenia. Ogólnie, im zasób jest bardziej unikalny, tym ma większą wartość i bardziej należy go chronić. Należy jednakże pamiętać, że żadne środki zabezpieczeń nie dadzą 100-procentowej gwarancji, że zagrożenie zostanie wyeliminowane. Biorąc pod uwagę koszty eliminowania zagrożeń, nie należy nawet do tego dążyć. W praktyce należy zatem mówić o środkach zabezpieczeń, które redukują, a nie eliminują ryzyko. Warunkiem uznania systemu informatycznego za bezpieczny jest spełnienie kryteriów: poufności, integralności, dostępności, rozliczalności i autentyczności (według normy ISO 7498-2:1989) oraz niezawodności (według normy PN ISO/IEC-I-13335-1) [3].

Immanentną cechą każdego zasobu jest podatność na uszkodzenia (*vulnerability*), która powoduje, że zasób jest narażony na oddziaływanie różnych zagrożeń. Określenie podatności zasobu jest konieczne do zrozumienia systemu zabezpieczeń. Zadanie wcale nie jest trywialne, wymaga bowiem połączenia intuicji, doświadczenia, zdolności uczenia się na błędach i regularnej oceny obecnych zabezpieczeń. Podatność poszczególnych zasobów bywa różna dla różnych organizacji i zmienia się w czasie. Jeśli atakujący nie może znaleźć słabego punktu w systemie obrony, system nie jest podatny, jest odporny [5]. Jednakże, rzadko można osiągnąć stan idealnej odporności. Wyrafinowany napastnik może wykryć słabość w systemie i wykorzystać ją dla własnych korzyści. Niejednokrotnie podatność systemu komputerowego ujawnia się przypadkowo – ktoś nieumyślnie wykona złą procedurę lub naciśnie zły przycisk, w rezultacie system kontroli zostanie pominięty i pojawia się sposobność realizacji ataku na system, który może nastąpić natychmiast lub w dowolnym innym momencie. Przy analizie podatności należy brać pod uwagę aspekt etyczny oraz poziom szkolenia osób, które powinny reagować w momencie wykrycia takiego przypadku.

Opisana definicja podatności jest inna niż definicja według normy PN ISO/IEC-I-13335-1. Tam podatność obejmuje słabość zasobu lub grupy zasobów, która może być wykorzystana przez zagrożenie oraz atrakcyjność aktywów informacyjnych [3].

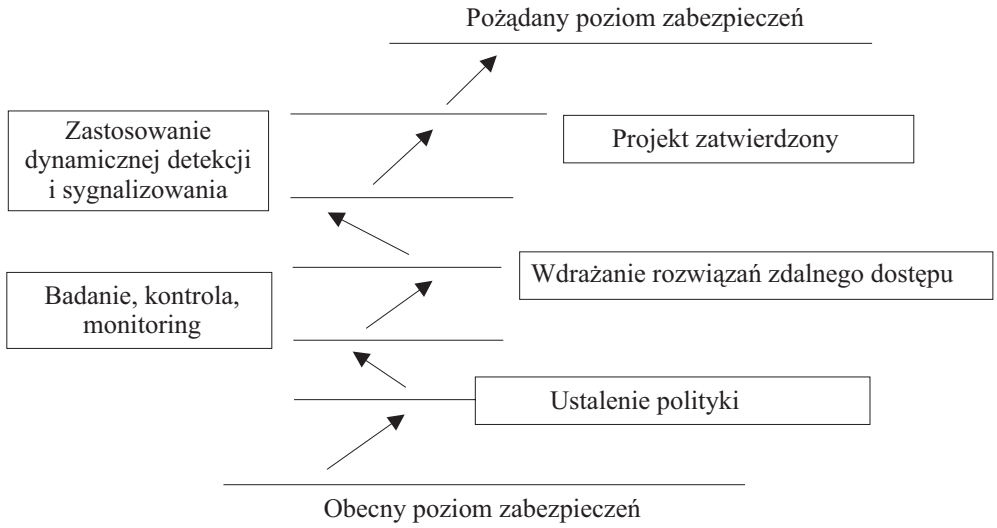
Podatność na zagrożenia i typ oddziaływania to elementy, które najtrudniej określić, ale bez nich model zabezpieczeń nie mógłby istnieć. Ważne jest zatem znalezienie miary zagrożenia zasobu. Często stosowaną metodą jest stymulator efektów, który umożliwia określenie kosztów wygenerowanych efektów przy różnym nasileniu działań stymulatora. Z otrzymanych wartości należy wybrać wariant najgorszy, czyli o najwyższym koszcie i w ten sposób oszacować zagrożenie.

Najogólniej, zabezpieczenia: redukują potencjalne straty i podatność zasobów, zwiększają odporność na atak (środki prewencji), w trakcie ataku wstrzymują emisję skutków negatywnych oraz mogą ułatwiać wykrycie zagrożeń (środki detekcji). Zabezpieczenia mogą powstrzymywać zagrożenia oraz sprawiać, że będą mniej efektywne i mniej prawdopodobne. Są to obiekty autonomicznie definiowane z takimi atrybutami, jak: koszt, wskaźnik deprecjacji, amortyzacji i oczekiwana długość życia.

Przy wyborze zabezpieczeń należy uwzględniać dwa komplementarne punkty widzenia: jak wyeliminować lub zredukować prawdopodobieństwo szczególnych zagrożeń zasobów (orientacja na zagrożenia) oraz co można zrobić, aby uchronić zasoby przed zagrożeniami (orientacja na zasoby).

Strategia i polityka zabezpieczeń

W obrębie programu zabezpieczeń są opracowywane: strategia i polityki zabezpieczeń. Strategia zabezpieczeń wytycza kierunki działań, które instytucja może podjąć, aby podnieść istniejący poziom bezpieczeństwa (rys. 2). Właściwe metodyki postępowania w tym zakresie obejmują ocenę obecnej pozycji instytucji w aspekcie ogólnych zabezpieczeń środowiska przetwarzania oraz określenie celów, które instytucja chciałaby osiągnąć.



Rys. 2. *Przykładowa strategia zabezpieczeń*

Strategia zabezpieczeń powinna składać się z kilku faz [4].

- **Zrozumienie obecnej sytuacji**. Ta faza strategii zabezpieczeń rozpoczyna się od bieżącej oceny poziomu zabezpieczeń istniejących w instytucji. Dokonuje się przeglądu technologii wykorzystanych przez instytucję, jej polityk, procedur oraz dyrektyw. Wykonuje się ocenę ryzyka przy użyciu technik i narzędzi, które testują siłę obecnych mechanizmów zabezpieczeń. W tej fazie należy jasno określić te obszary, które są wykluczone ze sfery zabezpieczeń.
- **Zdefiniowanie środowiska najbardziej pożądanego**. Dokonuje się przeglądu najlepszych polityk, procedur i działań praktycznych. Przeprowadza się rozmowy i wywiady z jak największą liczbą osób, z uwzględnieniem specjalistów technik informatycznych. Na podstawie analizy wymagań tworzy się architekturę zabezpieczeń.
- **Ocena najbardziej pożądanych, alternatywnych rozwiązań i ocena ryzyka**. Dokonuje się przeglądu potencjalnych aplikacji i kierunków rozwoju technik informatycznych.
- **Określenie najlepszej procedury postępowania**. W tej fazie są prezentowane zalecenia szczegółowych rozwiązań i procesów działań. Analizie poddaje się ryzyko oraz koszty, a także opracowuje się plan taktyczny.
- **Rozpoczęcie**. W tej fazie następuje wykonanie planu oraz wdrożenie rekomendowanych rozwiązań technologicznych i proceduralnych.

Jakkolwiek każda instytucja powinna opracować własną strategię zabezpieczeń, jednak można wskazać ich cechy wspólne.

- Celem strategii jest zapewnienie kierunku działań na przyszłość, a nie znalezienie bezpośredniego rozwiązania każdego problemu. Strategia może zalecać rozwiązanie pośrednie, co umożliwi ustosunkowanie się do danego problemu, ale celem końcowym budowy jest utworzenie całościowego obrazu.
- Strategia powinna harmonizować cele ogólne instytucji z celami indywidualnymi jej pracowników.
- Nie wszystkie cele można zrealizować natychmiast, ale wiele z nich można osiągnąć w przyszłości.
- Zmiany celów ekonomicznych oraz kierunków działania instytucji powodują ewolucję strategii. Strategia powinna być stale weryfikowana i modyfikowana.

Polityka zabezpieczeń to zbiór reguł oraz praktyk regulujących sposób planowania, zarządzania i oceny poziomu ochrony zasobów. Indykatorami polityki są:

– zgodność ze standardami, tzn. dostawca zabezpieczeń deklaruje zgodność z określonymi standardami, które mogą być klasyfikowane w poszczególnych grupach jako: techniczne standardy dla formatów danych, protokołów i komunikatów, techniczne standardy dla sprzętu i zabezpieczenia sprzętu oraz standardy dotyczące organizacji zabezpieczenia;
– zgodność z obowiązującym prawem: wykaz przepisów prawnych i uregulowań, z którymi dane rozwiązanie jest zgodne.

Polityka zabezpieczeń powinna kompleksowo uwzględniać rozwiązania techniczne, budowlane, organizacyjne, kadrowe i prawne. Dla każdego z rozwiązań można określić cykl życia, obejmujący: formułowanie koncepcji, implementację, eksploatację rozwiązania oraz jego likwidację (np. jeśli okaże się ono rozwiązaniem niezadowalającym). Taki cykl życia zakłada konieczność weryfikacji proponowanych rozwiązań. Formułowana polityka zabezpieczeń powinna w maksymalnym stopniu wykorzystywać rozwiązania istniejące. W poszukiwaniu rozwiązań należy uwzględnić rozsądny kompromis między wyznaczonym poziomem zabezpieczenia a poziomem nakładów finansowych, które instytucja gotowa jest ponieść.

Polityka zabezpieczeń musi być zgodna z ogólnymi celami działania instytucji i definiowana indywidualnie dla każdej instytucji. Poprawne zdefiniowanie polityki umożliwi zrealizowanie trzech zadań.

- **Zdefiniowanie wymagań w zakresie zabezpieczenia**. Należy wyeliminować niejednoznaczności co do stwierdzenia faktu naruszenia zabezpieczenia, np. brak definicji poufności dokumentów i danych może prowadzić do ujawnienia tajemnic instytucji.
- **Określenie zakresu odpowiedzialności**. Polityka zabezpieczenia przypisuje odpowiednim osobom ustalony zakres uprawnień. Definiowanie zakresu odpowiedzialności umożliwia określenie własności danych oraz zasad ich użytkowania.
- **Określenie zasad dostępu do zasobów systemu informatycznego**. Polityka zabezpieczenia ma wpływ na organizację działania instytucji, tzn. zasady prowadzenia rekrutacji pracowników, bezpieczeństwo i higienę pracy, kontrolę czasu pracy, zasady wprowadzania osób trzecich do instytucji [3].

W każdym przypadku polityka zabezpieczeń powinna zawierać:

– definicję celów zabezpieczenia systemu informatycznego;
– strukturę organizacyjną oraz zdefiniowanie odpowiedzialności za wszystkie aspekty zabezpieczenia;
– opis strategii zarządzania ryzykiem;
– określenie wymagań dotyczących zabezpieczenia systemu informatycznego, a w szczególności: zdefiniowanie klas poufności informacji, określenie obszarów zabezpieczenia systemu informatycznego, zdefiniowanie oraz wdrożenie procedur i regulaminów postępowania, zapewniających osiągnięcie i utrzymanie stanu bezpieczeństwa systemu informatycznego;
– opis wybranych mechanizmów zabezpieczeń;
– sposób akredytacji zabezpieczenia systemu informatycznego [3].

Podstawowym elementem polityki bezpieczeństwa jest dokument jasno określający zakres czynności i obowiązki użytkowników danego systemu. Ze względu na różnorodność zasobów, zagrożeń i mnogość zagadnień, związanych z ich ochroną, w instytucjach formułuje się polityki szczegółowe, obejmujące takie obszary, jak:

– zabezpieczenie informacji;
– środki zabezpieczenia fizycznego (zabezpieczenie podstawowej infrastruktury, budynków, zabezpieczenie sprzętu informatycznego);
– zabezpieczenie oprogramowania aplikacyjnego i sieciowego;
– zabezpieczenie użytkowników, identyfikacja, uwierzytelnianie, kontrola dostępu do zasobów;
– ochrona przed złośliwym oprogramowaniem;
– zabezpieczenie poczty elektronicznej i informacji udostępnianych w Internecie, ochrona prywatności użytkowników Internetu;
– ochrona własności intelektualnej;
– zarządzanie zabezpieczeniami.

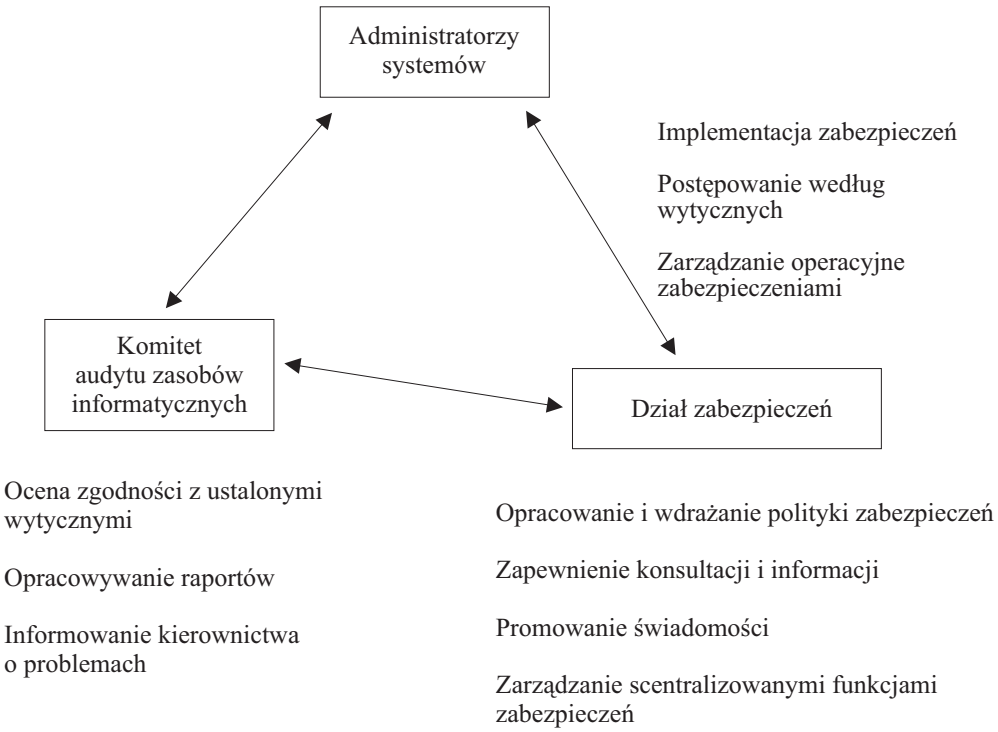
Do realizacji polityki zabezpieczeń jest konieczny wybór właściwych środków zabezpieczeń. Jest to proces złożony, który powinien uwzględniać następujące aspekty: technologię, procedury, kadry i fizyczne zabezpieczenie. Ważne jest zrozumienie, w jaki sposób każdy z tych środków oddziałuje na instytucję. Pomocne może być uwzględnienie następujących wytycznych.

- **Unikanie oddziaływania**. Jeśli działalność jest bardzo ryzykowna, należy ją wyeliminować, np. wyeliminowanie możliwości zapłaty gotówkowej pozwala uniknąć kradzieży pieniędzy.
- **Analiza oddziaływania**. Ze względu na możliwą wadliwość systemu przekazywania informacji należy, np. zintensyfikować działania kontrolne.
- **Redukcja oddziaływania**. Można ją osiągnąć, np. przez zainstalowanie nadmiarowych elementów systemowych, umożliwiających utrzymanie ciągłości działania w przypadku awarii w głównym systemie.
- **Redukcja prawdopodobieństwa**. Można podać przykład komputera, który nie będzie narażony na pożar, jeśli zostanie ulokowany w pokoju bez materiałów łatwo palnych, z systemem wykrywania dymu.

Audyt zabezpieczeń systemów informatycznych

Ocena polityki zabezpieczeń zasobów informatycznych jest prowadzona przez dział audytu (rys. 3).

W literaturze przedmiotu do tej pory brak jest zgodności poglądów, czym jest audyt. Dla jednych audyt oznacza proces gromadzenia danych na temat działań i zasobów systemów komputerowych. Inni uważają, że audyt jest przeglądem istniejących mechanizmów kontrolnych i wykrywaniem bezprawnych działań. Zgodnie z [4], audyt jest procesem, w którym niezależna jednostka gromadzi i ocenia dowody, świadczące o różnicach między wartościami wskaźników mierzalnych a ustalonymi kryteriami. Przykładowo, audyt finansowy polega na formalnym przeglądzie zestawień finansowych, jego rola ogranicza się do oceny, czy finansowe raporty pozostają w zgodności z ustalonymi praktykami księgowania. Raport audytu finansowego powinien zawierać informacje o istotnych odchyleniach, które mogą wynikać, np. z niewłaściwej interpretacji zasad rządzących zestawieniami finansowymi.



Rys. 3. *Zależności organizacyjne w zarządzaniu zabezpieczeniami*

Audyt w środowisku informatycznym powinien być niezależnym przeglądem aplikacji, systemu informatycznego i sieci do oceny zgodności z ustaloną polityką, przyjętymi wytycznymi oraz standardami. Wyniki audytu powinny być podstawą do działań prewencyjnych, zapobiegawczych lub wdrożenia stosownych mechanizmów zabezpieczeń. W ten sposób audyt może przyczynić się do uzyskania przez instytucję wyższego poziomu bezpieczeństwa. Jednakże, jeśli funkcja audytu jest realizowana w odosobnieniu, bez partycypacji i interakcji innych grup pracowniczych (w tym zwłaszcza kierownictwa instytucji), to audyt nie da pożądanych efektów.

Istotne jest pytanie, kto powinien prowadzić audyt zabezpieczeń zasobów informatycznych. W wielu instytucjach funkcjonuje komitet audytorski, powołany do audytu finansowego. Koncepcja komitetu audytorskiego może być przydatna również do audytu zabezpieczeń systemów informatycznych. Członkowie komitetu audytorskiego mogą wywodzić się z działu kontroli wewnętrznej lub działu informatyki. Niezależnie od usytuowania organizacyjnego, komitet taki powinien kierować się następującą zasadą: brak władzy wykonawczej oraz funkcji podejmowania decyzji i nadzoru, przy jednoczesnym zachowaniu prawa dostępu do danych (w tym finansowych), możliwości korzystania z rad konsultantów, zwoływania spotkań *ad hoc*, czy żądania obecności pracowników na tych spotkaniach. Członkowie komitetu mają także prawo do odpowiedniego szkolenia oraz informacji związanej z audytem i księgowością. Przy zachowaniu tych wymagań komitet może być jednostką opiniującą i wspomagającą decyzje kierownictwa. To wspomaganie wykracza poza analizę zestawień finansowych. Wielkość i struktura instytucji powinna mieć bezpośredni wpływ na liczebność komitetu audytorskiego oraz przypisane mu funkcje.

Ciągłość członkostwa w komitecie audytorskim jest ważna do realizacji zadań komitetu oraz jego funkcji motywacyjnych, ale jednocześnie zaleca się częściową rotację członków komitetu, aby zapewnić dopływ nowych doświadczeń. Przy doborze członków komitetu należy brać pod uwagę trzy zasadnicze cechy osobowe: wiedzę, niezależność i zaufanie. Podstawowe zasady działania komitetu (w tym czas trwania kadencji członków) powinny znaleźć się w statucie. Statut powinien być:

– zaaprobowany przez organ zarządzający,
– zbiorem wytycznych działania dla członków komitetu,
– przeglądany regularnie, aby zaspokoić potrzeby instytucji.

Innym rozwiązaniem, często stosowanym przez instytucje, jest rozszerzanie zakresu kompetencji działów wewnętrznej kontroli finansowej na sferę informatyki. Ogólnie, prowadzenie audytu przedsięwzięć informatycznych wydaje się uzasadnione ze względu na konieczność:

– ponoszenia wysokich nakładów inwestycyjnych na systemy informatyczne,
– oszacowania ogólnego poziomu bezpieczeństwa w instytucji,
– harmonizowania działań wewnętrznych i dyscyplinowania pracowników,
– wskazania działań, zmierzających do podniesienia poziomu zaufania do krytycznych aplikacji i systemów.

Obszary badań audytu zabezpieczeń systemów informatycznych

Uzyskanie pewności działania zabezpieczeń na etapie eksploatacji systemu informatycznego polega na sprawdzeniu utrzymywania ich skuteczności w czasie (wykrycie ewentualnych metod obchodzenia zabezpieczeń, ich podatności na dynamicznie zmieniające się środowisko lub braku przestrzegania odpowiednich procedur). Do utrzymania stanu zabezpieczeń systemu informatycznego powinny być stosowane dwie podstawowe metody:

– **audyt systemu**, tj. jednorazowe lub okresowo powtarzające się całościowe szacowanie poziomu bezpieczeństwa;
– **monitorowanie systemu**, tj. działanie o charakterze ciągłym, mające na celu nadzór nad zmieniającym się systemem, jego użytkownikami oraz środowiskiem.

Audyt może być realizowany różnymi metodami. Należą do nich:

- zautomatyzowane narzędzia wyszukiwania słabości systemu zabezpieczenia (np. narzędzia weryfikacji integralności plików, wyszukiwania słabych haseł, kontroli aktualności modyfikacji w systemach i aplikacjach);
- wewnętrzne mechanizmy audytu (badania, ankiety, obserwacje, testy zabezpieczeń i danych);
- testy penetracyjne (próby włamania się do systemu przy użyciu różnych metod, w tym nielegalne uzyskanie informacji od użytkowników); z uwagi na potencjalnie znaczne ryzyko wyrządzenia szkody w systemie informatycznym testy penetracyjne powinny być wykonywane tylko przez kompetentnych specjalistów pracujących pod nadzorem.

Wśród narzędzi monitorowania oprogramowania można wymienić: skanery wirusów, programy weryfikujące integralność plików i baz danych, narzędzia kontroli oraz oceny parametrów jakościowych działania systemu.

Tradycyjny audyt systemów komputerowych obejmuje trzy obszary zagadnień: przegląd zabezpieczeń, stwierdzenie zgodności zabezpieczeń z polityką i badanie śladu rewizyjnego (*audit trail*). Ślad rewizyjny jest zbiorem danych, generowanych przez działania w systemie komputerowym. Zapewnia informacje dotyczące działań użytkowników i procesów. Może być stosowany do śledzenia bezprawnych działań. Badanie śladu rewizyjnego umożliwia:

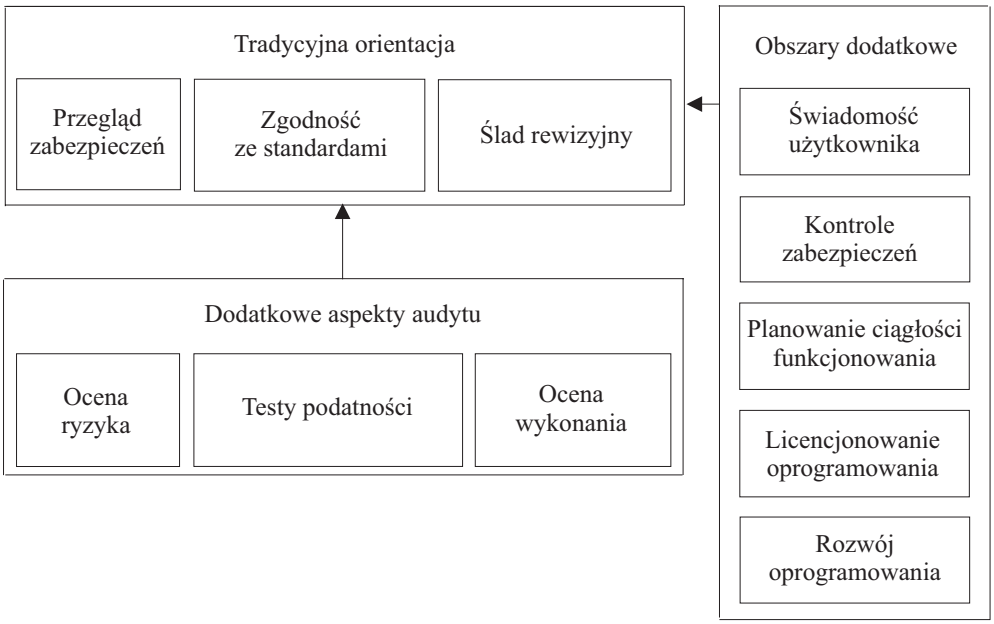
- wykrywanie nieuprawnionych działań, takich jak próby zgadywania haseł (np. rejestrowanie prób dostępu zakończonych niepowodzeniem);
- odtworzenie historii nieuprawnionego dostępu (np. zalogowania i zmiany w prawach dostępu);
- śledzenie dostępu do zasobów systemów;
- doprowadzenie do stanu sprzed ataku (np. odtworzenia plików konfiguracyjnych systemu).

W tym ujęciu, pojęcie audytu systemu jest rozumiane jako przegląd rejestrów (sekwencji rekordów), zawierających informacje o zdarzeniach w systemie operacyjnym, aplikacjach oraz działaniach użytkowników. Rejestry te zapewniają systemowi rozliczalność. Audyt rejestrów systemowych to także podstawowe źródło informacji przy wykrywaniu incydentów i rekonstrukcji zdarzeń. Rejestry zdarzeń systemowych powinny opisywać m.in. każdą próbę dostępu do aktywów systemu informatycznego (zakończoną sukcesem lub nie), identyfikator użytkownika, datę i czas próby dostępu, czas zarejestrowania oraz czas wyrejestrowania się użytkownika, wykorzystywane aktywa i funkcje (aplikacje programowe), które zostały wywołane po zarejestrowaniu się użytkownika, datę i czas zawieszenia oraz ponownego restartu systemu informatycznego [2]. Audyt jest potwierdzeniem działań poprawnych i wykrywaniem naruszenia systemu. W systemie powinny być zapisywane informacje o niecodziennych zdarzeniach, gdyż mogą one być przydatne w późniejszym czasie. Przykładowo, zapis powinien uwzględniać adresy sieciowe stacji, z których poszczególni użytkownicy (włączając intruza) próbowali się zarejestrować w systemie i dotyczy to zarówno działalności użytkownika zwykłego, jak i uprzywilejowanego (administratora).

Proces wykrywania naruszeń składa się z dwóch części. Część pierwsza jest związana z tworzeniem rekordów śledzenia (*audit records*). Zapisywane są m.in. udane i nieudane próby rejestracji w systemie, czytanie lub zapis do plików o zwiększonych wymogach bezpieczeństwa. Część druga dotyczy sprawdzania zapisów w dzienniku, czy nie została przekroczona wartość progowa, wskazująca wystąpienie

zdarzenia niepożądanego. W tej części też jest generowany raport, zawierający informacje o niepożądanych zdarzeniach, który powinien być przejrzany przez administratora w celu znalezienia śladów potencjalnego włamania. Przykładowy model wykrywania naruszeń systemu można znaleźć w [7].

Obecnie zadania audytu wykraczają poza kontrolę zabezpieczeń, obejmując również ocenę wykonania i zarządzanie ryzykiem zniszczenia uszkodzenia zasobów informatycznych (rys. 4). Audyt wykonania jest szczególnym rodzajem audytu, który ma ustalić, czy system zaspokaja cele ekonomiczne, dla których został utworzony, a także dokonać przeglądu opłacalności systemu.



Rys. 4. *Interpretacje audytu zabezpieczeń systemów informatycznych*

Ryzyko jest potencjalną stratą, która istnieje zarówno w wyniku zagrożenia, jak i słabości systemu. Jednakże, zgodnie z normą PN ISO/IEC-I-13335-1, ryzyko jest zbiorczą miarą prawdopodobieństwa i wagi sytuacji, w której dane zagrożenie wykorzystuje określoną słabość, powodując stratę lub uszkodzenie aktywów systemu informatycznego, a zatem pośrednią lub bezpośrednią szkodę dla instytucji [3]. W efektywnym zarządzaniu ryzykiem jest istotne określenie pod względem ilościowym i jakościowym elementów ryzyka oraz zredukowanie go do akceptowanego poziomu.

Sterowanie ryzykiem wymaga rozwoju opcjonalnych planów dla różnych sytuacji, które mogą wystąpić, a także wdrażania właściwych planów korygujących. Poszukuje ono sposobów podejmowania decyzji, czy i kiedy przyjąć, uniknąć oraz złagodzić ryzyko i ile wydać na ten proces. Dla sterującego ryzykiem zakres możliwości sięga od określenia „nie warto podejmować działań" do uznania, że „stracimy wszystko, jeśli to padnie". Sposób, w jaki menedżer ryzyka decyduje, co i gdzie znajduje się na skali ryzyka, opiera się na zrozumieniu natury instytucji oraz roli i znaczenia poszczególnych czynników do osiągnięcia sukcesu lub doznania niepowodzenia. Techniką często stosowaną w zarządzaniu ryzykiem jest podejście osłaniania. Należy ustalić listę ataków, listę środków i sposobów obrony oraz określić, w jakim stopniu każdy ze sposobów uniemożliwia każdy z podanych sposobów ataku. Celem

zarządzania ryzykiem jest wtedy ustalenie równowagi między tymi dwoma oddziaływaniami. Zgodnie z tym podejściem, menedżerowie powinni podjąć decyzje, jaki rodzaj ataku zostanie uniemożliwiony (wyeliminowany przez obronę) i czy obrona zdoła oprzeć się tym atakom. Sterowanie ryzykiem wiąże się z podejmowaniem i wykonywaniem decyzji – dotyczących przyszłych zdarzeń (sytuacji), które mogą powodować niekorzystne, niepożądane efekty – oraz tworzeniem planu strategicznego, działań taktycznych i operacyjnych, zapewniających radzenie sobie w sytuacjach zagrożeń, unikanie lub redukowanie niepotrzebnego ryzyka i utrzymywanie ryzyka na akceptowalnym poziomie.

Typowa analiza ryzyka obejmuje następujące etapy.

- **Identyfikowanie zasobów**. Zasoby mogą być częścią systemu informacji, mogą obejmować sprzęt, oprogramowanie wraz z dokumentacją, dane użytkowników i informatyków.
- **Określenie podatności, słabości systemu informatycznego**. Słabością systemu mogą być: osoba, zagrożenie, działanie lub idea, powodujące utratę tajności informacji, integralności i dostępności informacji oraz naruszenie jakiegokolwiek ustalonego środka lub sposobu zabezpieczeń.
- **Ocena prawdopodobieństwa nieautoryzowanego wykorzystania zasobów**. Estymacja jest oparta na kontroli w miejscu oraz ocenie prawdopodobieństwa bezprawnego dostępu i użycia.
- **Obliczanie rocznej oczekiwanej straty**. Należy uwzględnić: utratę sposobności biznesowych, koszty odzysku danych i ich rekonstrukcji, straty w sprzedaży i straty w relacjach publicznych z innymi jednostkami.
- **Badanie nowych sposobów kontroli i oceny ryzyka**. Inne środki i sposoby analizy ryzyka są oceniane w relacji do potencjalnych zagrożeń oraz słabości zasobów informatycznych.
- **Określenie oczekiwanej opłacalności przeprowadzonej analizy ryzyka**. Należy odpowiedzieć na pytanie, czy analiza ryzyka jest przedsięwzięciem efektywnym w sensie redukcji ryzyka zniszczenia zasobów i utraty wartości informacji.

Ta tradycyjna metodyka analizy ryzyka zapewnia racjonalne podejmowanie decyzji z punktu widzenia ochrony informacji. Zarządzanie ryzykiem jest pojęciem szerszym, obejmującym całkowity proces identyfikowania, obserwacji, eliminowania lub minimalizowania niepewnych zdarzeń, które mogą wpływać na zasoby systemu. Proces obejmuje: analizę ryzyka, analizę korzyści i kosztów, selekcję, wdrażanie, testowanie, ocenę zabezpieczeń i ogólny przegląd zabezpieczenia. Ocena słabości zabezpieczeń może być prowadzona w wybranych miejscach systemu [10]. Inni autorzy [8] uważają, że nie wszystkie straty można określić jako bezpośredni skutek określonego zdarzenia, wiele z nich może wystąpić później, zatem nie zawsze istnieje możliwość natychmiastowej oceny zaistniałej sytuacji.

W efekcie, tradycyjna analiza ryzyka została zmodyfikowana przez wprowadzenie i zastosowanie podejścia opartego na roli. Rola odnosi się do funkcji, którą jednostka pełni w modelu i jest definiowana przez określenie odpowiedzialności oraz oczekiwań użytkownika, zgodnie z przyjętym scenariuszem działań. Przykładem roli jest właściciel informacji. Role umożliwiają modelowanie zachowań dla lepszej symulacji rzeczywistych sytuacji. Z kolei aktor jest terminem używanym w odniesieniu do encji, która pełni zdefiniowaną rolę w modelu. Model analizy ryzyka (*Role-Based Risk Analysis* – RBRA) definiuje role i aktorów oraz umożliwia analizę według scenariuszy. Poza identyfikacją zagrożeń, analiza ryzyka oparta na rolach wprowadza dwa dodatkowe etapy: definiowanie roli i aktora. W takim ujęciu proces analizy ryzyka obejmuje: definiowanie ról, identyfikowanie aktorów, identyfikowanie zasobów z perspektywy aktorów, określenie słabości systemu, oszacowanie prawdopodobieństwa nadużyć, obliczanie rocznej oczekiwanej straty, badanie stosowanych zabezpieczeń, projektowanie rocznych oszczędności w wyniku zastosowania zabezpieczeń.

Badanie podatności systemów informatycznych na uszkodzenia i zniszczenia jest prowadzone przy użyciu testów. W testach podatności są stosowane narzędzia informatyczne, którymi posłużyłby się haker do uzyskania bezprawnego dostępu do systemu. Typowe działania obejmują:

– sprawdzenie tzw. słabych haseł,
– próby przejęcia zbioru haseł,
– sprawdzenie ochrony zbiorów,
– próby dostępu do danych.

Celem testów podatności jest znalezienie słabości przy użyciu metod, którymi posłużyłby się intruz. Do wyeliminowania tych słabości mogą być użyte: wiedza zdobyta podczas testowania, stosowne mechanizmy i środki zapobiegawcze. Testowaniem mogą być objęte: pojedynczy system, aplikacja lub sieć systemów.

Kształtowanie świadomości użytkowników systemów informatycznych i kontrola tej wiedzy (testy, pozorowane ataki) wynika z przekonania o konieczności współodpowiedzialności pracowników za zabezpieczenia. Bez wiedzy trudno oczekiwać poprawnych procedur zabezpieczeń. Konieczne jest uczenie się na wszystkich szczeblach zarządzania. Audyt powinien obejmować także treść szkoleń dla użytkowników. Formy uczenia się przedstawiono w tablicy 2.

Tabl. 2. Studium porównawcze form uczenia

Atrybut	Uświadamianie	Szkolenie	Edukacja
Podstawowe pytanie	„Co”	„Jak”	”Dlaczego”
Poziom	Informacja	Gromadzenie wiedzy	Analiza wiedzy
Cel uczenia	Rozpoznanie i zwrócenie uwagi	Kształtowanie umiejętności	Zrozumienie
Przykładowa metoda uczenia się	Media: filmy, plakaty	Praktyczne instrukcje: wykłady i demonstracje, studia przypadków, przykładowe działania praktyczne	Instrukcje teoretyczne: seminaria i dyskusje, studia, badania naukowe
Środki testowania	Test wielokrotnego wyboru	Rozwiązywanie problemu, tzn. rozpoznanie i ustalenie rozwiązania	Eseje
Okres oddziaływania	Krótkookresowe	Średniookresowe	Długookresowe
Opracowano na podstawie publikacji NIST Special Publication 800-16, US Department of Commerce, Technology Administration National Institute of Standards and Technology, Gaithersburg MD 20899-0001, April 1998, Information Technology Security Training Requirements: A Role- and Performance-Based Model.			

Celem planowania ciągłości działania jest zapewnienie ciągłości funkcjonowania wszystkich komórek organizacyjnych przedsiębiorstwa w warunkach wystąpienia zdarzeń zakłócających normalne działanie,

takich jak katastrofy i awarie. Dotyczy to nie tylko systemów komputerowych, ale także ręcznych procedur niezbędnych do realizacji funkcji przedsiębiorstwa [6]. Przed wdrożeniem planu utrzymania ciągłości działania należy wykonać prace przygotowawcze takie, jak: opracowanie i wdrożenie procedur tworzenia kopii bezpieczeństwa, zawarcie oraz negocjowanie kontraktów z dostawcami sprzętu i usług, uwzględniających potrzeby utrzymania ciągłości działania systemu informatycznego, utworzenie rezerwowych systemów i zarezerwowanie budynków. Regularnie powinny być przeprowadzane testy gotowości: wykonanie planu powiadamiania, funkcjonalne testy generatorów rezerwowego zasilania, symulacje uszkodzeń poszczególnych elementów systemu informatycznego oraz ich ponowne uruchomienie, sprawdzanie odtwarzalności kopii bezpieczeństwa, ćwiczenia przeciwpożarowe. Z tym jest związana okresowa kontrola: urządzeń, umożliwiających wstęp do budynków i pomieszczeń, przeciwpożarowa, zasilania w energię elektryczną, systemów ogrzewania i klimatyzacji oraz urządzeń sanitarnych.

Wdrożenie programu zarządzania oprogramowaniem jest najbardziej efektywnym, pod względem kosztów, sposobem zoptymalizowania zwrotu wydatków instytucji na oprogramowanie. Niemożność określenia, jakie zasoby ma instytucja i gdzie się one znajdują, prowadzi do wielu problemów:

– zasoby firmy są uszczuplane przez straty, nadużycia i kradzieże;
– do środowiska komputerowego dostają się wirusy i inne elementy zagrażające bezpieczeństwu;
– koszty integracji rosną w wyniku niezgodności systemów i różnorodności wersji oprogramowania;
– rosną koszty szkoleń, pomocy technicznej i serwisu;
– w związku z łamaniem prawa autorskiego rośnie ryzyko grzywien i kar;
– rosną całkowite koszty eksploatacji.

Audyt oprogramowania umożliwia ustalenie, w jaki sposób oprogramowanie jest nabywane, dystrybuowane i wykorzystywane w instytucji, służy zatem optymalizacji przyszłych zakupów. Polega on na kontroli oprogramowania zainstalowanego w komputerach pracowników danej instytucji, sprawdzeniu, czy jest ono zgodne z posiadaną licencją i czy są zainstalowane programy antywirusowe.

Ostatnim zagadnieniem audytu jest sterowanie procesem rozwoju oprogramowania. Oznacza to, że proces przeprowadzania zmian w oprogramowaniu powinien być kontrolowany w taki sposób, aby zminimalizować ryzyko uszkodzenia systemu informatycznego i jego zabezpieczeń. Procedura dokonywania zmian powinna obejmować: uzgodnienie propozycji zmiany oraz udokumentowanie uzgodnień między wszystkimi upoważnionymi użytkownikami, administratorami, projektantami i wykonawcami, analizę wpływu proponowanych zmian na działanie mechanizmów zabezpieczeń oraz przeprowadzenie testów integralności systemu zabezpieczenia, zidentyfikowanie wszystkich aktywów systemu informatycznego, w których należy dokonać stosownych zmian, zatwierdzenie proponowanych zmian przez upoważnione osoby, uaktualnienie dokumentacji systemu i zapisanie kopii archiwalnych poprzednich wersji.

Zakończenie

Audyt zabezpieczeń systemów informatycznych jest przedsięwzięciem koniecznym do oceny polityki zabezpieczeń. Można jednak przypuszczać, że – ze względu na swą przedstawioną w opracowaniu złożoność – w praktyce nie jest realizowany aż tak kompleksowo. Należy zwrócić uwagę na założenia, jakie powinny być spełnione, aby audyt zabezpieczenia systemów informatycznych był

przedsięwzięciem racjonalnym i skutecznym. Otóż, zawsze powinny być uwzględnione zasady stosowności podmiotów i przedmiotów audytu, bezstronności, obiektywności oceny, powtarzalności i wielokrotności realizacji. Wielokrotność realizacji różni się od powtarzalności tym, że wielokrotność realizacji jest związana z zapewnieniem zgodności i identyczności oceniających, podczas gdy powtarzalność dotyczy zgodności i identyczności wyników. U podstaw zasad leżą założenia dotyczące środowiska oceny i działań zaangażowanych stron, a mianowicie założenie analizy opłacalności przedsięwzięcia oraz wyboru metodyki oceny.

Bibliografia

[1] Ahuja V.: *Bezpieczeństwo w sieciach*. Warszawa, Wyd. Mikom, 1996

[2] Andrukiewicz E.: *Audyt i systemy*. PCkurier, 1999, nr 6, s. 96–101

[3] Andrukiewicz E.: *Terminologia i nie tylko*. PCkurier, 1998, nr 25, s. 116–120

[4] Bruce G., Dempsey R.: *Security in Distributing Computing*. Prentice-Hall, NJ, Hewlett-Packard Professional Books, 1997

[5] Caelli W., Longley D., Shain M.: *Information Security Handbook*. Nowy Jork, Macmillan, 1994

[6] Dabiński W.: *Planowanie ciągłości działania*. Informatyka, 1997, nr 2

[7] Denning D.E.: *An intrusion detection model*. IEEE Transactions on Software Engineering, vol. SE-13, no. 2, 1987, s. 222–232

[8] Drake D.L., Morse K.L.: *The security specific eight stage risk assessment methodology*. W: *Proceedings of the 17th National Computer Security Conference*, 1994

[9] Firdman G.R.: *Strategic Information Systems: Forging the Business & Technology Alliances*. Nowy Jork, McGraw-Hill, 1991

[10] Jaworski L. M.: *Tandem threat scenarios: a risk assessment approach*. W: *Proceedings of the 16th National Computer Security Conference*, September 1993

[11] Molski M.: *Podstawy bezpieczeństwa systemów informatycznych*. Bydgoszcz, Wyd. MSG Media, 1998

[12] *Vulnerability Assessment: Empowering IS to Manage Actual Risk*. Boston, Aberdeen Group, September 1997

Małgorzata Pańkowska

Dr Małgorzata Pańkowska (1957) – absolwentka kierunku Cybernetyka Ekonomiczna i Informatyka Akademii Ekonomicznej w Katowicach (1981); nauczyciel akademicki i pracownik naukowy Akademii Ekonomicznej w Katowicach (od 1990), School of Business na uniwersytecie Carleton University w Ottawie (1993–1994) oraz Faculty of Science and Computing na uniwersytecie University of Luton w Luton w Wielkiej Brytanii (1997); autorka około 50 artykułów; zainteresowania naukowe: gospodarka elektroniczna, zarządzanie zasobami informatycznymi w organizacjach gospodarczych.
e-mail: pank@figaro.ae.katowice.pl