PRACE NAUKOWE AKADEMII EKONOMICZNEJ WE WROCŁAWIU
Nr 1150 — 2007
Informatyka Ekonomiczna 10

Marianna Kowalska

AUDYT INFORMACYJNEGO SYSTEMU SIECIOWEGO

1. Wstęp

Systemy sieciowe stanowią obecnie najwyższy poziom rozwoju i zastosowania informatyki w przedsiębiorstwie. Użytkowanie tych systemów to proces mający na celu korzystanie z systemu zgodnie z jego przeznaczeniem. Dążenie do wykorzystania zakresu użytkowego wymaga zastosowania specyficznych metod, procedur, a także przepisów prawa.

W każdej firmie, która korzysta z technologii informacyjnej, powstają różne rodzaje ryzyka, wiążące się z poszczególnymi elementami systemu komputerowego, tj. sprzętem, oprogramowaniem, aplikacjami, zasobami ludzkimi, a także środowiskiem sieciowym. Ryzykiem tym można zarządzać dzięki szczegółowej identyfikacji wszystkich problemów. Doskonałym narzędziem do identyfikacji tych problemów jest audyt systemu informacyjnego. Audyt ten powinien się odbywać się zgodnie z przyjętymi procedurami oraz przepisami. Dzięki temu, że proces audytu jest sformalizowany, przedsiębiorstwo może mieć pewność, że eksploatowany system jest wiarygodny. Jego zasoby są kontrolowane z dużą dokładnością i w odpowiednim stopniu szczegółowości, dokumentacja eksploatacyjna jest pełna i kompletna.

W niniejszym artykule przedstawiono wybrane zagadnienia dotyczące audytu systemu sieciowego, takie jak: unormowania prawne, procedura audytowa oraz udokumentowanie prac audytowych.

2. Pojęcie audytu i przesłanki jego stosowania

W literaturze przedmiotu nie ma zgodności poglądów na temat tego, czym jest audyt systemów informacyjnych[1]. Niektórzy autorzy określają go jako proces gromadzenia danych o działaniach i zasobach systemów komputerowych. Inni

[1] W opracowaniu używa się zamiennie pojęć: system informacyjny, system informatyczny, system sieciowy.

uważają, że audyt jest przeglądem istniejącej kontroli i wykrywania bezprawnych działań. Według jeszcze innych autorów audyt jest to ocena niezależna i obiektywna tych czynników, które wpływają na wiarygodność i rzetelność systemów informacyjnych. Ocena ta nie ogranicza się jednak tylko do samych systemów, jej elementami są też (Bojanowski 2003):

- procedury operacyjne opierające się na wykorzystaniu systemów,
- zasady wdrożenia, eksploatacji i rozwoju systemów,
- sposób organizacji pracy służb informatycznych i dostawców.

Według innych autorów audyt zajmuje się przede wszystkim badaniem, oceną sprawności i skuteczności systemu kontroli wewnętrznej dla różnych procesów występujących w firmie. Celem tego działania jest usprawnienie funkcjonowania firmy.

Jak wynika z wybranych przykładowo definicji, audyt może być różnie definiowany i odnoszony do zróżnicowanego zakresu przedmiotowego działań. Audyt informatyczny może być traktowany jako samodzielne przedsięwzięcie lub jako element pomocniczy audytu operacyjnego czy finansowego.

I tak, jeżeli audyt informacyjny jest samodzielnym przedsięwzięciem, to ma duży zakres, od oceny zarządzania bezpieczeństwem pojedynczego stanowiska do oceny zarządzania bezpieczeństwem systemów informacyjnych w skali całej firmy. Zakres przedmiotowy audytu zależy od rodzaju systemu informatycznego funkcjonującego w danej firmie.

W systemach autonomicznych realizowane są pojedyncze systemy informatyczne. W praktyce gospodarczej są wykorzystywane następujące rodzaje systemów informatycznych:

- systemy autonomiczne – zwane także dziedzinowymi lub agendowymi,
- systemy cząstkowe funkcjonujące w oparciu o wspólną bazę danych,
- zintegrowane systemy sieciowe, np.: finansowo-księgowe, kadrowo-płacowe, gospodarki materiałowej.

Każdy z tych systemów funkcjonuje na podstawie własnej, niezależnej bazy danych. W przypadku tych systemów audyt dotyczyłby: oprogramowania aplikacyjnego, organizacji wejścia, zbiorów danych, procesu przetwarzania, organizacji wyjścia oraz wyposażenia technicznego.

W przypadku systemów cząstkowych zorganizowanych w oparciu o wspólną bazę danych informacje przetwarzane są szybciej i nie ma problemów z redundancją danych. Systemy te mogą funkcjonować jako scentralizowane lub zdecentralizowane[2]. Audyt systemów scentralizowanych będzie obejmował (w porównaniu do audytu systemów autonomicznych) dodatkowo procedury związane z udostępnianiem informacji ze wspólnej bazy danych. W systemach zdecentralizowanych audytor, przeprowadzając czynności kontrolne, powinien sprawdzić

[2] Systemy zdecentralizowane są zorganizowane w postaci tzw. sieci lokalnej.

procedury przekazywania i udostępniania danych, oprogramowanie sieciowe oraz poprawność działania sieci lokalnej.

Najwyższym etapem w rozwoju systemów informatycznych są systemy zintegrowane. Funkcjonują one jako rozległe systemy sieciowe[3], często wykorzystując sieć Internet. Systemy te z reguły pracują w czasie rzeczywistym. Do zakresu audytu tego typu systemów należą (dodatkowo w stosunku do systemów cząstkowych zorganizowanych w oparciu o wspólną bazę danych): procedury dostępu z zewnątrz do danych zgromadzonych w bazie i mechanizmy szyfrujące przekazywanie danych.

Niezmiernie istotne, a często lekceważone przez audytora, są umiejętności personelu działu informatyki w zakresie obsługi systemu oraz procedury związane z dokumentacją dotyczącą wprowadzania modyfikacji i usprawnień w systemie.

Zadania audytu informacyjnego systemów sieciowych można podzielić na cztery główne grupy, tj:

1) weryfikację zgodności systemów informacyjnych z wymogami prawa, pozwalającą na uzyskanie niezależnej oceny stopnia spełnienia wymogów narzuconych przez przepisy prawa oraz uzyskanie rekomendacji w stosunku do niezbędnych modyfikacji systemów i środowiska;

2) weryfikację stanu bezpieczeństwa systemów informacyjnych, pozwalającą na uzyskanie niezależnej oceny stopnia zabezpieczenia przed zewnętrznymi i wewnętrznymi zagrożeniami systemu informacyjnego;

3) weryfikację stanu zasobów systemów informacyjnych, pozwalającą na uzyskanie wyczerpujących i aktualnych informacji o zainstalowanym oprogramowaniu, posiadanych licencjach, zasobach informacyjnych i technicznych oraz na uzyskanie niezależnej oceny w tym zakresie.

4) weryfikację stanu zasobów sieciowych, pozwalającą na uzyskanie niezależnej oceny prawidłowości funkcjonowania sieci, połączeń sieciowych oraz stanu bezpieczeństwa sieci.

Ze względu na ograniczone ramy w dalszej części opracowania przedmiotem rozważań będzie pierwsza grupa zagadnień dotycząca unormowań prawnych, a także procedury audytu sieciowego.

3. Unormowania prawne w zakresie audytu

W Polsce prowadzi się prace, których celem jest opracowanie jednoznacznych przepisów nakładających obowiązek prowadzenia audytu systemów informacyjnych, w tym także systemów sieciowych. Wydano już jednak kilka regulacji prawnych ściśle związanych z audytem; są to np.:

- ustawa o rachunkowości z 29 września 1994 r. (DzU nr 86 z 2002 r. – tekst jednolity), nakładająca na biegłego rewidenta obowiązek wydawania opinii

[3] Rozległe systemy sieciowe charakteryzują się tym, że nie ma praktycznie ograniczeń lokalizacji, jeśli chodzi o połączenia między użytkownikiem końcowym a bazą danych systemu.

o audytowanym sprawozdaniu finansowym, a więc także o księgach rachunkowych prowadzonych za pomocą komputera,
- ustawa z 27 lipca 2001 r. o zmianie Ustawy o finansach publicznych (DzU nr 77 z 2002 r.),
- ustawa o biegłych rewidentach i ich samorządzie (DzU nr 31 z 2001 r.),
- ustawy o działach administracji rządowej oraz ustawy o służbie cywilnej, które mówią m.in. o audycje wewnętrznym w przedsiębiorstwach państwowych,
- międzynarodowe standardy rewizji finansowej (Kurzawski, Mierzejewski 2004, s. 25),
- rekomendacje nadzoru dla sektora bankowego (GINB).

W ustawie o rachunkowości mówi się m.in. o wymogach nałożonych na ,,księgi rachunkowe prowadzone za pomocą komputera". Ze względu na to, że księgi rachunkowe stanowią podstawę sporządzania sprawozdania finansowego, audytor (biegły rewident), aby wydać opinię o sporządzonym sprawozdaniu finansowym, musi ocenić prawidłowość działania systemów informatycznych rachunkowości. Prace związane z przeglądem środowiska komputerowego stają się integralną częścią badania sprawozdania finansowego. Audytor sprawozdań finansowych musi określić swój poziom zaufania do procesów przetwarzania danych w badanej organizacji. Do tego celu może wykorzystać specjalne procedury, takie jak: test na istnienie, ustalenie ryzyka ogólnego czy ryzyka kontroli.

O audycie systemu informacyjnego mówią m.in. rekomendacje GINB, ale dotyczą one jedynie sektora finansowego i nie mają charakteru obligatoryjnego. Warto zaznaczyć, iż nie należy łączyć wymagań określanych w innych aktach prawnych np. w zakresie ustaw odnoszących się do bezpieczeństwa, poufności informacji, przestępstw komputerowych z wymogiem przeprowadzania audytu. Zapewnienie bezpieczeństwa to nie to samo co przeprowadzenie audytu bezpieczeństwa, chociaż taki audyt może być narzędziem weryfikującym, ale nie gwarantującym kierownictwu organizacji i radzie nadzorczej, że poziom bezpieczeństwa w systemach informacyjnych jest odpowiedni, spełnia wymagania stawiane wobec tych systemów (Bojanowski 2001).

W polskich aktach prawnych znajdują się przede wszystkim odwołania do roli biegłego rewidenta (zewnętrznego audytora finansowego), a także do roli audytora wewnętrznego w jednostkach samorządowych i w bankach. Jak wynika z powyższych rozważań, o audycie systemów informacyjnych mówi się niewiele. Jest on zazwyczaj przeprowadzany w sytuacji nieprawidłowego funkcjonowania systemu lub w przypadku sporu z dostawcą rozwiązań informatycznych. Taka sytuacja oznacza jednak, że firma poniosła już niekontrolowane straty, czyli nie zabezpieczyła się właściwie przed ryzykiem informatycznym. Przedsiębiorstwa, w których od sprawności funkcjonowania informatyki zależy efektywne prowadzenie biznesu, powinny zlecać przeprowadzenie audytu jednostkom, które posiadają specjalne certyfikaty w tym zakresie. Jednym z takich jest Międzynarodowe Stowarzyszenie do spraw Audytu i Kontroli Systemów Informatycznych (ISACA).

Stowarzyszenie to opublikowało metodologię prowadzenia kontroli środowiska informatycznego, zgodnie z którą powinny być prowadzone prace audytorskie. Zlecając przeprowadzenie usługi takiemu audytorowi, firma ma pewność prawidłowości przeprowadzenia audytu.

W Polsce tego typu certyfikat posiada około 40 osób, w związku z tym z ich usług mogą korzystać jedynie zamożne firmy. Pozostałe zaś mogą zlecać wykonanie usługi innym specjalizowanym firmom doradczym lub wiarygodnym firmom informatycznym.

4. Procedura audytu systemu sieciowego

Istnieje kilka standardów audytu informatycznego. Jeden z takich standardów został opracowany przez COBIT (*Control Objectives for Information and Related Technology*) (Korytowski 2002). Według tego standardu procedura audytu systemu sieciowego składa się z pięciu etapów.

Etap I to analiza działania systemu. W etapie tym audytor uzyskuje wiedzę na temat audytowanego obiektu.

Etap II to ocena środowiska kontroli.

Etap III dotyczy analizy procedur kontrolnych.

Etap IV to testowanie systemu.

Etap V polega na ocenie działania systemu.

W czasie realizacji I etapu audytor posługuje się takimi technikami, jak (Piattini 2000):

- testy zgodności do weryfikacji poprawnego wykonania procedur przetwarzania danych, wielokrotne wykonanie procedur testowych na przygotowanych danych, przeglądy struktury logicznej systemu,
- testy uzasadniające, które obejmują analityczne przeglądy rzeczywistych danych, sprawdzają ich jakość przy użyciu oprogramowania audytorskiego CAATs.

Przeprowadzając testy zgodności, audytor może w swojej pracy posłużyć się następującymi metodami badawczymi: obserwacją, wywiadem, analizą i weryfikacją.

Metoda obserwacji jest szczególnie przydatna w wypadku nie udokumentowanej czynności audytowanej. Wynikiem obserwacji może być np. ustalenie, czy dostęp do serwerów lub zasobów sieciowych systemu (który zgodnie z procedurami ma być ograniczony i kontrolowany) jest możliwy dla osób nieupoważnionych.

Metoda wywiadu polega na tym, że audytor przeprowadza rozmowy z poszczególnymi grupami zawodowymi, począwszy od zarządu, poprzez użytkowników do operatorów końcowych systemu.

Metoda analizy może dotyczyć wytycznych wcześniejszego audytu. Wykorzystując tę metodę, audytor w szczególności koncentruje się na ocenie struktur

organizacyjnych, diagramów przepływu informacji, diagramów hierarchii organizacyjnej i ról pracowników. Analizie mogą podlegać np. podział obowiązków i obsada stanowisk w dziale informatyki, oddzielenie funkcji administratora baz danych od użytkownika końcowego czy konserwatora sieci.

Metoda weryfikacji polega na porównaniu faktów ze standardami, normami, procedurami, dokumentacją. Stosując tę metodę, audytor dowiaduje się o aktualności i potrzebie stosowanych procedur, o odbytych przez pracowników szkoleniach (czy są ważne i aktualne, czy pracownicy przeszli odpowiednie szkolenia), a także o ciągłym monitorowaniu i usprawnianiu pracy systemu.

W efekcie przeprowadzenia I etapu audytor powinien uzyskać odpowiedź na pytania:

- kto wykonuje zadania?
- gdzie i kiedy są wykonywane zadania?
- jakie są informacje wejściowe i wyjściowe?
- jakie są procedury przetwarzania?

Ten etap przygotowuje audytora do prowadzenia dalszych działań audytorskich, które realizowane są w ramach drugiego etapu.

Celem etapu II jest dokonanie oceny środowiska kontrolnego na podstawie informacji uzyskanych na I etapie, a następnie określenie jego skuteczności i sprawności.

Rezultatami tego etapu są:

- ustalanie praw, regulacji i kryteriów organizacyjnych,
- ocena procedur oraz mechanizmów kontrolnych.

Etap ten kończy gruntowna ocena środowiska kontroli.

Celem III etapu jest ocena działania systemu kontroli. Sprowadza się to do ustalenia, czy działania są zgodne z przyjętymi procedurami. Dotyczy to jednak tych mechanizmów kontrolnych, które są ustanowione wcześniej, a nie wszystkich, które powinny funkcjonować (ale nie są stosowane).

Etap IV. Testowanie systemu. Celem tego etapu jest przeprowadzenie testów, które dostarczą jednoznaczne dowody na to, że system funkcjonuje prawidłowo. Podczas testowania systemu wykorzystuje się dokumentację testową, która jest opracowana przez audytora na potrzeby przeprowadzenia czynności kontrolnych. Dokumentacja testowa może obejmować pytania dotyczące: struktury sieci, szybkości działania systemu sieciowego, wyposażenia technicznego, zakresu uprawnień użytkowników, bezpieczeństwa archiwizacji i dostępu do danych. Według COBIT na tym etapie audytor dodatkowo powinien zwrócić szczególną uwagę na funkcjonowanie systemu kontroli w systemie sieciowym. Nieprawidłowe funkcjonowanie kontroli może mieć decydujący wpływ na osiągnięcie celów biznesowych przez firmę.

Etap V dotyczy oceny działania systemu. Wykonanie czterech poprzednich etapów audytu daje możliwość przedstawienia wniosków na temat właściwego działania systemu kontroli. Audytor w formie pisemnej ocenia funkcjonowanie

systemu informatycznego. Według COBIT na tym etapie audytor dodatkowo powinien dokonać specyfikacji błędów występujących w zakresie struktury oraz realizacji systemu kontroli. Kolejnym krokiem w czynnościach audytora jest przygotowanie dokumentacji, w której będą zawarte dowody zawierające wykryte błędy oraz ich wpływ na osiąganie celów systemu.

Zaprezentowany standard jest dokumentem ogólnym, nie zawierającym szczegółowych opisów postępowania audytora w konkretnych sytuacjach. Pomaga w ustaleniu właściwej metodyki, zakresu i obiektów audytu, a także służy do oceny jakości audytu.

W przygotowaniu i przeprowadzaniu audytu powinny być uwzględniane następujące normy i metodyki:

- PN-ISO 10011-1 Wytyczne do audytowania systemów jakości. Audytowanie;
- ISO/IEC 17799 Technologie informacyjne. Zasady postępowania w zarządzaniu bezpieczeństwem informacji;
- PN-1-13335-1 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Pojęcia i modele bezpieczeństwa systemów informatycznych;
- PrPN-1-13335-2 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Aspekty zarządzania i planowania.
- PrPN-1-1335-3 Technika informatyczna. Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. Techniki bezpieczeństwa.
- ISO/IEC 15408-1 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wprowadzenie i generalny model (ang.);
- ISO/IEC 15408-2 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wymagania bezpieczeństwa funkcjonalnego (ang.);
- ISO/IEC 15408-3 Technologie informacyjne. Techniki bezpieczeństwa – kryteria oceny bezpieczeństwa informacji. Wymagania zapewnienia bezpieczeństwa (ang.);
- PN-I-02000 Technika informatyczna. Zabezpieczenia w systemach informatycznych. Terminologia.
- *IT Baseline Protection Manual* – poradnik wydany przez Bundesamt für Sicherheit in der Informationstechnik.

W Polsce pojawiło się już wiele firm mających w swojej ofercie usługę audytu systemów sieciowych. Są wśród nich duże firmy konsultingowe, takie jak np. Andersen Business Consulting oraz nowe firmy specjalizujące się w usługach audytu bezpieczeństwa.

5. Udokumentowanie audytu

Audytor w czasie prowadzenia audytu gromadzi informacje, które pozwalają mu uzyskać wiarygodne (oparte na faktach, obiektywne i możliwe do zaakcepto-

wania), relewantne (odnoszące się do celów audytu i logicznie powiązane ze stwierdzeniami oraz wnioskami) i użyteczne dowody umożliwiające osiągnięcie celów audytu (*Wskazówki*... 2002). Dowody te mogą obejmować:
- zaobserwowane procesy,
- dokumentację związaną z realizacją systemu informacyjnego,
- dokumenty prezentujące zasady funkcjonowania obszaru audytowanego,
- analizy porównawcze.

W zakresie zaobserwowanych procesów dokumentacja ta może przykładowo obejmować:
- spis nośników i miejsce ich przechowywania,
- opis zabezpieczeń pomieszczeń, dostępu do zasobów i procesów przetwarzania danych,
- opis działania systemu w warunkach awarii i możliwości jego odtworzenia.

Dokumentacja związana z realizacją audytu systemu informacyjnego dotyczy:
- wyników ekstrakcji danych,
- zapisów transakcji,
- listingów programów,
- dokumentacji określającej tryb pracy systemu i aplikacji,
- dokumentacji stosowanych programów wspomagających, języków programowania,
- dokumentacji przepływu danych aplikacji w ramach sieci (ze szczególnym uwzględnieniem metod ochrony tych danych oraz miejsc styku z siecią zewnętrzną),
- dokumentacji rozwoju systemu.

Kolejna grupa dowodów to dokumenty prezentujące zasady funkcjonowania jednostek audytowanych. Podstawowym dokumentem, który powinna mieć każda jednostka eksploatująca system informatyczny, jest „Polityka systemu informatycznego”[4]. Polityka ta powinna zawierać:
- procedury oraz wymagania prawne w zakresie systemu informatycznego,
- wymagania wobec osób odpowiedzialnych za bezpieczeństwo systemu,
- schematy fizyczne i logiczne aplikacji oraz przyłączonych sieci,
- schematy organizacyjne służb informatycznych wraz z dokumentacją określającą odpowiedzialność,
- listę dostawców usług transmisji danych,
- oświadczenia dotyczące funkcjonowania systemu informacyjnego,
- raporty audytorów zewnętrznych,
- raporty osób trzecich będących dostawcami usług,
- procedury dotyczące ochrony danych oraz uprawnień nowo przyjętych pracowników.

[4] Według autorki jest to dokument, który powinien być opracowany przez jednostkę i stanowić swego rodzaju opis funkcjonowania systemu informatycznego w firmie.

Analizy porównawcze mogą również stanowić dowody audytu. Przykładowo mogą one obejmować:
- badania porównawcze wydajności aplikacji w stosunku do innych organizacji lub okresów,
- porównanie wskaźników błędów między aplikacjami, transakcjami i użytkownikami.

Audytor powinien posługiwać się najnowszymi technikami badania, zebrać wiarygodne dowody i wychwycić wszystkie nieprawidłowości w funkcjonowaniu systemu informacyjnego.

Dowody audytu zebrane przez audytora powinny być odpowiednio udokumentowane i zorganizowane, tak by poprzeć jego stwierdzenia i wnioski. Dowody te audytor gromadzi w dokumentacji rewizyjnej. Dokumentacja ta jest odpowiednio opisywana przez audytora i przechowywana przez niego lub w firmie, na której zlecenie był prowadzony audyt systemu informatycznego. Okres przechowywania dokumentacji rewizyjnej wynosi 5 lat, tak jak pozostałych dokumentów. Przykładowo, dokumentacja ta może zawierać:
- opis przez audytora systemu informacyjnego obszaru i środowiska poddanego kontroli,
- dowody modyfikacji systemu,
- opis algorytmów przetwarzania informacji,
- opis procedur zarządzania siecią i jej zasobami zasad zarządzania,
- odpowiedzi i wyjaśnienia osób kontrolowanych na rekomendacje audytorskie.

Po zebraniu dokumentacji rewizyjnej i ukończeniu audytu, audytor powinien opracować w formie pisemnej odpowiednią dokumentację zwaną raportem z przeprowadzonego badania. Dokumentacja ta stanowi zapis przeprowadzonej przez audytora pracy oraz jego wnioski. Dotychczas nie ma jednoznacznego standardu, który by określał zawartość raportu systemu informatycznego funkcjonującego w przedsiębiorstwie. Niektóre wytyczne co do treści raportu zawarte są w normach wykonywania zawodu biegłego rewidenta oraz we wskazówkach zawartych w sprawie sporządzania raportu (*Normy*... 2002; *Wskazówki*... 2002).

W raporcie sporządzonym przez audytora z przeprowadzonego audytu informatycznego systemu sieciowego, powinny się znaleźć m.in. takie informacje, jak:
- charakterystyka systemu informatycznego,
- przedstawienie zakresu systemu, do którego audytor zastosował standardy audytu,
- ocena przez audytora programu zabezpieczenia jakości dotycząca funkcjonowania systemu informacyjnego,
- ocena zbiorów danych, prawidłowości ich zabezpieczania oraz archiwizowania,
- ocena wyposażenia informatycznego systemu sieciowego.

Warto zaznaczyć, że zakres dokumentacji zgromadzonej przez audytora, a następnie opracowanie raportu zależą od potrzeb określonego audytu, czyli od zleceniodawcy, na rzecz którego przeprowadzany jest audyt.

Dokumentacja powinna zawierać informacje kontrolne wymagane przez prawo, regulacje rządowe lub stosowane standardy jakości. Powinna być czytelna, kompletna i zrozumiała dla korzystających z niej. Należy ją przechowywać zgodnie z przepisami prawa i przez obowiązujący czas.

6. Podsumowanie

Głównym celem opracowania było przedstawienie realizacji procesu audytu systemu informacyjnego w firmie. Audyt jest jednym z elementów zarządzania ryzykiem gospodarczym. Może być realizowany jako odrębne przedsięwzięcie lub zostać wykonany w ramach audytu sprawozdań finansowych. W przypadku realizacji w ramach audytu sprawozdań finansowych przez biegłych rewidentów należałoby dodatkowo w tej dziedzinie przeszkolić biegłych. Powinien dać odpowiedzi na pytania dotyczące zagrożeń, powodów ich występowania, wpływu tych zagrożeń na funkcjonowanie systemu informacyjnego oraz systemu zarządzania. W czasie audytu systemu sieciowego audytor powinien stwierdzić, czy wykorzystywane w firmie systemy są wiarygodne, rzetelne i bezpieczne. Usługa audytu systemu informacyjnego, w tym także sieciowego, nie jest jeszcze zbyt popularna w Polsce i na ogół stosowana wówczas, gdy użytkownik stwierdzi zakłócenia w zainstalowanym systemie i chce uzyskać opinię eksperta w sporze z dostawcą systemu. Wiele firm (głównie spółek publicznych lub przedsiębiorstw z kapitałem zagranicznym) nawiązuje także długofalową współpracę z firmami audytorskimi, które badając ich sprawozdania finansowe, oceniają również stan infrastruktury IT. Ze względu na to, że infrastruktura komputerowa jest jedną z podstaw funkcjonowania współczesnej firmy, audyt systemu informacyjnego jest istotną częścią badania jej sprawności. Natura systemu informacyjnego powoduje, że audyt i umiejętności jego prowadzenia wymagają istnienia jasno określonych standardów. Międzynarodowe Stowarzyszenie ds. Audytu i Kontroli Systemów Informatycznych (ISACA) szczegółowo reguluje kwestie organizacji i przebiegu badań dotyczących systemów IT. Podstawowym zbiorem standardów i wytycznych dla audytorów jest metodologia COBIT, która konsoliduje i harmonizuje ogólne wytyczne w jedno opracowanie o zasadniczym znaczeniu dla kierownictwa, użytkowników i audytorów. Coraz większego znaczenia nabiera też certyfikat *Certified Information Systems Auditor* (CISA), który jest jedynym, globalnym i powszechnie uznawanym programem certyfikacji audytorów systemów informacyjnych. Uzyskanie CISA nie jest warunkiem koniecznym do prowadzenia audytu, tylko wiarygodnym potwierdzeniem posiadanej wiedzy. W międzynarodowych wytycznych sporo uwagi poświęcono niezależności audytorów, którzy powinni być trzecią stroną w przypadku sporu klienta z dostawcą systemu.

Literatura

Bojanowski J., *Systemy informatyczne z perspektywy audytora – bariera czy wezwanie*, „Monitor" 2001 nr 3.

Bojanowski J., *Wykorzystanie standardów audytu informatycznego ISACA na przykładzie audytu sieci*, Warszawa 2003.

Korytowski J., *Podstawy audytu aplikacji*, www.isaca.org.pl, 2002.

Kurzawski R., Mierzejewski S., *Dokumentacja rewizyjna badania sprawozdania finansowego*, SKwP, Warszawa 2004.

Normy wykonywania zawodu biegłego rewidenta, Biuletyn KIBR nr 53, Warszawa 2002.

Piattini M., *Auditing Information Systems*, Idea Group Publishing, Herschey 2000.

Wskazówki w sprawie sporządzania opinii, raportu i udziału biegłego rewidenta w inwentaryzacji, Biuletyn KIBR nr 57, Warszawa 2002.

AUDIT OF THE NETWORK INFORMATION SYSTEM

Summary

The article is focused on audit of network information system. The main attention is concentrated on the audit issue as well as legal matters of its functionality. Additionaly, the paper contains also the audit procedure with all its important phases. The last part of the article presents standard audit documentation.