Modele i praktyka audytu informatycznego

Andrzej Zalewski, Rafał Cegieła, Krzysztof Sacha

Instytut Automatyki i Informatyki Stosowanej, Wydział Elektroniki i Technik Informacyjnych, Politechnika Warszawska

{a.zalewski, r.cegiela, k.sacha}@ia.pw.edu.pl

Streszczenie

W rozdziale wyróżniono i scharakteryzowano trzy modele audytu informatycznego: klasyczny (przez analogię do roli audytu ksiąg rachunkowych), formalny i merytoryczny. W odniesieniu do każdego z nich przedstawiono czynniki warunkujące działania podejmowane przez audytora: źródła i sposób pozyskania informacji o przedmiocie audytu, kryteria oceny, zakresy wiedzy niezbędnej do przeprowadzenia oceny. Szczególnie dużo miejsca poświęcono tzw. audytowi merytorycznemu, którego istotą jest ocena rozwiązań informatycznych na różnych etapach ich cyklu życia.

1. Wstęp

Rosnące uzależnienie współczesnych przedsiębiorstw i innych organizacji od sprawnego funkcjonowania systemów informacyjnych, przy coraz większej złożoności rozwiązań informatycznych wchodzących w skład tych systemów, dało impuls do rozwoju tzw. *audytu informatycznego* – usług polegających na niezależnej ocenie rozwiązań informatycznych i organizacyjnych składających się na systemy informacyjne działające w organizacjach.

Celem niniejszego rozdziału jest przedstawienie podstawowych modeli, w jakich audyt informatyczny jest wykorzystywany w zarządzaniu przedsięwzięciami i systemami informatycznymi. Artykuł ten stanowi wynik doświadczeń w zakresie audytu informatycznego w projektach realizowanych przez Zespół Inżynierii Oprogramowania Instytutu Automatyki i Informatyki Stosowanej Politechniki Warszawskiej.

2. Modele audytu informatycznego

Przedmiotem oceny w audycie informatycznym są:

- kontrola/nadzór nad systemami informacyjnymi w organizacji;
- sposób zarządzania przedsięwzięciami informatycznymi;
- konkretne rozwiązania informatyczne (działające lub projektowane).

Wymienionym wyżej przedmiotom odpowiadają poszczególne, rozważane w niniejszej pracy modele audytu:

- model klasyczny – ocena kontroli i nadzoru nad systemami informacyjnymi w organizacji;
- audyt formalny – ocena organizacji przedsięwzięć;
- audyt merytoryczny – ocena rozwiązań informatycznych.

Przyjęta klasyfikacja ma przede wszystkim walor poznawczy. W ramach jednego przedsięwzięcia audyt jest bardzo często realizowany wg kilku wymienionych wyżej modeli jednocześnie.

Główne zadania i problemy, jakie stają przed audytorem, to:

- określenie kryteriów oceny;
- pozyskanie informacji o przedmiocie audytu;
- posiadanie lub uzyskanie wiedzy niebędnej dla przeprowadzenia oceny.

Powyższe kwestie wyznaczają sytuację audytora w omówionych poniżej modelach audytu informatycznego.

2.1. Model klasyczny

W modelu klasycznym (nazwanym w nawiązaniu do funkcji pełnionej przez audyt finansowy) audyt informatyczny stanowi jeden z mechanizmów nadzoru nad organizacją. Jego celem jest odpowiedź na pytanie: czy dana organizacja posiada wystarczający nadzór nad wykorzystywanymi w niej systemami informacyjnymi (w szczególności nad systemami informatycznymi) oraz ich rozwojem. Ocena ta stanowi, obok oceny sprawozdań i ksiąg finansowych, składnik oceny wiarygodności przedsiębiorstwa i, w założeniu, element tzw. „ładu korporacyjnego" (ang. *corporate goveranance*).

W modelu tym ocenia się rozwiązania techniczne i organizacyjne składające się na funkcjonowanie systemów informacyjnych w danej organizacji względem modelu referencyjnego. Najpowszechniej stosowany jest model opisany w standardzie COBIT (ang. *Control Objectives for Information and Related Technology*) [COBIT].

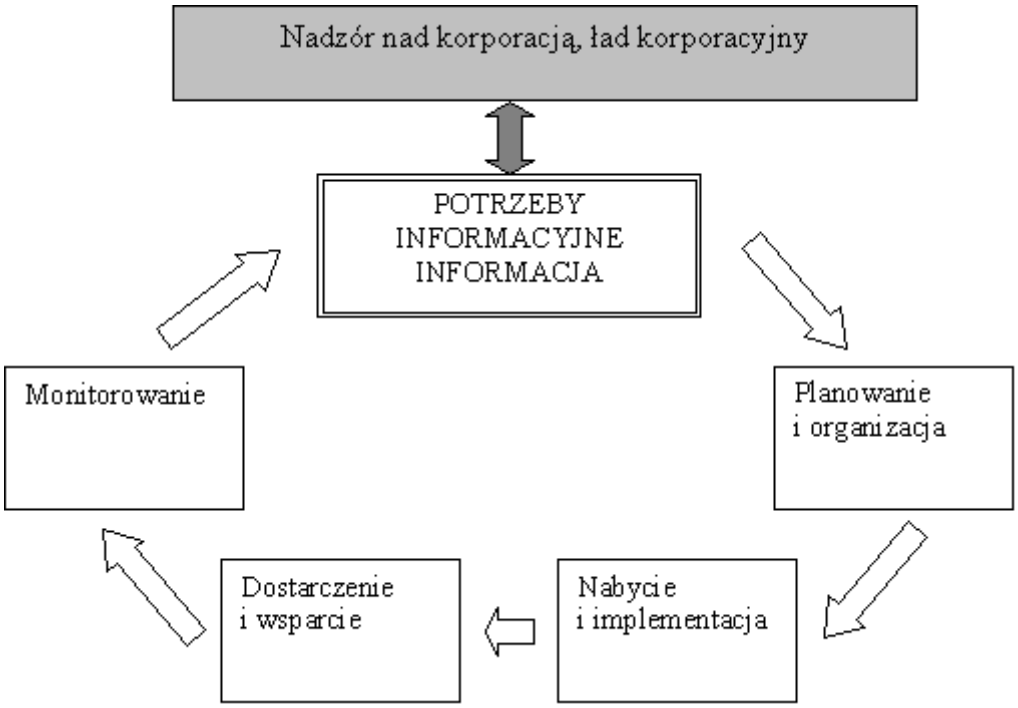
Źródła i sposób pozyskania informacji zależą od dojrzałości danej organizacji. Informację o przedmiocie audytu pozyskuje się więc przede wszystkim na podstawie:

- dokumentacji procesów biznesowych;
- wywiadów z pracownikami;
- bezpośrednich czynności na systemie informatycznym (np. badanie konfiguracji).

Do przeprowadzenia tak rozumianego audytu niezbędna jest wiedza na temat modelu referencyjnego opisanego w standardzie COBIT. Standard ten określa wzorcowy model procesów organizacyjnych zapewniających prawidłowy nadzór nad funkcjonowaniem i rozwojem infrastruktury teleinformatycznej przedsiębiorstwa. W modelu tym wyróżniono 4. dziedziny (ang. *domains*) odpowiadające cyklowi życia rozwiązań informatycznych w organizacji (por. rysunek 1). Obejmują więc one: planowanie i organizację, nabycie i implementację, dostarczenie i wsparcie, monitorowanie. W każdej z dziedzin wyróżniono procesy niezbędne dla prawidłowego nadzoru nad systemami informatycznymi w organizacji. Dla każdego procesu zdefiniowane zostały:

- cel biznesowy,
- kryteria oceny systemu zależne od realizacji procesu,
- kluczowe wskaźniki celu i wydajności,
- krytyczne czynniki sukcesu,
- zasoby konieczne do realizacji procesu,
- 6-stopniowy model dojrzałości,
- kluczowe i szczegółowe mechanizmy kontrolne.

Standard obejmuje także wytyczne dotyczące procesu prowadzenia audytu poszczególnych procesów.



Rysunek 1. Dziedziny modelu COBIT.

2.2. Model audytu formalnego

Istotą audytu formalnego jest ocena procesu wytwarzania (budowy) systemu informatycznego. Organizację przedsięwzięcia informatycznego można zobrazować jako strukturę dwuwarstwową, na którą składa się:

- Przyjęta metodyka zarządzania projektem;
- Stosowane w ramach tej metodyki metody projektowania.

W audycie formalnym podstawą oceny są metodyki zarządzania i projektowania.

Metodyka zarządzania określa zwykle: procesy związane z zarządzaniem przedsięwzięciem i ich wzajemne powiązania, strukturę zespołu projektowego oraz sposób dokumentowania jego przebiegu. Przykładem metodyki zarządzania jest popularna na świecie metodyka PRINCE2 (ang. PRojects IN Controlled Environments). Metodyki zarządzania projektem nie są zwykle związane z żadną konkretną dziedziną zastosowań.

W ramach metodyki zarządzania projektem wykorzystywane są z kolei metodyki projektowania.

Definiują one sam proces projektowania konkretnych rozwiązań informatycznych, sposób dokumentowania rozwiązań konstrukcyjnych (notacje i modele) oraz artefakty będące rezultatem poszczególnych faz projektowania.

W audycie formalnym bada się:

- Czy i jak w zarządzaniu przedsięwzięciem realizowane są procesy określone w metodyce?
- Czy przedsięwzięcie jest dokumentowane zgodnie z przyjętą metodyką?
- Czy zgodne z dokumentacja procesu wytwarzania systemu informatycznego, organizacyjna zespołu projektowego?
- Czy wszystkie artefakty procesu projektowego zostały wytworzone?

Źródłem informacji o przedmiocie audytu jest przede wszystkim dokumentacja związana z procesem projektowym oraz dokumentacja projektowa. Brak wymienionej wyżej dokumentacji lub nie stosowanie się do jakiejkolwiek metodyki zarządzania, czy projektowania sprowadza audyt formalny do stwierdzenia braku wyżej wymienionych. Praktyka dowodzi, że nie jest to przypadek odosobniony nawet w dużych przedsięwzięciach.

2.3. Model audytu merytorycznego

Audyt merytoryczny ma na celu ocenę konkretnych rozwiązań informatycznych, a także całych systemów informatycznych na różnych etapach ich cyklu życia. Typowe sytuacje, w których przeprowadzany jest tak rozumiany audyt, to:

- Trwająca realizacja projektu – audyt stanowi wówczas jeden z mechanizmów nadzoru organizacji nad przedsięwzięciem – zwykle dotyczy on wielkich przedsięwzięć informatycznych, gdy zlecająca ich realizację organizacja nie posiada wystarczającej wiedzy merytorycznej by „zapanować" nad realizowanymi rozwiązaniami;
- Związany jest z procesem odbioru zamówionego rozwiązania informatycznego;
- Po klęsce przedsięwzięcia – w poszukiwaniu przyczyn klęski.

2.3.1. Kryteria oceny

Celem audytu merytorycznego jest najogólniej: ocena *sprawności* rozwiązań informatycznych, przy czym przez sprawność rozumie się możliwość realizacji przez dane rozwiązanie powierzanych mu funkcji, w wymagany sposób. Jednakże przełożenie pojęcia *„sprawność"* na zestaw uniwersalnych kryteriów oceny nie wydaje się w ogólnym przypadku możliwe. W praktyce rozwiązania informatyczne oceniane są pod kątem właściwości takich, jak:

- użyteczność,
- jakość,
- wydajność,
- niezawodność,

- bezpieczeństwo,
- wiarygodność,
- zgodność z odpowiednimi normami technicznymi (np. kategorie okablowania).

Z kolei wymienione powyżej właściwości rozwiązań informatycznych przekładają się na szereg kryteriów szczegółowych. Poniżej przedstawiono sytuację audytora przystępującego do oceny rozwiązań informatycznych pod kątem ww. właściwości.

2.3.1.1. Użyteczność

Przez użyteczność rozumiemy spełnienie przez system wymagań funkcjonalnych, przy założeniu, że osiągnięte parametry wydajności i niezawodności systemu umożliwiają badanie funkcjonalności.

Przedmiotem oceny może być rozwiązanie informatyczne na dowolnym etapie jego cyklu życia, w skrajnym przypadku ocenie podlegać może specyfikacja wymagań względem dokumentów źródłowych.

2.3.1.2. Jakość

Jakość nie jest pojęciem samoistnym lecz agregatem pojęciowym łączącym w sobie inne cechy składające się na to pojęcie (np. niezawodność, staranność wykonania, przydatność, ergonomia). W ocenie jakości oprogramowania wykorzystuje się m.in. powszechnie znany standard ISO 9126. Kryteria oceny jakości oprogramowania wg tego standardu zestawiono w tabeli 1. Ponadto standard definiuje:

- Metryki zewnętrzne (ang. External metrics) – miary związane z poszczególnymi kryteriami umożliwiające ocenę oprogramowania na podstawie funkcjonowania systemu, w skład którego oprogramowanie to wchodzi; znajdują one zastosowanie w trakcie testów i eksploatacji,
- Metryki wewnętrzne (ang. Internal metrics) – związane z poszczególnymi kryteriami miary umożliwiające bezpośrednią ocenę oprogramowania, znajdujące zastosowanie w trakcie projektowania i kodowania.

Tabela 1. Kryteria oceny jakości oprogramowania

Grupa kryteriów	**Kryterium**
Funkcjonalność	Adekwatność Dokładność Współdziałanie Zgodność Bezpieczeństwo
Niezawodność	Dojrzałość Tolerancja błędów

Grupa kryteriów	Kryterium
	Odtwarzalność
Użyteczność	Zrozumiałość Łatwość nauki Łatwość użytkowania
Wydajność	Charakterystyki czasowe Gospodarka zasobami
Pielęgnowalność	Podatność na analizę Podatność na zmiany Stabilność Testowalność
Przenośność	Łatwość adaptacji Łatwość instalacji Zgodność Zastępowalność

W odniesieniu do innych składników systemów informatycznych trudno jest przywołać właściwe normy jakościowe. W tym przypadku kryteriami oceny stają się:

- Istnienie udokumentowanych przypadków zastosowań danej technologii w zbliżonych zastosowaniach;
- Deklarowana przez producenta niezawodność urządzeń, mierzona np. długością udzielanej na nie gwarancji;
- Normy i systemy zarządzania jakością stosowane przez wytwórcę danych rozwiązań.

2.3.1.3. Wydajność

Ocena wydajności, w teorii, winna polegać na porównaniu wymaganych parametrów wydajnościowych rozwiązania z ich wartościami osiągniętymi przez zrealizowane rozwiązanie. Przeszkodą w zastosowaniu tego podejścia jest:

- Brak standardów regulujących sposób definiowania parametrów wydajnościowych;
- Niepełna adekwatność stosowanych miar wydajności – np. miara liczby transakcji przetwarzanych w ciągu sekundy nie jest adekwatna we wszystkich sytuacjach;
- Brak możliwości użycia istniejących modeli analitycznych do oceny rzeczywistych rozwiązań komercyjnych;
- Niestacjonarność właściwości wydajnościowych – wydajność zwykle spada na przestrzeni eksploatacji systemu informatycznego, co wiąże się np. z zapełnianiem baz danych, ocena wydajności rozwiązania musi więc zakładać pewien dłuższy horyzont

czasowy.

Typowo wymagania wydajnościowe formułowane są w kategoriach czasu reakcji na działania użytkownika oraz liczby przetwarzanych przez system danych, dokumentów itp. Oszacowanie tych wielkości na podstawie informacji projektowych jest zwykle nie możliwe. W efekcie ocena wydajności może być w sposób adekwatny prowadzona dopiero przez badanie już zrealizowanego rozwiązania.

Zagadnienie oceny wydajności rozwiązania informatycznego w wielu sytuacjach może zostać zdekomponowane na:

- Ocenę wydajności systemu wprowadzania danych do systemu z wykorzystaniem np. tradycyjnych modeli systemów masowej obsługi;
- Ocenę wydajności przetwarzania danych realizowanego przez system informatyczny.

Pierwsze z ww. aspektów zmierza do oceny wiarygodności przyjętych założeń odnośnie ilości danych napływających lub przechowywanych w systemie oraz zastosowanych urządzeń wejściowych lub wyjściowych.

Ocena wydajności przetwarzania danych obok badań empirycznych może być poparta weryfikacją pod kątem stosowania tzw. dobrych praktyk, np. w konfiguracji bazy danych. Źródłem informacji o tych praktykach jest zwykle dokumentacja stosowanego komponentu (np. systemu zarządzania bazą danych).

2.3.1.4. Niezawodność

Niezawodność jest miarą odporności rozwiązań na awarie. Wymagania niezawodnościowe winny być formułowane w sposób ilościowy. W odniesieniu do rozwiązań sprzętowych korzysta się zwykle z modelu średniego czasu między awariami (MTBF – ang. *Mean Time Between Failure*) – producenci poszczególnych komponentów systemu, zwłaszcza tych mechanicznych podają parametry tego typu dla wytwarzanych przez nich urządzeń.

W odniesieniu do wyższych warstw systemu obejmujących oprogramowanie aplikacyjne wymagania niezawodnościowe formułuje się w kategoriach maksymalnego akceptowalnego czasu awarii. Określenie wymagań w kategoriach MTBF jest wprawdzie możliwe, jednakże model ten nie obejmuje sytuacji niesprawności oprogramowania aplikacyjnego będącej rezultatem istniejącej usterki w oprogramowaniu, jak również na obecnym etapie brak jest możliwości oszacowania rzeczywistej wartości tego parametru dla złożonych rozwiązań.

Ocena niezawodności złożonych rozwiązań informatycznych ma więc przede wszystkim charakter jakościowy i obejmuje:

- Ocenę adekwatności, dostateczności i poprawności zastosowanych rozwiązań redundancyjnych;
- Ocenę parametrów niezawodnościowych stosowanego sprzętu;
- Ocenę realności i adekwatność wymagań na maksymalny czas trwania awarii;
- Ocenę skuteczności mechanizmów ograniczających skutki awarii i czas ich trwania.

2.3.1.5. Bezpieczeństwo

Bezpieczeństwo systemu jest miarą jego podatności na niepożądane zmiany i ingerencje. Właściwym punktem odniesienia dla oceny bezpieczeństwa są istniejące i uznawane standardy bezpieczeństwa TCSEC i ITSEC scharakteryzowane krótko poniżej.

Standard TCSEC

Standard TCSEC (ang. *Trusted Computer Security Evaluation Criteria*) [TCSEC] został opublikowany przez Departament Obrony USA. Standard definiuje klasy bezpieczeństwa systemów komputerowych. Zostało zdefiniowanych 7 klas systemów (A1, B1, B2, B3, C1, C2, C3, D), przy czym systemy klasy A są najbezpieczniejsze a klasa D zawiera systemy nie spełniające norm właściwych dla pozostałych klas. Wymagania związane z każdą klasą bezpieczeństwa zostały podzielone na następujące kategorie:

- polityka bezpieczeństwa (ang. *security policy*) – zasady przydziału uprawnień do zasobów systemu,
- identyfikatory (ang. *marking*) – zasady przydziału identyfikatorów do poszczególnych obiektów/zasobów systemu,
- identyfikacja (ang. *identification*) – zasady identyfikacji użytkowników systemu,
- rozliczenia (ang. *accountability*) – zasady identyfikacji użytkowników, śledzenia i monitorowania ich aktywności.
- pewność (ang. *assurance*) – rozwiązania i techniki projektowe zmierzające do wiarygodnej i skutecznej realizacji deklarowanych rozwiązań.
- ciągła ochrona (ang. *continuous protection*) – rozwiązania zapewniające trwałość zaimplementowanych mechanizmów bezpieczeństwa.

Standard ITSEC

Standard ITSEC (ang. *information technology security criteria*) [ITSEC] został sporządzony i przyjęty przez Unię Europejską w wyniku harmonizacji kryteriów wykorzystywanych w poszczególnych państwach Unii.

Standard definiuje dwie klasyfikacje systemów: związaną z deklarowanymi właściwościami systemu, określającymi jego bezpieczeństwo (ang. *functionality class*) oraz związaną z zapewnianiem, że zadeklarowany poziom bezpieczeństwa zostanie osiągnięty (ang. *assurance class*).

Deklarowane właściwości systemu mogą zostać skonfrontowane z właściwościami zdefiniowanymi przez tzw. sponsora systemu lub z właściwościami jednej z 10 przykładowych klas: F-C1, F-C2, F-B1, F-B2, F-B3, IN, AV, DI, DC, DX. Pierwsze 5 z przykładowych klas, to klasy mające odpowiedniki w standardzie TCSEC. Pozostałe, to klasy uwzględniające aspekty bezpieczeństwa związane z przyłączeniem do sieci komputerowej.

Standard sugeruje aby definicja klasy bezpieczeństwa składała się z następujących sekcji:

- identyfikacja i uwierzytelnianie (ang. *Identification and Authentication*) – wymagania dotyczące zasad identyfikacji i metod uwierzytelniania użytkowników,
- kontrola dostępu (ang. *Access Control*) – wymagania dotyczące mechanizmów zapewniających selektywne udostępnianie informacji i zasobów użytkownikom,
- rozliczenia (ang. *Accountability*) – wymagania dotyczące mechanizmów rejestracji informacji umożliwiającej powiązanie użytkowników z wykonywanymi przez nich operacjami,
- audyt (ang. *Audit*) – wymagania dotyczące mechanizmów rejestracji informacji na potrzeby audytu,
- ponowne użycie (ang. *Object Reuse*) – wymagania dotyczące zapewniania bezpieczeństwa w kontekście współdzielenia zasobów,
- dokładność (ang. *Accuracy*) – wymagania dotyczące mechanizmów zapewniających spójność i integralność danych,
- wiarygodność usług (ang. *Reliability of Service*) – wymagania dotyczące dostępności i niezawodności usług,
- wymiana danych (ang. *Data Exchange*) – wymagania dotyczące mechanizmów transmisji danych, sklasyfikowane w kategoriach: uwierzytelnianie (ang. *Authentication*), kontrola dostępu (ang. *Access Control*), poufność danych (ang. *Data Confidentiality*), integralność danych (ang. *Data Integrity*) oraz niezaprzeczalność (ang. *Non-Repudiation*).

Ocena stopnia pewności, że system posiada zadeklarowane właściwości odbywa się na podstawie dwóch kryteriów:

- efektywności – czy system jest odporny na ataki lub awarie i czy jest prawdopodobne, że zostanie skonfigurowany w sposób naruszający zasady bezpieczeństwa?
- poprawności – czy zostały zaimplementowane rozwiązania techniczne zapewniające bezpieczeństwo?

Na podstawie tych kryteriów system jest przypisywany do jednej z klas noszących oznaczenia od E1 do E6. Zależność pomiędzy wynikami klasyfikacji zgodnej z ITSEC a klasami zdefiniowanym przez standard TCSEC przedstawia tabela 2.

Standardowi ITSEC towarzyszy dokument ITSEM (ang. *IT Security Evaluation Manual*) [ITSEM] określający szczegółowo zasady korzystania z tego pierwszego.

Tabela 2. Metody zapewnienia i oceny jakości. Źródło: [ITSEC]

Klasyfikacja ITSEC	Klasa TCSEC
E1, F-C1	C1
E2, F-C2	C2
E3, F-B1	B1
E4, F-B2	B2

E5, F-B3	B3
E6, F-B3	A1

2.3.1.6. Wiarygodność

Pod pojęciem *wiarygodności rozwiązania informatycznego* rozumiemy stopień racjonalnego umotywowania poszczególnych decyzji konstrukcyjnych. W prawidłowo prowadzonych projekcie informatycznym każda istotna decyzja projektowa powinna zmierzać do osiągnięcia założonego celu, jakim jest realizacja zidentyfikowanych wymagań obejmujących zarówno funkcjonalność, jak i inne pożądane właściwości w tym właściwości niefunkcjonalne.

Cele te powinny więc być znane, udokumentowane i czytelnie powiązane z realizującymi je rozwiązaniami. Przedmiotem oceny staje się więc istnienie i poprawność ww. elementów.

Źródłami informacji są tutaj: w idealnym przypadku dokumentacja projektowa, a w praktyce także wywiady z autorami poszczególnych rozwiązań i innymi osobami zaangażowanymi w projekt.

2.3.1.7. Zgodność z odpowiednimi normami technicznymi

Ocena względem tego kryterium dotyczy wyłącznie rozwiązań sprzętowych i polega na zbadaniu czy dane rozwiązanie posiada właściwości określone w odpowiednich normach technicznych. Ocena ta jest przeprowadzana w drodze badania deklaracji zgodności z odpowiednimi normami dawanymi przez wytwórców sprzętu lub bezpośrednich pomiarów ocenianej instalacji (np. sieci LAN, sieci zasilającej) lub urządzeń.

2.3.2. Źródła informacji

Sposób pozyskania i źródła informacji w audycie merytorycznym są silnie uzależnione od konkretnej sytuacji projektowej: w idealnym przypadku informacje o przedmiocie audytu uzyskuje się na podstawie dokumentacji projektowej, powykonawczej, projektu i raportów testów oraz dokumentacji technicznej zastosowanych narzędzi komercyjnych, w nieco gorszym przypadku badając istniejący system i/lub dokumentację, w skrajnym zaś na podstawie informacji wydobytych w drodze wywiadu z osobami zaangażowanymi w realizację projektu oraz przez analizę dokumentacji technicznej produktów komercyjnych wykorzystanych przy budowie systemu.

Audyt merytoryczny wymaga posiadania obszernej i różnorodnej wiedzy na temat ocenianych rozwiązań informatycznych lub możliwości jej szybkiego pozyskania. W praktyce audytu często zachodzi konieczność konsultacji z ekspertami dziedzinowymi.

4. Uwarunkowania audytu według poszczególnych jego

modeli

	Audyt klasyczny	**Audyt formalny**	**Audyt merytoryczny**
Źródła informacji o przedmiocie oceny	Dokumentacja procesów biznesowych. Pracownicy. Bezpośrednie czynności na systemie wykonywane przez audytora.	Dokumentacja procesu zarządzania projektem. Dokumentacja projektowa.	Trudne do kompletnego określenia *a priori*, przede wszystkim: dokumentacja projektowa, badanie instalacji, makiet programów, wytworzonego oprogramowania, projekty i raporty z testów, dokumentacja użytkownika, dokumentacja powykonawcza, itd.
Kryteria oceny	Model wzorcowy np. COBIT.	Zgodność z metodyką zarządzania. Zgodność z metodyką projektowania.	Wymagają indywidualnego zdefiniowania w zależności od analizowanych rozwiązań informatycznych. Niekiedy wynikają ze standardów i norm.
Zakres niezbędnej wiedzy	Zrozumienie procesów związanych z nadzorem nad SI.	Znajomość metodyk zarządzania i projektowania.	Wiedza merytoryczna na temat konkretnych rozwiązań informatycznych. Konieczność konsultacji specjalistycznych.
Właściwe normy	COBIT	Standardy dokumentowania, UML, RUP, Metodyki i notacje strukturalne. Metodyki zarządzania projektami (np. PRINCE2, FOCUS PM)	Normy dziedzinowe, ISO 9126 (jakość oprogramowania), normy bezpieczeństwa (ITSEC, TCSEC)

5. Podsumowanie

W rozdziale zaproponowano klasyfikację podstawowych modeli, w ramach których

audyt informatyczny jest wykorzystywany w zarządzaniu przedsięwzięciami i systemami informatycznymi. Scharakteryzowano ponadto: dostępność i źródła informacji o przedmiocie audytu, kryteria oceny, zakres niezbędnej wiedzy oraz wskazano najistotniejsze normy wykorzystywane w audycie. Czynniki te określają sytuację audytora przy przeprowadzaniu audytu wg opisanych tutaj modeli.

Audyt klasyczny, dzięki istnieniu dobrze zdefiniowanych standardów systemu nadzoru nad systemami informatycznymi, jest obecnie zadaniem precyzyjnie zdefiniowanym. Jego przeprowadzenie wymaga ograniczonej wiedzy specjalistycznej i dobrej wiedzy z zakresu standardów nadzoru nad systemami informatycznymi.

Audyt formalny wymaga wiedzy z zakresu metodyk projektowania rozwiązań informatycznych oraz zarządzania projektami. Może on zostać przeprowadzony również przez osoby nie posiadające specjalistycznej wiedzy dziedzinowej, w szczególności informatycznej.

Audyt merytoryczny wymaga szczegółowej wiedzy specjalistycznej pozwalającej poznać i ocenić rzeczywiste rozwiązania techniczne i organizacyjne. Wymaga on samodzielnego, indywidualnego zdefiniowania kryteriów oceny, a często także umiejętności przeprowadzenia badań na konkretnym, działającym rozwiązaniu.

Przeprowadzenie oceny rozwiązań informatycznych na odpowiednim etapie ich tworzenia może znacząco ograniczyć ryzyko przedsięwzięcia i zwiększyć jakość ostatecznego rozwiązania. Z kolei kryteria oceny rozwiązań informatycznych mogą stanowić istotne wytyczne przy ich projektowaniu. W tym kontekście prace nad metodyką audytu merytorycznego mogą w istotny sposób wpłynąć na metody wytwarzania rozwiązań informatycznych.

Bibliografia

[COBIT] *COBIT 3rd Edition*, IT Governance Institute, 2002.

[ISO9126] *ISO/IEC 9126 : Information technology - Software Product Evaluation - Quality characteristics and guidelines for their use*, 1991.

[ITSEC] *European Orange Book*, EC advisory group, Senior Officials Group - Information Systems Security, Department of Trade and Industry, London.

[ITSEM] *Information Technology Security Evaluation Manual*, EC advisory group, Senior Officials Group - Information Systems Security, Department of Trade and Industry, London.

[PRINCE2] *strona internetowa metodyki PRINCE2*, www.prince2.org.uk, www.prince2.com.

[TCSCEC] *DoD 5200.28-STD Orange Book*, American Department of Defence (DoD).