BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 21, 2004

Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny" ?

Krzysztof LIDERMAN

Zakład Systemów Komputerowych, Instytut Teleinformatyki i Automatyki WAT
ul. Kaliskiego 2, 00-908 Warszawa

STRESZCZENIE: W artykule została przeprowadzona dyskusja, często używanych w ramach szeroko rozumianego bezpieczeństwa teleinformatycznego, terminów „audyt informatyczny" oraz „audyt bezpieczeństwa teleinformatycznego". Niniejsza publikacja jest wstępem do metodyki LP–A audytu bezpieczeństwa teleinformatycznego i dla zapewnienia kompletności przedstawionego wywodu zawiera fragmenty artykułów zamieszczonych w [2], [3] i [4].

1. Wstęp

Słowo „audyt" jest kojarzone głównie z kontrolą dokumentów księgowych przedsiębiorstwa. Znajomość terminu „audyt informatyczny" – jak wynika z badań przeprowadzonych przez CBOS – deklaruje 60 proc. małych i dużych przedsiębiorców[1]. Większość z nich (75%) rozumie jego znaczenie jako weryfikację legalności oprogramowania używanego w firmie, jako inne cele wskazując kontrolę bezpieczeństwa systemu komputerowego (24%) i sprawdzenie jego efektywności (13 %).

Jak wynika z przytoczonych wyników badań, określenie audytu jakimś przymiotnikiem wcale nie przyczynia się do zlikwidowania niejasności, a wręcz przeciwnie, niejasności pogłębia. Robiąc nawet pobieżny przegląd witryn

[1] *Bartłomiej Witucki:* W firmach małe zainteresowanie. *Gazeta Prawna. 23.05.03*

internetowych firm, które w swojej ofercie mają audyt związany w jakiś sposób z informatyką, można natknąć się na następujące sformułowania:

- Audyt informacyjny – jako diagnoza stanu posiadania strategii biznesowej, ocena jej poprawności oraz ocena postrzegania i stopnia jej akceptacji wśród pracowników firmy.
- Audyt informatyczny – jako ocena stanu informatyzacji badanej organizacji, w szczególności sprawdzenie, czy odpowiada ona odpowiada celom biznesowym zidentyfikowanym np. w audycie informacyjnym. W ramach tego audytu realizowana jest inwentaryzacja zasobów teleinformatycznych oraz identyfikowane są cele, jakie stawiane są przed informatyką w danym przedsiębiorstwie dziś i w dającej się przewidzieć przyszłości.
- Audyt informatyczny e-biznes – jako analiza możliwości wejścia firmy na rynek e-biznesu. Prace audytorów dotyczą szacowania kosztów, oceny korzyści z wykorzystania rozwiązań e-biznesowych, propozycji strategii e-biznesowej, doboru odpowiednich narzędzi informatycznych, propozycji integracji z istniejącym systemem informatycznym.
- Audyt telekomunikacyjny – jako ocena wykorzystania infrastruktury telekomunikacyjnej.
- Audyt bezpieczeństwa – jako wykonanie tzw. testów penetracyjnych oraz ocena bliżej nie zdefiniowanej polityki i procedur bezpieczeństwa, czasami połączona z oceną czegoś, co nazywane jest bezpieczeństwem fizycznym[2].

Ograniczając się tylko do audytu informatycznego, można stwierdzić, że rozumiany jest on potocznie jako:

- analiza wsparcia przez poszczególne systemy informatyczne funkcji biznesowych,
- ocena możliwości dostosowania i rozbudowy zasobów informatycznych zgodnie z potrzebami przedsiębiorstwa,
- ocena bezpieczeństwa zasobów informatycznych przedsiębiorstwa i przyjętej polityki ochrony danych,
- sposób uzyskania wyczerpujących i aktualnych informacji o zainstalowanym oprogramowaniu, posiadanych licencjach oraz zasobach sprzętowych.

[2] Dla uzupełnienia podanych przykładów jeszcze dwa cytaty z rzeczywistych umów:

1. „ ... wykonanie *audytu bezpieczeństwa systemu i sieci teleinformatycznej* ... Audyt ma obejmować całą sieć korporacyjną ... (Biuro Prezesa, xx oddziałów terenowych/filii, yy przedstawicielstwa/sekcje zamiejscowe) i mieć następujący zakres: ... ”
2. „Przedmiotem niniejszej umowy jest *ocena bezpieczeństwa teleinformatycznego* w firmie ... obejmująca zasoby i systemy teleinformatyczne zlokalizowane w siedzibie ... ”

Odpowiedź na pytanie zawarte w tytule wymaga zatem szerszego wprowadzenia. W praktyce bowiem okazuje się często, że zainteresowane w realizacji umowy strony różnie interpretują takie terminy, jak:

- bezpieczeństwo teleinformatyczne,
- ocena (w szczególności: ocena bezpieczeństwa teleinformatycznego),
- audyt (w szczególności: audyt bezpieczeństwa systemów i sieci teleinformatycznych).

Celem niniejszego artykułu jest przedstawienie propozycji interpretacji ww. terminów i na tej podstawie wskazanie różnic w realizacji audytów wymienionych w tytule artykułu.

2. Bezpieczeństwo teleinformatyczne

Sam termin „bezpieczeństwo" jest trudny do zdefiniowania. Wydaje się że jest zrozumiały, ale jest to rozumienie intuicyjne. Potocznie oznacza on niepodleganie obawie, spokój; pewność, że się nic złego nie stanie. Bardziej precyzyjnie – poziom racjonalnie uzasadnionego zaufania, że potencjalne straty nie zostaną poniesione. Mając na uwadze takie rozumienie bezpieczeństwa, proponuje się następującą definicję bezpieczeństwa teleinformatycznego [1]:

> *Termin* **bezpieczeństwo teleinformatyczne** *oznacza poziom uzasadnionego*[3] *zaufania, że potencjalne straty, wynikające z niepożądanego (przypadkowego lub świadomego) ujawnienia, modyfikacji, zniszczenia lub uniemożliwienia przetwarzania informacji przechowywanej i przesyłanej za pomocą systemów teleinformatycznych, nie zostaną poniesione.*

Zgodnie z tą definicją, że bezpieczeństwo teleinformatyczne dotyczy **informacji** oraz pośrednio, jako środka przechowywania, przesyłania i przetwarzania informacji, **systemów teleinformatycznych**. Warto sobie uświadomić, że celem wszelkich działań z zakresu bezpieczeństwa teleinformatycznego jest ochrona informacji a nie komputerów. Komputery (ogólnie: zasoby teleinformatyczne) chronimy przed nieupoważnionym dostępem, zniszczeniem itd. przede wszystkim dlatego, że są nosicielami informacji. Brak tej świadomości prowadzi do skupienia się podczas budowy systemu bezpieczeństwa (lub podczas oceny stanu bezpieczeństwa) na zasobach,

[3] Np. analizą ryzyka.

a nie na informacji, co w konsekwencji często prowadzi do zbudowania nieskutecznego systemu ochrony (lub błędnej oceny).

Dlaczego chronimy informację? Chronimy informację, ponieważ:

2) Jest ona towarem o znaczeniu strategicznym (dla kraju, firmy, konkretnego człowieka).

   Od zarania dziejów ci, którzy dysponowali właściwą informacją we właściwym czasie, wygrywali wojny oraz osiągali sukcesy rynkowe. Dlatego, podobnie jak współcześnie rudy uranu czy nowe technologie, informacja jest towarem, który można kupić, dzięki któremu można osiągnąć określone korzyści i który trzeba chronić, mając na względzie własne interesy.

3) Jest podstawowym elementem procesów biznesowych.

   Podstawą działania prawie wszystkich współczesnych firm i organizacji jest poprawny obieg informacji. Przerwanie tego obiegu lub sfałszowanie informacji powoduje straty kończące się często dla firmy bankructwem.

4) Tak nakazują przepisy obowiązującego prawa lub wynika to z zawartych umów.

   Ze względów przedstawionych w punktach 1 i 2 oraz ze względu na ochronę dóbr osobistych obywateli, we wszystkich cywilizowanych krajach ustanowiono przepisy prawne mające na celu ochronę informacji przed nieuprawnionym dostępem, zapewnienie jej właściwego przetwarzania, przechowywania i przesyłania oraz określające zasady zbierania określonych kategorii informacji.

Przepisy obowiązującego prawa, o których jest mowa w punkcie 3, obejmują część artykułów Kodeksu Karnego oraz pokaźną listę ustaw i rozporządzeń, jak np.:

1. Konstytucja Rzeczpospolitej Polskiej.
2. Ustawa z dnia 22.01.1999 r. „*o ochronie informacji niejawnej*". Dz. U. 11/99 poz. 95. Znowelizowana 3.02.2001 (nowelizacja weszła w życie 8.04.2001).
3. Rozporządzenie Prezesa Rady Ministrów z dn. 25.02.1999 „*w sprawie podstawowych wymagań bezpieczeństwa systemów i sieci teleinformacyjnych*". Dz. U. 18/99 poz. 162.
4. Rozporządzenie MSWiA oraz ON z dn. 26.02.1999 „*w sprawie sposobu oznaczania materiałów, w tym klauzulami tajności, oraz sposobu umieszczania klauzul na tych materiałach*". Dz. U. 18/99 poz. 167.

5. Ustawa z dn. 29.08.97 „*o ochronie danych osobowych*". Dz. U. z dn. 29.10.97 (znowelizowana ustawą z dn. 25.08.2001).

6. Rozporządzenia Ministra Spraw Wewnętrznych i Administracji 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"* (Dz. U. z 2004 r. Nr 100, poz. 1024).

7. Ustawa z dn. 29.09.1994 „*o rachunkowości*"**.** Dz.U. Nr 121 poz.591. Znowelizowana – nowelizacja obejmuje również szczegółowe wytyczne dotyczące techniki komputerowej stosowanej w rachunkowości (nowelizacja obowiązuje od 01.01.2002).

8. Ustawa z dn. 18.09.2001 *„o podpisie elektronicznym"* Dz.U. Nr 130, poz.1450 (wejście w życie 16.08.2002).

9. Ustawa z dn. 4.02.1994 „*prawo autorskie i prawa pokrewne*". Dz.U.94.24.83.

10. Ustawa z dn. 21.08.1997 „*prawo o obrocie papierami wartościowymi*"**.** Dz.U. 118/97.

11. Ustawa z dn. 16.04.1993 „*o zwalczaniu nieuczciwej konkurencji*". Dz.U.93.47.211[4].

12. Ustawa z dn. 10.01.2003 *„o zmianie ustawy – Kodeks postępowania karnego, ustawy – Przepisy wprowadzające Kodeks postępowania karnego, ustawy o świadku koronnym oraz ustawy o ochronie informacji niejawnych"*. Dz.U. Nr 17, poz.155.

13. Ustawa z dn. 21.07.2000 *„Prawo telekomunikacyjne"* Dz.U. Nr 73, poz.852.

14. Ustawa z dn. 6.09.2001 „*o dostępie do informacji publicznej*" Dz.U. Nr 112, poz.1198.

15. Ustawa z dn. 27.07.2001 *„o ochronie baz danych"* Dz.U. Nr 128, poz.1402 (wejście w życie 9.11.2002).

16. Ustawa z dn.18.07.2002 *„o świadczeniu usług droga elektroniczną"*. Dz.U.Nr 144, poz. 1204 (wejście w życie 10.03.2003 z wyjątkiem art.5 ust.5 który stosuje się od dnia uzyskania przez Polskę członkostwa w Unii Europejskiej).

[4] Art.11 pkt. 4: „Przez **tajemnicę przedsiębiorstwa** rozumie się nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, **co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności"**.

17. Ustawa z dn. 05.07.2002 *„o ochronie niektórych usług świadczonych drogą elektroniczną opartych lub polegających na dostępie warunkowym”*. Dz.U.Nr 126/02 poz. 1068 (wejście w życie 10.11.2002).

Należy mieć na uwadze fakt, że oprócz ww. dokumentów podstawowych, w praktyce obowiązuje szereg przepisów i zarządzeń resortowych (bankowych [19], [20], wojskowych, Agencji Bezpieczeństwa Wewnętrznego) regulujących szczegółowo poszczególne zakresy tematyczne bezpieczeństwa teleinformatycznego. Poza tym w prawie polskim wyróżnia się wiele rodzajów informacji prawnie chronionych (tajemnic), takich jak: tajemnicę postępowania administracyjnego i karnego, tajemnicę lekarską, tajemnicę skarbową, tajemnicę handlową, tajemnicę bankową, tajemnicę ubezpieczeń społecznych, tajemnicę publicznego obrotu papierami wartościowymi, tajemnicę dziennikarską, tajemnicę pomocy społecznej itd. Jednak dokumenty najważniejsze pod względem praktycznym, to (przynajmniej tak wynika z dotychczasowej praktyki piszącego te słowa) dokumenty wymienione na pozycjach 2, 3, 5 i 6 przedstawionej wcześniej listy.

3. Ocena bezpieczeństwa teleinformatycznego i standardy

Zarówno użytkownicy systemów teleinformatycznych, jak i kierownictwo instytucji eksploatujących te systemy, szczególnie po zainwestowaniu dużych sum w bezpieczeństwo teleinformatyczne, które przecież nie przynosi natychmiastowych, wymiernych zysków, są zainteresowani odpowiedzią na pytanie *„czy eksploatowany system teleinformatyczny jest bezpieczny?”* (w sensie: czy *informacja* w nim przetwarzana jest bezpieczna). Żeby móc rzetelnie odpowiedzieć na takie pytanie, należy najpierw przeprowadzić proces oceny bezpieczeństwa teleinformatycznego [1], [2].

> ***Ocenianiem bezpieczeństwa informacji w systemach teleinformatycznych***[5] *nazywa się proces określenia wartości miary gwarantowanej odporności systemu teleinformatycznego na czynniki mogące spowodować utratę tajności*[6]*, integralności i dostępności przetwarzanej w nim informacji.*

[5] Definicja podana za [14].

[6] **Tajność** opisuje stopień ochrony informacji jakiej ma ona podlegać. Stopień ten jest uzgadniany przez osoby lub organizacje dostarczające i otrzymujące informację (z tajnością jest ściśle związana, *dotycząca ludzi,* poufność, czyli prawo jednostki do

Ocenianie bezpieczeństwa informacji w systemach teleinformatycznych powinno być realizowane na podstawie:

- konkretnej polityki bezpieczeństwa teleinformatycznego,
- spójnego opisu wymaganych funkcji zabezpieczenia,
- docelowego, pożądanego poziomu miary gwarantowanej odporności.

Wynikiem oceniania jest **raport** oceniającego, opisujący procedury badawcze i testujące, zastosowane podczas analizy właściwości zabezpieczenia systemu teleinformatycznego, **wraz z opisem i wynikami testów** zastosowanych w celu potwierdzenia lub zaprzeczenia istnienia określonych wad (podatności) systemu.

Miary gwarantowanej odporności[7] są zwykle określane przez odpowiednie standardy, np: w *Common Criteria* będą to tzw. *Evaluation Assurance Level* (EAL), a w TCSEC[8] klasy bezpieczeństwa D, C, B, A.

Proces oceny może być przeprowadzony własnymi siłami firmy, o ile posiada ona odpowiednio kompetentny w tym zakresie pion teleinformatyki i komórkę bezpieczeństwa (i wtedy mówi się o ocenie poziomu bezpieczeństwa teleinformatycznego według np. zaleceń standardu BS 7799) lub ocena może być zlecona zewnętrznemu, niezależnemu zespołowi (i wtedy może to być audyt).

Najważniejsze międzynarodowe normy i standardy w zakresie oceny bezpieczeństwa teleinformatycznego to:

1. *Trusted Computer System Evaluation Criteria* (TCSEC – tzw. *Orange Book)*;
2. *Information Technology Security Evaluation Criteria* (ITSEC);
3. *Evaluation Criteria for Information Technology Security* – norma ISO/IEC 15408 (Common Criteria);
4. *Control Objectives for Information and Related Technology* (COBIT™) – standard ISACA (*Information Systems Audit and Control Association*);
5. Standard brytyjski *BS 7799* (w grudnia 2000 roku na jego podstawie została wydana norma ISO/IEC 17799:2000);
6. Raport techniczny *ISO/IEC TR 13335:1997* (arkusz 1 został wydany jako norma polska PN–I–13335–1:1999).

---

decydowania o tym, jakimi informacjami chce się podzielić i jakie jest skłonna przyjąć).

[7] Omówienie terminu „miara gwarantowanej odporności" zostało zamieszczone m.in. w [2] i [3].

[8] *Trusted Computer System Evaluation Criteria. DoD. 15 August 1983. CSC-STD-001-83*. Dokument znany jest pod nazwą „Pomarańczowej książki".

Miara gwarantowanej odporności powinna dawać pewność[9], że obiekt oceniany spełnia cele zabezpieczenia. Zwykle jest nią właściwość obiektu ocenianego, dająca podstawy, aby sądzić, że jego funkcje zabezpieczenia realizują koncepcję bezpieczeństwa określoną dla obiektu. Zgodnie z normą terminologiczną PN–I–02000 wyróżnia się:

- miarę gwarantowanej odporności związaną z oceną (ang. *evaluation assurance***)** – jest to część miary gwarantowanej odporności, wynikająca z zestawienia składników miary gwarantowanej odporności, określających fakty i działania wymagane od oceniającego;
- miarę gwarantowanej odporności związaną z projektowaniem (ang. *development assurance*) – jest to część miary gwarantowanej odporności, wynikająca z zestawienia składników miary gwarantowanej odporności, określająca parametry i działania wymagane od wytwórcy.

Poziom gwarantowanej odporności systemu jest to określony zestaw składników miary gwarantowanej odporności, za pomocą którego przypisuje się miarę właściwej jakości zabezpieczenia do obiektu.

Poziom oceny gwarantowanej odporności jest to określony zestaw składników miary gwarantowanej odporności[10], reprezentujący punkt na skali miary gwarantowanej odporności nadzorowanej konfiguracji (np. w *Common Criteria* będzie to tzw. EAL – *Evaluation Assurance Level* po polsku przetłumaczony jako Poziom Uzasadnionego Zaufania).

Próby ustandardowienia zagadnień związanych z ochroną i oceną bezpieczeństwa informacji w systemach informatycznych były podejmowane w praktyce od połowy lat sześćdziesiątych, gdy zaczęły wchodzić do powszechnego użytku systemy wielodostępne oraz pojawiły się pierwsze sieci komputerowe. Pierwszymi udanymi (tj. takimi, które wywarły istotny wpływ na sposób rozumienia problematyki bezpieczeństwa w systemach informatycznych i na wiele lat stały się podstawą do opracowywania lokalnych standardów w tym zakresie) były zalecenia wydane w USA w 1983 w postaci tzw. „Pomarańczowej książki".

Można wyróżnić dwa rodzaje standardów z zakresu bezpieczeństwa teleinformatycznego:

1) standardy, na podstawie których można przeprowadzać certyfikacje systemów

[9] Skuteczność i poprawność są głównymi składnikami pewności (za [14]).

[10] Składnik miary gwarantowanej odporności jest to indywidualne kryterium na najniższym poziomie opisu, przedstawiające cechę i wymagane działania niezbędne do osiągnięcia skuteczności i poprawności przetwarzania informacji.

i produktów teleinformatycznych, np. ISO–15408 (*Common Criteria*), ITSEC, TCSEC;

2) standardy stanowiące tzw. *best practices*, np. BS 7799, PN–I–13335–1, traktujące o tym jak powinno budować się „bezpieczne" systemy teleinformatyczne.

Cechą charakterystyczną standardów z punktu 1) jest podawanie miar w postaci:

- klas – w TCSEC (np. Windows NT 4.0 jako produkt – przy pewnych ograniczeniach – posiada klasę C2 według TCSEC);
- poziomów E0–E6 – w ITSEC;
- poziomów uzasadnionego zaufania EAL – w PN-ISO/IEC-15408[11].

Przykładowo, taki produkt jak Oracle 9i może posiadać certyfikaty dla standardów z grupy 1); dla standardów z grupy 2) certyfikatów się nie wystawia, bo nie podają one miar, dla których taką certyfikację można przeprowadzić. Obie grupy standardów mogą natomiast stanowić podstawę audytu w zakresie bezpieczeństwa teleinformatycznego dla konkretnych systemów teleinformatycznych.

Podstawową zaletą standardów z **punktu widzenia audytora** (definicja terminu „audytor" i omówienie procesu audytu por. rozdz. 4) jest to, że systematyzują proces oceny systemu zabezpieczeń oraz stanowią platformę odniesienia pozwalającą uzyskać powtarzalność procesu oceny i porównywanie uzyskanych wyników. Mogą stanowić również punkt wyjścia przy formułowaniu kontraktu na przeprowadzenie audytu, ponieważ zawarcie w kontrakcie klauzuli mówiącej, że proces oceny ma zostać przeprowadzony np. zgodnie z zaleceniami ISO/IEC 15408, znacznie upraszcza rozliczalność takiego przedsięwzięcia.

Należy jednak pamiętać, że posiadanie certyfikatu przez produkt (system) oznacza tylko tyle, że produkt/system został wykonany zgodnie z zaleceniami określonego standardu. Jeżeli np. system operacyjny został zakwalifikowany do klasy B3 według standardu TCSEC, oznacza to, że: umożliwia dostęp do zasobów na podstawie etykietowania, jest dostępna pełna dokumentacja projektowa systemu, system został zaprojektowany z wykorzystaniem metodyk strukturalnych etc. Zakłada się, że jeżeli produkt zostanie wytworzony zgodnie z wymaganiami określonego standardu, to jego cechy związane z bezpieczeństwem teleinformatycznym będą na wyższym poziomie jakościowym niż wtedy, gdy z zaleceń standardów się nie korzysta. Podobnie posiadanie przez firmę certyfikatów z rodziny ISO-9000 nie chroni

[11] Windows 2000 w 2002 roku uzyskał certyfikat poziomu EAL 4 (+ Flaw Remediation).

automatycznie przed produkcją bubli, chociaż powinno radykalnie taką możliwość ograniczyć.

Pojawia się tutaj pytanie, czy certyfikaty (i w konsekwencji określone standardy i normy) są potrzebne. Odpowiedź brzmi „tak", ponieważ firmy które nie będą ich posiadały dla eksploatowanych systemów teleinformatycznych i używanych produktów, stawiają się w niekorzystnej sytuacji w porównaniu firmami które taki certyfikat uzyskały. Do uzasadnienia tej tezy może posłużyć chociażby zawartość dokumentu *„Council Resolution of 28 January 2002 on a common approach and specificactions in the area of network and information security(2002/C 43/02)"*[12] i stosowane na Zachodzie praktyki. Na przykład w USA firma, która nie posiada certyfikatu SEI CMM określającego odpowiedni stopień „dojrzałości organizacyjnej", z definicji nie jest dopuszczana do kontraktów realizowanych na zamówienie Departamentu Obrony. Inny przykład: od III kwartału 2003 wszystkie kraje członkowskie NATO muszą (przynajmniej w zakresie związanym z działalnością NATO, a jest ona bardzo obszerna), wdrożyć stosowanie normy ISO-15408. Podsumowując – certyfikaty są potrzebne, bo wymagają ich formalne zasady postępowania w szeroko rozumianej działalności biznesowej, szczególnie jeżeli jest ona prowadzona na arenie międzynarodowej.

Na zakończenie ogólnych rozważań o standardach i normach jeszcze często stawiane w kontekście norm i standardów pytania: *Czy warto stosować pewne z góry założone procedury i metodyki przy testowaniu bezpieczeństwa? Czy intruzi trzymają się standardów albo sztywnych metodyk działania?* Piszący te słowa uważa, że trzeba korzystać ze standardów bo, jak już zostało to wspomniane wcześniej, porządkują one proces audytu i umożliwiają porównywanie wyników. Brak metodyki przy każdym postępowaniu w dziedzinie technicznej (nie dotyczy to oczywiście różnych dziedzin sztuki) jest amatorstwem, a nie profesjonalizmem. Wbrew pozorom, również intruzi działają najczęściej metodycznie. Gdyby było inaczej, nie można byłoby np. opracować sygnatur dla narzędzi IDS. Należy jednak zauważyć, że zgodnie z proponowanym w rozdz. 4 rozumieniem, audyt jest **działaniem kompleksowym** – obejmuje czynności sprawdzające zarówno zgodność ze standardami (lista audytowa), jak i testy penetracyjne, które w pewnym sensie można potraktować jako element „sztuki".

[12] Dokument ten zaleca stosowanie standardów ISO-15408 i ISO-17799.

3.1. Standard ISACA COBIT™ audytu informatycznego

Jednym z tzw. „otwartych" standardów związanych z oceną bezpieczeństwa teleinformatycznego jest, preferowany zwłaszcza w organizacjach takich jak banki czy towarzystwa ubezpieczeniowe, standard audytu informatycznego COBIT™ opracowany i rozwijany w ramach ISACA (*Information Systems Audit and Control Association*).

Działania ISACA koncentrują się na zagadnieniach audytu i bezpieczeństwa systemów teleinformatycznych. W ramach tej problematyki ISACA opracowuje standardy, prowadzi szkolenia i certyfikacje. Wraz z ISACF (*Information Systems Audit and Control Foundation*) tworzy i publikuje opracowania pomagające dotrzymywać kroku ciągle zmieniającemu się środowisku systemów informatycznych. Najbardziej znanymi działaniami ISACA są: program certyfikacji CISA (*Certified Information System Auditor*), oraz opracowanie i opublikowanie w 1996 roku standardu COBIT™ (*Control Objectives for Information and Related Technology*).

Celem tego ostatniego przedsięwzięcia jest („jest", a nie „było", ponieważ jest to ciągle rozwijany, otwarty standard dostępny częściowo również w Internecie) *„... badanie, rozwijanie, publikowanie i promowanie autorytatywnego, aktualnego zbioru celów kontroli systemów teleinformatycznych dla codziennego użytku przez kierownictwo i audytorów, akceptowanych przez społeczność międzynarodową"*. Podstawowe części dokumentacji standardu to:

- „Executive Summary",
- „Framework"
- „Control Objectives"
- „Audit Guidelines"
- „Implementation Tool Set"

Zasadniczą częścią tego zestawu są „Control Objectives", które zawierają 302 szczegółowe wymagania przypisane do 34 procesów przebiegających w systemach informatycznych. Tabela 1.1 pokazuje w syntetyczny sposób lansowaną przez ISACA ideę audytu informatycznego. Poszczególne wiersze zawierają procesy biznesowe organizacji związane z wykorzystaniem informatyki, kryteria oceny tych procesów (1–7) oraz zasoby których dotyczą (I–V). Dla każdego procesu w COBIT są zdefiniowane tzw. punkty kontrolne (w sumie jest ich 302), dla których osoba przeprowadzająca ocenę musi znaleźć uzasadnione potwierdzenie ich spełnienia lub niespełnienia w ramach ocenianej organizacji.

Tabela 1.1. Audyt informatyczny według COBIT

		Kryteria							Zasoby informatyczne				
PROCES	**NAZWA**	1	2	3	4	5	6	7	I	II	III	IV	V
Planowanie i organizowanie													
PO1	Definiowanie planu strategicznego IT	P	S						X	X	X	X	X
PO2	Definiowanie architektury IT	P	S	S	S					X			X
PO3	Determinowanie kierunku technologicznego	P	S								X	X	
PO4	Definiowanie organizacji i relacji IT	P	S						X				
PO5	Zarządzanie inwestycjami IT	P	P					S	X	X	X	X	
PO6	Przedstawienie celów i kierunków rozwoju formułowanych przez kierownictwo	P					S		X				
PO7	Zarządzanie zasobami ludzkimi	P	P						X				
PO8	Zapewnianie zgodności z wymogami otoczenia	P					P	S	X	X			X
PO9	Szacowanie ryzyka	S	S	P	P	P	S	S	X	X	X	X	X
PO10	Zarządzanie projektami	P	P						X	X	X	X	
PO11	Zarządzanie jakością	P	P		P			S	X	X			
Nabywanie i wdrażanie													
AI1	Identyfikacja rozwiązań	P	S							X	X	X	
AI2	Nabywanie i utrzymywanie oprogramowania aplikacyjnego	P	P		S		S	S		X			
AI3	Nabywanie i utrzymywanie architektury technologicznej	P	P		S						X		
AI4	Rozwijanie i utrzymywanie procedur IT	P	P		S		S	S	X	X	X	X	
AI5	Instalowanie i akredytowanie systemów	P			S	S			X	X	X	X	X
AI6	Zarządzanie zmianami	P	P		P	P		S	X	X	X	X	X
Dostarczanie i wspieranie													
DS1	Definiowanie poziomów serwisowych	P	P	S	S	S	S	S	X	X	X	X	X
DS2	Zarządzanie obcym serwisem	P	P	S	S	S	S	S	X	X	X	X	X
DS3	Zarządzanie efektywnością i wydajnością	P	P			S				X	X	X	
DS4	Zapewnianie ciągłości serwisu	P	S			P			X	X	X	X	X
DS5	Zapewnianie bezpieczeństwa systemów			P	P	S	S	S	X	X	X	X	X
DS6	Identyfikowanie i przypisywanie kosztów		P					P	X	X	X	X	X
DS7	Edukowanie i szkolenia użytkowników	P	S						X				
DS8	Asystowanie i pomaganie klientom IT	P							X	X			
DS9	Zarządzanie konfiguracją	P				S		S		X	X	X	
DS10	Zarządzanie problemami i incydentami	P	P			S			X	X	X	X	X
DS11	Zarządzanie danymi				P			P					X
DS12	Zarządzanie urządzeniami				P	P						X	
DS13	Zarządzanie operacjami	P	P		S	S			X	X		X	X
Monitorowanie													
M1	Monitorowanie procesów	P	S	S	S	S	S	S	X	X	X	X	X
M2	Ocena odpowiedniości kontroli wewnętrznej	P	P	S	S	S	S	S	X	X	X	X	X
M3	Uzyskiwanie niezależnej opinii	P	P	S	S	S	S	S	X	X	X	X	X
M4	Zapewnienie niezależnego audytu	P	P	S	S	S	S	S	X	X	X	X	X

Oznaczenia w tabeli:

P – znaczenie pierwszorzędne dla oceny procesu wykorzystania i przetwarzania informacji

S – znaczenie drugorzędne dla oceny procesu wykorzystania i przetwarzania informacji

Kryteria oceny procesu wykorzystania i przetwarzania informacji: 1 – skuteczność, 2 – wydajność, 3 – poufność, 4 – integralność, 5 – dostępność, 6 – zgodność, 7 – rzetelność

Zasoby informatyczne: I – ludzie, II – aplikacje, III – technologie, IV – urządzenia, V – dane

Na przykład dla procesu DS12 „Zarządzanie urządzeniami" punkty kontrolne dotyczą:

- DS12.1: bezpieczeństwa fizycznego
- DS12.2: utrudnienia osobom obcym identyfikacji rozmieszczenia sprzętu komputerowego
- DS12.3: nadzoru nad osobami obcymi przebywającymi na terenie organizacji
- DS12.4: BHP
- DS12.5: przeciwdziałania skutkom zagrożeń środowiskowych (upał, wilgoć, ogień itd.)
- DS12.6: zasilania awaryjnego.

3.2. Standard BS 7799 oceny bezpieczeństwa teleinformatycznego

Standard BS 7799 został opracowany w połowie lat 90-tych przez British Standards Institute i podlega cały czas aktualizacji. W części pierwszej *„Code of practice for Information Security Management"* [7] dokumentu opisane są „najlepsze praktyki", które powinny być stosowane w budowie i zarządzaniu bezpiecznych systemów teleinformatycznych. Na tej podstawie, w części drugiej BS 7799 pt. *„Specification for Information Security Management Systems"* [8], zdefiniowanych jest 127 punktów kontrolnych (wymagań na bezpieczeństwo teleinformatyczne), zgrupowanych w dziesięć tematów. Te tematy (w oryginale numerowane poczynając od liczby trzy) to:

1. Polityka bezpieczeństwa;
2. Organizacja bezpieczeństwa;
3. Kontrola i klasyfikacja zasobów;
4. Bezpieczeństwo a personel;
5. Bezpieczeństwo fizyczne;
6. *Zarządzanie komputerami i siecią komputerową;*
7. *Kontrola dostępu do systemu;*
8. *Projektowanie i utrzymywanie systemu;*
9. Planowanie ciągłości procesów biznesowych;

10. Zgodność z obowiązującymi regulacjami prawnymi.

Warto zauważyć, że to, co w powszechnym rozumieniu kojarzy się z pojęciem bezpieczeństwa teleinformatycznego i audytu, w tym zakresie to punkty 6-8 powyższej listy. Jest to niestety prowadzący do nieporozumień powszechny pogląd kadry kierowniczej (a więc osób zlecających i płacących za audyt) i również, przynajmniej części, informatyków. Zdarza się bowiem, że realizując zlecenie na audyt, gdy padają pytania o:

- inwentaryzację zasobów teleinformatycznych w firmie,
- schemat obiegu informacji w firmie,
- podległość wykorzystywanej w firmie informacji pod obowiązujące ustawy, itp.

spotkać się można z niezrozumieniem i pytaniem *„a po co wam to, przecież macie tylko sprawdzić, czy nie ma luk w sieci”*.

Przedstawiona lista tematów wspiera również podstawowe założenie bezpieczeństwa teleinformatycznego: system bezpieczeństwa powinien być systemem **kompleksowym**, wykorzystującym w spójny sposób zabezpieczenia:

- organizacyjne i kadrowe,
- fizyczne i techniczne
- sprzętowo-programowe,

i systemem pozwalającym na wykrycie przełamania zabezpieczeń (oraz prób takich działań) oraz skuteczną ochronę pomimo przełamania części zabezpieczeń.

Od 1.12.2000 zalecenia brytyjskie opublikowane w *„Code of Practice for Information Security Management”* zostały przyjęte jako norma ISO/IEC 17799:2000[13].

4. Audyt

Termin „audyt” jest powszechnie znany i często (również nieprawidłowo) używany. Podstawową przyczyną nieporozumień jest fakt, że termin „audyt” jest zapożyczony wprost z języka angielskiego i nie ma właściwego odpowiednika w języku polskim. Np. [21] nie zawiera definicji terminu „audyt”, natomiast zawiera definicję terminu „audytor”, który to termin jest również (ale w innym znaczeniu!) używany w żargonie informatycznym. Zgodnie z [21], audytor to:

[13] Od września 2003 dostępna jest również polska norma PN–ISO/IEC 17799:2003.

> audytor *m IV, DB*. –a, *Ms*. ~orze; *lm M*. ~ orzy a. –owie 1. <<rzecznik przy sądzie wojskowym; sędzia wojskowy>> 2. <<w sądownictwie kościelnym: sędzia delegowany do przygotowania materiału procesowego, gromadzenia środków dowodowych itp.; członek trybunału Roty>> <łc.>

W słownikach języka angielskiego, np. w [22] definiuje się te terminy następująco:

> audit *n* official examination of accounts to see that they are in order. *vt* exmine,eg. accounts, officially.
>
> auditor *n* 1 listener to a speaker. etc. 2. person who audits.

Dalej podane są definicje z normy *PN–EN ISO 9000:2001 – terminologia* [11]. Norma ta dotyczy systemów jakości ale, ze względu na jej międzynarodowe znaczenie i wpływ na szeroko rozumiane procesy audytu, zostały dalej z niej przytoczone odpowiednie definicje. Przy okazji warto zauważyć, że Polski Komitet Normalizacyjny, tj. organizacja która powinna m.in. dbać o spójność i jednoznaczność terminologii, przyjęła w tej normie pisownię „audit", odmienną od stosowanej chociażby w normie [14] (wydanej przez ten sam organ normalizacyjny) pisowni „audyt" oraz utartej wieloletnią praktyką wymowy tego wyrazu.

> **3.9.1**
> **audit**
> usystematyzowany, niezależny i udokumentowany **proces** (3.4.1) uzyskania **dowodu z auditu** (3.9.5) i obiektywnej oceny w celu określenia w jakim stopniu spełniono uzgodnione **kryteria auditu** (3.9.3).
>
> UWAGA: Audity wewnętrzne czasami nazywane są auditami *pierwszej strony*, są przeprowadzane przez, lub w imieniu **organizacji** (3.9.4), dla wewnętrznych celów i mogą mieć postać samodeklaracji **zgodności** (3.6.1) organizacji. Zewnętrzne audity zawierają określenia auditów „drugiej" lub „trzeciej strony".
>
> Audity *drugiej strony* przeprowadzane są przez strony zainteresowane takie jak klienci lub inne osoby w ich imieniu.
>
> Audity *trzeciej strony* przeprowadzane są przez zewnętrzne niezależne organizacje. Takie organizacje poświadczają certyfikacją lub rejestracją zgodność z wymaganiami takimi jak ISO 9001 czy ISO 14001:1996.
>
> Gdy poddawany auditowi jest jednocześnie **system zarządzania** (3.2.2) jakością i środowiskiem, audit taki definiowany jest jako „audit połączony".
>
> Gdy dwie lub więcej jednostek współdziała ze sobą podczas wspólnego auditowania auditowanego (3.9.8), audit taki definiowany jest jako „audit wspólny".
>
> **3.9.9**
> **auditor**
> osoba posiadająca **kompetencje** (3.9.12) do przeprowadzenia **auditu** (3.9.1).

3.9.10
zespół auditujący
osoba lub grupa osób przeprowadzająca **audit** (3.9.1).

UWAGA_1: Zwykle jeden z auditorów z zespole auditującym jest mianowany liderem tego zespołu (tzw. „auditor wiodący").

UWAGA_2: Do zespołu auditującego mogą także należeć auditorzy szkolący się, a także, gdy jest to wymagane, **eksperci techniczni** (3.9.12).

UWAGA_3: Obserwatorzy mogą towarzyszyć zespołowi auditującemu, ale nie mogą działać jako część zespołu.

3.9.11
ekspert techniczny
(audit) osoba, która dysponuje określoną wiedzą lub jest specjalistą w odniesieniu do przedmiotu podlegającemu auditowaniu.

UWAGA_1: określona wiedza lub opinia zawierającą określoną wiedzę wydana w odniesieniu do **organizacji** (3.3.1), **procesu** (3.4.1) lub działania, podlegających auditowaniu traktowana jest na równi z poradnictwem językowym lub kulturowym.

UWAGA_2: ekspert techniczny nie występuje jako **auditor** (3.9.9) w **zespole auditującym** (3.9.10).

Próbując wyjaśnić znaczenie jakiegoś terminu, warto również sprawdzić, czy nie został on zapisany w stosownych normach terminologicznych. Dla rozważanego zakresu przedmiotowego odpowiednia jest norma [14], w której można znaleźć następujące definicje[14]:

3.1.007
audyt zabezpieczenia systemu
dokonanie niezależnego przeglądu i oceny (3.1.044) działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się, czy system działa zgodnie z ustaloną polityką zabezpieczenia (3.1.068) i procedurami operacyjnymi oraz w celu wykrycia przełamań zabezpieczenia (3.1.080) i zalecenia wskazanych zmian w środkach nadzorowania, polityce zabezpieczenia oraz procedurach
audit

3.9.013
audyt zabezpieczenia
przeprowadzenie niezależnego przeglądu i oceny (3.1.044), tj. zapisów i działalności systemu informatycznego w celu przetestowania adekwatności

[14] Zdaniem piszącego te słowa, norma ta wprowadza również sporo zamieszania, bo szereg podanych tam definicji kłóci się nie tylko z tzw. „dobrą praktyką inżynierską" ale również ze zdrowym rozsądkiem. Niestety, w takiej postaci norma została „do wierzenia podana", i jako takiej wypada chyba się jej trzymać, bo w końcu lepsza taka, niż żadna.

środków nadzoru systemu, upewnienia się o zgodności (3.9.130) z ustaloną polityką zabezpieczenia (3.1.068) i procedurami eksploatacyjnymi, wykrycia przełamań zabezpieczenia (3.1.080) oraz wskazanie zmian dotyczących środków nadzoru, polityki zabezpieczenia i procedur eksploatacyjnych
security audit

3.9.014
audyt zabezpieczenia wewnętrzny
audyt zabezpieczenia systemu (3.1.007) przeprowadzony przez personel odpowiedzialny za zarządzanie w organizacji dokonującej przeglądu
internal security audit

3.9.015
audyt zabezpieczenia zewnętrzny
przegląd zabezpieczenia (3.1.104) przeprowadzany przez organizację niezależną od podlegającej przeglądowi
external security audit

Z przytoczonych definicji wynika, że audyt jest:

1) oficjalnym sprawdzeniem, czy wszystko jest w porządku [22],
2) niezależnym przeglądem i oceną „czegoś" w systemie teleinformatycznym [11], [14].

W celu uniknięcia nieporozumień warto przyjąć, że:

audytem *jest nazywane postępowanie dla oceny zgodności audytowanego obiektu z wzorcem (normą, wzorcem proceduralnym lub arbitralnie ustanowionym wektorem wartości pewnych cech) prowadzone przez stronę niezależną (firmę, osobę lub zespół).*

W przypadku audytu z zakresu bezpieczeństwa teleinformatycznego, ta niezależność powinna być zachowana w stosunku do:

1) organizacji/zespołu budującego system zabezpieczeń;
2) dostawców sprzętu i oprogramowania;
3) organizacji podlegającej przeglądowi w takim sensie, że w skład zespołu audytowego nie mogą wchodzić pracownicy organizacji zlecającej audyt.

Jeżeli nie jest dotrzymany któryś z ww. punktów, to można mówić co najwyżej o *„przeglądzie zabezpieczeń według listy audytowej ..."*, a nie o audycie.

W praktyce audyt dla celów bezpieczeństwa teleinformatycznego przeprowadza się z jednego z następujących powodów:

1) żeby wykazać, że informacja i system teleinformatyczny został zabezpieczony zgodnie z ustaleniami pomiędzy zleceniodawcą a zespołem budującym system bezpieczeństwa;
2) żeby wykazać, że system bezpieczeństwa spełnia wymagania norm i standardów w tym zakresie, np. ISO/IEC-15408;
3) żeby wystawić ocenianemu systemowi tzw. *certyfikat bezpieczeństwa*, co w związku z wejściem Polski do NATO (i obowiązującej ustawie „*o ochronie informacji niejawnych"*) oraz dążeniem do wejścia do Unii Europejskiej jest coraz częstsze;
4) żeby ocenić jakość systemu bezpieczeństwa i przedstawić ocenę zleceniodawcy do decyzji (modernizujemy/zostawiamy jak jest).

Z przytoczonych uwag wynika, że:

1) audytem nie jest sprawdzanie zapisów w dziennikach systemowych i zabezpieczeń systemu teleinformatycznego (tzw. inspekcja logów) w celu wykrycia ewentualnych włamań, chociaż takie sprawdzanie może być elementem procesu audytu;
2) audytem nie jest sprawdzanie konfiguracji stacji roboczych, serwerów i urządzeń sieciowych, chociaż takie sprawdzanie może być elementem procesu audytu;
3) w szczególności audytem, ani elementami audytu, nie są czynności wymienione w punktach 1 i 2, jeżeli są przeprowadzane przez administratorów konkretnych systemów w ramach ich bieżących bądź zleconych zadań.

W tym miejscu, niestety, trzeba poddać krytyce zawartość polskiej normy terminologicznej [14]. Nie można się zgodzić, że audyt obejmuje również „*wykrycie przełamań zabezpieczenia*" oraz „*wskazanie zmian dotyczących środków...*", ponieważ:

1) Jeżeli wykrycie przełamań, to za jaki okres? Roku? Miesiąca? A co w przypadku, gdy sprawdzany system nie daje możliwości takiego wykrycia (np. nie archiwizuje się zawartości dzienników)?
2) W praktyce audyt nie obejmuje „wskazania zmian dotyczących środków..." (bo to jest zwykle objęte oddzielnym kontraktem), ale wskazanie, gdzie w systemie są podatności, które mogą być wykorzystane przez zagrożenia. Niezależny zespół audytorów nie powinien się wikłać w poprawianie systemu zabezpieczeń, bo staje się jego współkonstruktorem i tym samym przestaje być niezależny.

Niejasności dotyczące audytu pogłębia fakt, że w organizacjach związanych z szeroko rozumianym audytem wyróżniane są następujące typy audytów[15]:

1) **Finansowy** – jest to analiza działalności organizacji dotycząca wyników finansowych i zagadnień księgowych. Polega na niezależnej i obiektywnej weryfikacji i wyrażeniu opinii o prawidłowości i rzetelności sprawozdania finansowego. Audyt ten jest wykonywany przez biegłego rewidenta na podstawie „Ustawy o biegłych rewidentach" oraz zgodnie z „Normami wykonywania zawodu".
2) **Zgodności** – jest to analiza kontroli finansowych i operacyjnych oraz transakcji pod kątem ich zgodności z przepisami, planami, procedurami i standardami.
3) **Operacyjny** – jest to analiza wszystkich lub wybranych funkcji organizacji (np. wsparcia informatycznego w podejmowaniu decyzji przez kierownictwo) pod kątem wydajności, ekonomiczności oraz efektywności z jaką są te funkcje realizowane w celu osiągnięcia celów biznesowych organizacji.

W ramach trzeciego z typów – audytu operacyjnego – szczególną uwagę zwraca się zwykle na **audyt informatyczny** (w sensie: audyt wykorzystywanych w procesach biznesowych organizacji systemów informatycznych oraz projektów takich systemów). Cele wykonywania audytu informatycznego to przede wszystkim:

1) Weryfikacja zgodności działania systemów informatycznych z wymogami prawa (ustawa o rachunkowości, o ochronie danych osobowych itp. – por. rozdz.2).
2) Weryfikacja stanu bezpieczeństwa systemów informatycznych oraz, w razie potrzeby, pojedynczych aplikacji z perspektywy występującego ryzyka[16] oraz zaimplementowanych procedur kontrolnych i ich efektywności.
3) Analiza ryzyka związanego z prowadzeniem projektu informatycznego.

Jednym ze standardów dających pogląd na to, czego dotyczy audyt informatyczny, jest wspomniany w rozdz.3.1 standard COBIT. W tabeli 1.1 są zebrane procesy biznesowe organizacji podlegające audytowi informatycznemu, kryteria oceny tych procesów oraz zasoby teleinformatyczne związane z tymi procesami. Jeżeli audyt będzie dotyczył wszystkich 34 procesów wymienionych w tabeli, ocenianych zarówno przez pryzmat pierwszo-, jak i drugorzędnych kryteriów, będzie to **pełny audyt informatyczny**. Jeżeli procesy będą oceniane

[15] Według klasyfikacji IIA (Institute of Internal Auditors – Instytut Audytorów Wewnętrznych)

[16] Należy zauważyć, że termin „ryzyko" oraz „analiza ryzyka" jest często bardzo swobodnie interpretowany, co również może prowadzić do nieporozumień.

tylko według wybranych kryteriów, np. poufności, integralności i dostępności, to będzie to wycinkowy audyt informatyczny, który w tym przypadku można określić mianem **audytu bezpieczeństwa teleinformatycznego**.

W tabeli 1.1 taki audyt bezpieczeństwa teleinformatycznego, ograniczony tylko do procesów ocenianych według kryteriów pierwszorzędnych tzn. do tych wierszy, na przecięciu których z kolumną „3", „4", „5" (kryteria) znajduje się literka „P", jest wyodrębniony poprzez zacieniowanie. Pojawia się tutaj pierwsza z odpowiedzi na pytanie postawione w tytule: *audyt bezpieczeństwa teleinformatycznego jest częścią audytu informatycznego*.

W praktyce brak jest jednak zaleceń co do sposobu prowadzenia audytu w zakresie bezpieczeństwa teleinformatycznego. Szereg organizacji, takich jak ISACA czy British Standards Institution (opublikowany standard BS 7799), szkoli audytorów i przeprowadza, na zlecenie, audyty na zgodność z opublikowanymi przez te organizacje standardami z zakresu zarządzania bezpieczeństwem teleinformatycznym. Szczegółowa metodyka przeprowadzania takich audytów nie została jednak nigdzie opublikowana, a przynajmniej piszącemu te słowa takie publikacje, poza uzupełnieniami normy ISO/IEC 15408, nie są znane. Wydawane przez ISACA standardy można co najwyżej uznać za zbiór pytań, na które audytor powinien znaleźć odpowiedzi, a nie za metodykę. Różne kraje opracowały wprawdzie standardy audytu dla instytucji sektora publicznego, np. w Stanach Zjednoczonych przykładem są podręczniki opracowywane przez GAO (*General Accounting Office*) zgodne ze standardami GAGAS (*Generally Accepted Government Auditing Standards*), ale ze względu na odmienne uwarunkowania ekonomiczne i prawne trudno mówić o ich bezpośrednim przeniesieniu na grunt polski.

Poza tym, o ile metodyki przeprowadzania audytów z zakresu norm jakości (rodzina ISO 9000) są znane, dobrze udokumentowane i stosowane w praktyce oraz są szkoleni również w Polsce, przez PCBC[17], dla tych potrzeb audytorzy, o tyle szkoleniem w Polsce[18] audytorów dla potrzeb przeprowadzania audytów z zakresu bezpieczeństwa teleinformatycznego nikt się nie zajmuje.

Często firmy podejmujące się wykonania „audytu bezpieczeństwa" wykonują działania wynikające z chwilowego stanu wiedzy zespołu „audytorów" zebranego *ad hoc*, dla potrzeb konkretnej umowy. Wynikiem takiego stanu rzeczy, przynajmniej na gruncie polskim, jest brak rozeznania kadry menedżerskiej firm i instytucji, czym jest audyt z zakresu bezpieczeństwa teleinformatycznego i czego można po nim oczekiwać (jakich dokumentów wynikowych, jakie działania mogą zostać przeprowadzone na terenie instytucji zleceniodawcy przez audytorów, jakiego dodatkowego zaangażowania w prace

[17] Polskie Centrum Badań i Certyfikacji.
[18] Stan na rok 2003.

audytowe swoich pracowników może spodziewać się zleceniodawca itd.). Nieprawidłowości, wynikające z braku wiedzy (tym razem także zleceniodawcy) na temat audytu z zakresu bezpieczeństwa teleinformatycznego, pojawiają się zresztą już podczas formułowania zapytania ofertowego oraz konstrukcji umowy, gdzie często pod przykrywką „audytu" wymaga się od zleceniobiorcy wykonania czynności związanych z budową systemu bezpieczeństwa.

Na podstawie praktycznych doświadczeń i wypracowanych metod działania zespołu, którego członkiem jest także piszący te słowa, można stwierdzić, że na proces audytu w zakresie bezpieczeństwa teleinformatycznego składają się następujące, podstawowe czynności:

1) Sporządzenie listy audytowej (*checklist*) według wybranego standardu. Dla standardu BS 7799 będzie to lista 127 punktów „do odhaczenia", dla COBIT™, przy pełnym audycie informatycznym, 302 punkty, dla TCSEC 134 punktów itd. Zalecenia poszczególnych punktów audytowych (w miarę potrzeb opatrzone komentarzami) są kwalifikowane do jednej z poniższych klas:
   - *„spełnione"*
   - *„nie spełnione"*
   - *„spełnione częściowo"*
   - *„nie dotyczy".*

2) Wypełnienie listy audytowej z punktu 1 na podstawie ankietowania, wywiadów, wizji lokalnych, kontroli i analizy dokumentów firmy oraz wykonanych testów i badań (por. punkt 3).

3) Badania systemów ochrony fizycznej i technicznej oraz sieci i systemów teleinformatycznych eksploatowanych w audytowanym obiekcie. Badania te są przeprowadzane przy użyciu wyspecjalizowanych narzędzi i są uzupełniane testami penetracyjnymi, głównie heurystycznymi, przy czym należy pamiętać, że testy penetracyjne same w sobie nie są audytem, jak to się zwykło uważać. Testy penetracyjne (tzw. kontrolowane włamania) są prowadzone w celu określenia podatności badanego systemu teleinformatycznego na ataki wewnętrzne i zewnętrzne i obejmują zwykle następujące, kontrolowane czynności:
   - Identyfikowanie systemu (rodzaju i wersji systemu operacyjnego, użytkowanego oprogramowania, użytkowników itd.).
   - Skanowania:
     - przestrzeni adresowej
     - sieci telefonicznej firmy
     - portów serwerów i urządzeń sieciowych firmy.

- Włamania.
- Podsłuch sieciowy (ang. *sniffing*).
- Badanie odporności systemu na ataki typu *„odmowa usługi”* (ze względu na potencjalne możliwości wyrządzenia szkód w poddanej badaniom organizacji wyłącznie na specjalne życzenie zleceniodawcy, po szczegółowym spisaniu i zatwierdzeniu zakresu tej części testu penetracyjnego).

4) Sporządzenie dokumentacji z audytu (raportu), obejmującej udokumentowane przedsięwzięcia, wyniki i wnioski dla punktów 2 i 3. Dokumentacja końcowa musi być podpisana przez audytorów, imiennie gwarantujących rzetelność przeprowadzonej oceny.

Pełny opis przedstawionej tutaj w zarysie metodyki można znaleźć w [1] i [4]. Przedstawiona tam w postaci dokumentu metodyka LP–A jest wykorzystywana przez jej autorów w praktyce. Warto zauważyć, że wymienione przedsięwzięcia w pełni wpisują się w schemat pięciu etapów audytu zaproponowanych w COBIT, do których należą:

1. **Zapoznanie się z procesem**. Cel: uzyskanie wiedzy na temat zaprojektowanych mechanizmów kontrolnych
2. **Ocena mechanizmów kontrolnych**. Cel: wypracowanie oceny rzetelności i efektywności zidentyfikowanego systemu kontrolnego.
3. **Ocena zgodności**. Cel: zidentyfikowanie stopnia wdrożenia mechanizmów kontrolnych.
4. **Ocena ryzyka**. Cel: uzyskanie dowodów, że podatności i braki (błędy struktury i realizacji) w systemie kontrolnym mogą prowadzić do strat (nieosiągania celów biznesowych).
5. **Określenie osiągania celów**. Cel: opracowanie raportu z audytu z oceną osiągnięcia każdego z celów kontroli.

W ramach audytu bezpieczeństwa teleinformatycznego nie ocenia się czynników ekonomicznych, na przykład tego, czy outsourcing usług informatycznych:

- prowadzi do obniżenia kosztów „informatyki”;
- daje usługi o lepszej jakości,
- daje dostęp do nowych technologii,
- daje dostęp do wiedzy i umiejętności specjalistów strony świadczącej usługi outsourcingowe.

Natomiast sprawdza się, czy usługi outsourcingowe nie prowadzą do naruszenia

poufności, integralności lub dostępności informacji, których właścicielem[19] jest badana organizacja, tj. do pogorszenia poziomu bezpieczeństwa teleinformatycznego.

Można zatem sformułować drugą odpowiedź na pytanie zawarte w tytule: *audyt z zakresu bezpieczeństwa teleinformatycznego nie dotyczy strony ekonomicznej stosowania środków informatyki w procesach biznesowych*.

Zgodnie z definicją bezpieczeństwa teleinformatycznego podaną w rozdziale 2 oraz przedstawionym w tym rozdziale schematem prowadzenia audytu z tego zakresu należy stwierdzić, że audyt taki *nie dotyczy ryzyka związanego z prowadzeniem przez audytowaną organizację projektów z dziedziny informatyki* (chodzi tutaj oczywiście o ryzyko związane z niepowodzeniem projektu, tj. ryzyko projektowe dotyczące utrzymania w założonym limicie kosztów oraz czasu wykonania projektu i spełnienia przez otrzymany produkt wymagań funkcjonalnych i operacyjnych zleceniodawcy). Ocena taka natomiast, jak już wcześniej wspomniano, jest zwykle częścią audytu informatycznego.

W odróżnieniu od klasycznego (np. w ujęciu COBIT) audytu informatycznego, audyt bezpieczeństwa teleinformatycznego nie obejmuje zwykle szczegółowego badania aplikacji (w sensie badania kodu i spełnienia wymagań funkcjonalnych i operacyjnych – chyba, że jest to wyraźnie zaznaczone w umowie). Badany jest natomiast stopień zaaplikowania łat i uaktualnień likwidujących znane podatności.

Część firm, jak wynika chociażby z przeglądu informacji wystawionych przez nie w witrynach internetowych, pod nazwą „audytu informatycznego" lub jako element „audytu bezpieczeństwa" oferuje wykonanie spisu inwentaryzacyjnego zasobów informatycznych klienta. Przy tej okazji reklamują się wykonaniem takiego spisu w sposób „lekki, łatwy i przyjemny", poprzez wykorzystaniu specjalnego oprogramowania do inwentaryzacji, tzw. skanerów inwentaryzacyjnych (zwykle są podawane nazwy takie jak GASP, KeyAudit, Languard Network Security Scanner i inne). Należy tutaj podkreślić, że tak przeprowadzona inwentaryzacja może być co najwyżej wstępem do przeprowadzenia rzetelnej inwentaryzacji zasobów teleinformatycznych. Uzasadnieniem takiego stwierdzenia może być chociażby fakt, że np. w standardzie BS 7799 zasoby teleinformatyczne są definiowane bardzo szeroko i obejmują nie tylko komputery (w sensie stacji roboczych), urządzenia sieciowe i oprogramowanie, ale także dokumentację systemową, zasoby informacyjne firmy oraz urządzenia infrastruktury informatycznej, takie jak gniazda sieciowe,

[19] Lub za które odpowiada.

tablice krosowe, urządzenia klimatyzacyjne, zasilające itd.[20] A tego już żadne oprogramowanie inwentaryzacyjne automatycznie nie zarejestruje. Poza tym rzetelny spis inwentaryzacyjny zasobów teleinformatycznych musi zawierać także lokalizację zasobu oraz wskazanie jego właściciela-administratora (pracownika, którego obarczono odpowiedzialnością za zasób i uprawniono do manipulacji nim).

Należy zauważyć, że audyt to sprawdzenie i ocena, a nie wykonanie czegoś (np. spisu inwentaryzacyjnego). Dlatego nieporozumieniem jest nazywanie „audytem" czynności inwentaryzacyjnych, chociaż w ramach audytu, zarówno informatycznego, jak i bezpieczeństwa teleinformatycznego, będzie sprawdzane posiadanie przez audytowaną organizację rzetelnych spisów inwentaryzacyjnych. Jeżeli audytorzy sami będą takie spisy wykonywali, to oznacza to, że w następnym kroku będą sprawdzali sami siebie, co przeczy podstawowym zasadom wykonywania audytu.

5. Podsumowanie

Podsumowując przedstawione rozważania z zakresu terminologii i praktyki audytu można, odpowiadając na pytanie zawarte w tytule, stwierdzić, co następuje:

1. Audyt bezpieczeństwa teleinformatycznego może występować jako samodzielne przedsięwzięcie lub może być częścią audytu informatycznego.
2. Audyt bezpieczeństwa teleinformatycznego wymaga **specjalistycznej wiedzy**, różnej od wiedzy wymaganej np. przy audycie finansowym.
3. Audyt bezpieczeństwa teleinformatycznego nie dotyczy strony ekonomicznej stosowania środków informatyki w procesach biznesowych (pomimo że procesy biznesowe są uwzględniane przy ocenie ryzyka i podatności systemu). Oceny takie są natomiast zwykle przeprowadzane w ramach audytów informatycznych i operacyjnych.
4. Audyt bezpieczeństwa teleinformatycznego nie dotyczy ryzyka związanego z prowadzeniem przez audytowaną organizację projektów z dziedziny informatyki ani oceny takich projektów. Oceny takie są natomiast zwykle przeprowadzane w ramach audytów informatycznych i operacyjnych.

[20] Jeżeli w pomieszczeniu służbowym będzie stał sejf, w którym będą przechowywane kopie bezpieczeństwa systemu, to sejf ten staje się zasobem teleinformatycznym, tj. zasobem który podlega ochronie. Jeżeli sejf ten służy pracownikowi pracującemu w tym pomieszczeniu tylko do przechowywania drugiego śniadania, to oczywiście sejfu takiego nie uważa się za zasób teleinformatyczny.

5. Audyt bezpieczeństwa teleinformatycznego nie zawiera szczegółowego badania aplikacji (w sensie badania kodu i spełnienia wymagań funkcjonalnych i operacyjnych – chyba że jest to wyraźnie zaznaczone w umowie). Badany jest natomiast stopień zainstalowanych łat i uaktualnień likwidujących znane podatności. Jeżeli organizacja prowadzi własne prace projektowe, to sprawdzeniu podlega także przestrzeganie pewnych reguł: bezpiecznego projektowania i otrzymywania bezpiecznych produktów (np. norma BS 7799 zawiera stosowne pozycje checklisty).
6. Audyt bezpieczeństwa teleinformatycznego nie obejmuje analizy kontroli finansowych i operacyjnych oraz transakcji pod kątem ewentualnych nadużyć i oszustw popełnianych przez uprawnionych użytkowników systemów teleinformatycznych, chociaż procedury nadawania uprawnień i bezpieczeństwo osobowe (razem zawierające zwykle podatności systemu na nadużycia popełniane przez uprawnionych użytkowników) są obiektami badania.
7. Audyt bezpieczeństwa teleinformatycznego nie obejmuje wykonania inwentaryzacji zasobów teleinformatycznych, chociaż może obejmować (i zwykle obejmuje) sprawdzenie rzetelności posiadanych przez audytowaną organizację spisów zasobów teleinformatycznych. To samo stwierdzenie dotyczy także (por. wcześniejszą dyskusję) audytu informatycznego.

Wykraczające poza ramy niniejszego opracowania są pytania o to, jaki jest szczegółowy zakres audytu bezpieczeństwa teleinformatycznego, na ile jego przeprowadzenie może zakłócić normalną pracę organizacji oraz jakiego wsparcia ze strony audytowanej organizacji potrzebują audytorzy.

Pomocna może być w tym przypadku opisana w [1], [4] metodyka LP-A która, zdaniem jej autorów, może wspomóc kadrę kierowniczą firm i instytucji, zainteresowaną oceną stanu bezpieczeństwa teleinformatycznego eksploatowanych systemów i sieci komputerowych, w podejmowaniu trafnych decyzji już na etapie zapytań ofertowych i formułowania umowy. Również zespoły audytorskie stosujące tę metodykę mogą precyzyjniej szacować nakłady ponoszone na przeprowadzenie audytu oraz planować niezbędne przedsięwzięcia. Na przykład: opis metodyki LP–A zawiera wykaz 13 grup dokumentów niezbędnych do przeprowadzenia prac audytowych, wykaz 36 dokumentów wytwarzanych w procesie audytu oraz relacje pomiędzy tymi dokumentami.

Nie bez znaczenia może być też fakt, że w przypadku znajomości metodyki LP–A przez obie zainteresowane strony (zleceniodawcę i zleceniobiorcę), posługują się one jednolicie rozumianą terminologią i posiadają jednolitą podstawę pojęciową do prowadzenia dyskusji i podejmowania konkretnych decyzji.

Dodatkowa konkluzja przedstawionych rozważań jest taka: w informatyce termin „audyt" jest nadużywany. Często w konkretnych umowach z klientem lepiej byłoby używać terminu „ocena". Termin ten jest znacznie pojemniejszy i łączy się dobrze z terminem „wykonanie" (np. spisu inwentaryzacyjnego). Daje również pole do negocjowania z klientem jego rzeczywistych potrzeb. Ale cóż, „audyt" brzmi bardziej ezoterycznie i można pod nim ukryć zarówno własną nieznajomość problemu jak również namówić klienta do wydania większej sumy pieniędzy niż przy „zwykłej" ocenie.

Literatura

[1] Liderman K.: *Podręcznik administratora bezpieczeństwa teleinformatycznego*, MIKOM, Warszawa, 2003.

[2] Liderman K.: *Międzynarodowe kryteria oceny bezpieczeństwa informacji w systemach informatycznych*, Biuletyn IAiR. Nr 11, WAT, Warszawa, 2000.

[3] Liderman K.: *Standardy w ocenie bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, Nr 17, WAT, Warszawa, 2002.

[4] Liderman K., Patkowski A.: *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, Biuletyn IaiR, Nr 18, WAT, Warszawa, 2003.

[5] COBIT™ Control Objectives, April 1998. 2nd Edition, COBIT Steering Committe and the Information Systems Audit and Control Foundation.

[6] COBIT® 3rd Edition. Management Guidelines, July 2000, COBIT Steering Committe and the IT Governance Institute™

[7] BS 7799-1:1999: Part 1: *Code of practice for Information Security Management*, British Standards Institute.

[8] BS 7799-2:1999: Part 2: *Specification for Information Security Management Systems*, British Standards Institute.

[9] ISO/IEC 17799:2000: *Information technology – Code of practice for information security management*.

[10] PN-ISO 9000-3: *Wytyczne do stosowania normy ISO 9001 podczas opracowywania, dostarczania i obsługiwania oprogramowania*, 1994.

[11] PN-EN-ISO 9000:2001: *Systemy zarządzania jakością – Podstawy i terminologia*.

[12] PN-EN-ISO 9001:2001: *Systemy zarządzania jakością – Wymagania*.

[13] PN-EN-ISO 9004:2001: *Systemy zarządzania jakością – Wytyczne doskonalenia funkcjonowania*.

[14] PN-I-02000: *Technika informatyczna – Zabezpieczenia w systemach informatycznych*, 1998.

[15] PN-ISO/IEC 15408-1:2002: *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 1: Wprowadzenie i model ogólny*.

[16] PN-ISO/IEC 15408-3:2002: *Technika informatyczna – Techniki zabezpieczeń – Kryteria oceny zabezpieczeń informatycznych – Część 3: Wymagania uzasadnienia zaufania do zabezpieczeń*.

[17] PN-I-13335-1: 1999. *Technika informatyczna – Wytyczne do zarządzania bezpieczeństwem systemów informatycznych. – Pojęcia i modele bezpieczeństwa systemów informatycznych*.

[18] ISO/IEC TR 13335-3:1997 *Guidelines for the Management of IT Security – Part 3: Techniques for the Management of IT Security*.

[19] Bazylejski Komitet ds. Nadzoru Bankowego: *Zasady zarządzania ryzykiem w bankowości elektronicznej*, Maj 2001.

[20] Rekomendacja D z dn. 20.10.97 dotycząca zarządzania ryzykami towarzyszącymi systemom informatycznym i telekomunikacyjnym używanym przez banki (wraz z pismem przewodnim NB/ZPN/790/97 Generalnego Inspektoratu Nadzoru Bankowego).

[21] Słownik Języka Polskiego, T.1, PWN, Warszawa, 1982.

[22] Oxford Advanced Learner's Dictionary of Current English. A S Hornby. Oxford University Press, 1981.

Recenzent: prof. dr hab. inż. Włodzimierz Kwiatkowski

Praca wpłynęła do redakcji: 11.11.2004