BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 19, 2003

Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego

Krzysztof LIDERMAN, Adam E. PATKOWSKI

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

STRESZCZENIE: W artykule została przedstawiona propozycja metodyki LP–A© przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego. Prezentowana metodyka była stosowana przez autorów w praktyce.

1. Wprowadzenie

W artykule jest zamieszczony opis metodyki LP–A© przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego. Proponowana metodyka została przedstawiona w postaci dokumentu (załącznik). Inspiracją do spisania tej metodyki był fakt, że w praktyce brak jest zaleceń co do sposobu prowadzenia audytu w tym konkretnym zakresie tematycznym, pomimo że sam termin „audyt" jest powszechnie znany i często (również nieprawidłowo) używany.

Szereg organizacji takich jak ISACA (*Information Systems Audit and Control Association* – opublikowany standard COBIT™) 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 autorom niniejszego artykułu takie publikacje, oprócz uzupełnienia standardu Common Criteria w postaci *„Common Methodology for Information Technology Security Evaluation"*

CEM-99/008, nie są znane). Poza tym, o ile metodyki przeprowadzania audytów z zakresu norm jakości (rodzina ISO 9000) są znane, dobrze udokumentowane i stosowane w praktyce oraz szkoleni są także w Polsce (przez PCBC[1]) audytorzy, o tyle szkoleniem audytorów dla potrzeb przeprowadzania audytów z zakresu bezpieczeństwa teleinformatycznego w Polsce nikt się nie zajmuje.

Często firmy podejmujące się wykonania „audytu bezpieczeństwa" (cokolwiek miałoby to znaczyć), 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 audytowe swoich pracowników może spodziewać się zleceniodawca etc.). 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.

Konsekwencji opisanej sytuacji autorzy niniejszego artykułu doświadczają od wielu lat w praktyce, podczas prowadzenia prac związanych przede wszystkim z oceną stanu bezpieczeństwa teleinformatycznego w firmach i instytucjach sektora zarówno prywatnego, jak i państwowego.

Z podanych przyczyn autorzy niniejszej metodyki mają nadzieję, że będzie ona przydatna nie tylko zespołom zajmującym się oceną stanu bezpieczeństwa teleinformatycznego, ale również szerokiej kadrze kierowniczej firm i instytucji, i że przyczyni się do uporządkowania panującego w tej dziedzinie chaosu pojęciowego. Metodyka została przedstawiona w formie dokumentu-załącznika, który może być bezpośrednio wykorzystany w praktyce.

W niniejszym tekście, dla uproszczenia opisu, przyjęto, że instytucja audytowana i zlecająca audyt są tożsame i nazywane są zleceniodawcą.

[1] Polskie Centrum Badań i Certyfikacji

ZAŁĄCZNIK

Metodyka LP–A© przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego

Spis treści

Wykaz używanych terminów i symboli graficznych

TERMINY

audyt – 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.

audytor – członek zespołu audytowego przeprowadzający badania i analizy.

audytor kwalifikujący – członek zespołu audytowego uprawniony do formułowania ocen uogólniających z badań przeprowadzonych przez zespół audytowy; w szczególności uprawniony do ferowania ostatecznych sądów audytowych o zgodności rozpoznanego stanu rzeczy z generalnym wzorcem audytowym.

bezpieczeństwo – stopień racjonalnie uzasadnionego (np. analizą ryzyka) zaufania, że potencjalne straty nie zostaną poniesione. (pot.) – niepodleganie obawie; spokój; pewność, że się nic złego nie stanie.

bezpieczeństwo teleinformatyczne – stopień uzasadnionego zaufania (por. np. ISO/IEC 15408) 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.

informacja wrażliwa – dla określonego podmiotu są to wszelkie informacje, które mogą zostać wykorzystane przeciwko temu podmiotowi poprzez ujawnienie, uniedostępnienie oraz zmanipulowanie jawne lub skryte. W szczególności, są to wszystkie informacje, które muszą być chronione, bo tak nakazują obowiązujące przepisy prawne (np. ustawa „*o ochronie danych osobowych”*) oraz takie informacje, których nakaz ochrony nie jest zawarty w żadnych regulacjach prawnych, a które dla konkretnych organizacji je wytwarzających i przetwarzających, są wskazywane przez kompetentne organy, np. Agencję Bezpieczeństwa Wewnętrznego, wewnętrzne komórki

bezpieczeństwa w danej organizacji, pełnomocnika ds. bezpieczeństwa informacji itp.

metodyka sposób postępowania, stosowany świadomie, konsekwentnie i systematycznie; zespół czynności i środków użytych do osiągnięcia celu; sposób wykonania zadania, rozwiązania problemu; zespół założeń ogólnych, przyjętych w określonych badaniach. („*Słownik wyrazów obcych i zwrotów obcojęzycznych Władysława Kopalińskiego*")[2]

podatność (ang. *vulnerability*) – wady lub luki struktury fizycznej, organizacji, procedur, personelu, zarządzania, administrowania, sprzętu lub oprogramowania, które mogą być wykorzystane do spowodowania szkód w systemie informatycznym lub działalności użytkownika.

UWAGI
1 – Istnienie podatności nie powoduje szkód samo z siebie. Podatność jest jedynie warunkiem lub zestawem warunków, które umożliwiają uszkodzenie systemu lub zakłócenie działalności użytkownika przez atak
2 – jeśli podatność odpowiada zagrożeniu, istnieje ryzyko.
(*punkt 3.1.064 w PN-I-02000:1998*)

środki bezpieczeństwa – środki fizyczne (np. płot), techniczne (np. system alarmowy), ludzkie (np. wartownik), programowe (np. oprogramowanie antywirusowe) lub działania organizacyjne (np. szkolenia), stosowane w celu przeciwdziałania wykorzystaniu podatności przez zagrożenia. Często, w skrócie, środki bezpieczeństwa są nazywane **zabezpieczeniami.**

zagrożenie (ang. *threat*) – potencjalne naruszenie zabezpieczeń systemu informatycznego (*punkt 3.1.115 w PN-I-02000:1998*)

zasoby teleinformatyczne – wszelkie zasoby fizyczne (np. sejf), techniczne (np. urządzenia klimatyzacyjne, komputery), informacyjne w różnej postaci (np. papierowa dokumentacja techniczna sieci, zawartość elektronicznych baz danych), do których nieupoważniony dostęp lub zniszczenie może być przyczyną utraty poufności, integralności lub dostępności informacji przetwarzanych, przechowywanych i przesyłanych w systemach i sieciach teleinformatycznych.

UWAGA

W polskiej wersji normy ISO/IEC 17799 termin „zasoby" jest zastąpiony terminem „aktywa".

[2] Ten termin często jest błędnie zastępowany słowem „metodologia" (naiwne przeniesienie znaczenia angielskiego, podobnego brzmieniem, słowa); por. tamże: „**metodologia** znawstwo hist., analityczne, krytyczne i normatywne metod badań nauk., budowy systemów nauk., wyrażania i utrwalania osiągnięć nauki."

SYMBOLE GRAFICZNE

symbol **procesu** na DFD (*Data Flow Diagram*)

symbol **terminatora**, tj. elementu zewnętrznego w stosunku do procesów opisywanych za pomocą DFD.

symbol **magazynu**, tj. elementu mogącego gromadzić dane (dokumenty lub inne, zależne od modelowanego kontekstu, elementy)

symbol **przepływu** danych (dokumentów, informacji itd.) pomiędzy elementami DFD

UWAGA!
Symbole graficzne procesów i magazynów rysowane na diagramach DFD linią przerywaną oznaczają procesy i magazyny powielone, tzn. są to te same procesy i magazyny, co narysowane linią ciągłą, tylko umieszczone jeszcze raz na diagramie w celu uzyskania lepszej przejrzystości (zwykle, gdy prowadzenie przepływów od oryginałów powodowałoby plątaninę nieczytelnych strzałek na rysunku).

Wstęp

Niniejszy dokument opisuje metodykę LP-A© wykonywania audytu z zakresu bezpieczeństwa teleinformatycznego. Metodyka dotyczy przeprowadzania audytu systemów i sieci teleinformatycznych (biurowych, bazodanowych, etc.), gdzie przedmiotem chronionym jest informacja. Metodyki tej nie stosuje się przy przeprowadzaniu audytów z zakresu szeroko rozumianego bezpieczeństwa systemów i sieci sterowania (przemysłowych, do których ma zastosowanie norma IEC 61508), gdzie przedmiotem chronionym przed skutkami niepoprawnego działania tych systemów jest ich środowisko.

Na przedstawioną dalej metodykę składają się:

1) organizacja, zakresy kompetencji i kwalifikacje zespołu audytowego (rozdz.1),
2) wyposażenie narzędziowe zespołu audytowego (rozdz.2)
3) dokumenty niezbędne do zainicjowania audytu oraz wytwarzane podczas audytu (rozdz.4),
4) model w postaci diagramów DFD opisujący procesy wytwarzania dokumentów i powiązania pomiędzy nimi (rozdz.3 i 5),
5) wykaz tzw. „rzetelnych praktyk", tj. heurystycznych sposobów postępowania, wypracowanych i sprawdzonych podczas dotychczasowej praktyki audytorskiej twórców metodyki (rozdz.6).

Do przedstawienia procesów i przepływu dokumentów podczas audytu zostały wykorzystane elementy metody strukturalnej projektowania systemów informatycznych. Elementy te to przede wszystkim tabele IPO (ang. *Input–Process–Output*), diagramy przepływu danych (DFD – ang. *Data Flow Diagram*) oraz stosowane na nich oznaczenia procesów, przepływów i magazynów (por. *„Wykaz używanych terminów i symboli graficznych"* na początku niniejszego dokumentu).

Zgodnie z przedstawioną na początku niniejszej publikacji definicją, audyt to postępowanie dla oceny zgodności audytowanego obiektu z wzorcem. Dla potrzeb niniejszej metodyki przyjęto, że wzorzec ten stanowi norma ISO/IEC 17799. Założenie takie wynika z doświadczeń zawodowych twórców niniejszej metodyki – obecnie właściwie wszystkie zamówienia na prace z zakresu bezpieczeństwa teleinformatycznego odwołują się do tej normy i nie należy raczej oczekiwać zmiany w tym zakresie, szczególnie w okresie wchodzenia Polski do Unii Europejskiej. Pogląd ten znajduje wsparcie chociażby w zaleceniu Unii Europejskiej z dn. 28.02.2002 „…*on a common*

approach and specific actions in the area of network and information security" (2002/C 43/02) wskazującym na konkretne standardy z zakresu bezpieczeństwa teleinformatycznego: ISO/IEC 15408 w zakresie certyfikacji oraz ISO/IEC 17799 w zakresie tzw. „rzetelnych praktyk". Niemniej nic nie stoi na przeszkodzie, aby zamiast normy ISO/IEC 17799 w tabelach IPO wpisać inną normę lub standard, oczywiście pod warunkiem posiadania dla niego odpowiednio przygotowanych narzędzi, w zakresie materialnym głównie tzw. kwestionariuszy audytowych.

Należy podkreślić, że audyt z zakresu bezpieczeństwa teleinformatycznego zgodny z prezentowaną metodyką nie polega wyłącznie na udokumentowaniu na podstawie analizy dokumentacji, wywiadów i wizji lokalnych stopnia przystawania sposobu zarządzania bezpieczeństwem teleinformatycznym w audytowanym obiekcie (np. instytucji) do wzorca. Dokumentowanie takie następuje w trakcie realizacji czynności tzw. *ścieżki formalnej* (por. rozdz.3**)**. Porównywanie z zaleceniami prowadzone jest jednak z pewnym naruszeniem równorzędności poszczególnych sprawdzeń: niektóre z nich, uznane za szczególnie ważne, sprawdzane są znacznie dokładniej niż pozostałe. O ile normalne postępowanie to sprawdzanie, w szczególnych przypadkach wykonywane działania zasługują już na miano badań. Do tej kategorii zaliczono badania skuteczności zabezpieczeń technicznych i informatycznych oraz analizę systemową zabezpieczeń. **Cechą charakterystyczną metodyki LP–A© jest realizacja** w ramach tzw. *ścieżki technicznej* (por. rozdz.3) **badań** 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.

Efektem przyjęcia takiego schematu postępowania jest:

1) możliwość wykrycia szczególnie groźnych podatności i przekazanie zleceniodawcy przez audytorów wykazu podatności „do natychmiastowego usunięcia" (odrębną kwestią pozostaje, kto ma usuwać zidentyfikowane podatności – ze względów formalnych nie powinien tego robić zespół audytowy);
2) uzupełnienie i polepszenie wnikliwości i jakości ocen generowanych w ramach ścieżki formalnej;
3) przekazanie zleceniodawcy pełnego obrazu (zarówno technicznego jak i organizacyjnego) stanu zabezpieczeń jego sieci i systemów, co zwykle stanowi podstawę do dalszych działań zleceniodawcy w zakresie bezpieczeństwa teleinformatycznego.

Na podstawie informacji zamieszczonych w niniejszym opisie metodyki można:

1) ocenić złożoność procesów składających się na audyt;
2) prześledzić zależności pomiędzy dokumentami wytwarzanymi w procesie audytu;
3) dobrać skład Zespołu Audytowego, uwzględniając wymagane zakresy kompetencji (kwalifikacji i uprawnień) członków Zespołu;
4) ocenić na podstawie zależności pomiędzy procesami (oraz składu osobowego Zespołu) możliwości równoległego prowadzenia zadań audytowych;
5) skonstruować harmonogram realizacji audytu (po uwzględnieniu konkretnych warunków wynikających z umowy z zleceniodawcą);
6) oszacować koszty przeprowadzenia audytu (także z uwzględnieniem warunków umowy).

W rozdziale 6 zostały przedstawione tzw. „rzetelne praktyki" (nazywane też „najlepszymi praktykami" – z ang. *best practices*), tj. należące do kategorii know–how metody postępowania, wypracowane i sprawdzone podczas dotychczasowej praktyki audytorskiej twórców metodyki. Chociaż praktyki takie zostały wymienione wcześniej jako element metodyki, to należy zauważyć, że są one ściśle związane z konkretnym zespołem ludzi (ich kwalifikacjami, doświadczeniem, etyką itd.). Z tego względu zawartość rozdziału 6 należy traktować raczej jako wskazówkę niż „twarde" zalecenie – każdy zespół audytorski prawdopodobnie wypracuje sobie własny zestaw „rzetelnych praktyk". Autorzy prezentowanej metodyki mają jednak nadzieję, że zamieszczony w rozdz. 6 zestaw zostanie dobrze oceniony i włączony do repertuaru działań innych zespołów audytorskich.

Rozdział 1. Skład zespołu audytowego, kwalifikacje jego członków i zakresy kompetencji

Jednym z kluczowych elementów decydujących o rzetelności przeprowadzonego audytu są kwalifikacje i sposób pracy członków zespołu audytowego. W tym rozdziale są przedstawione informacje nt. składu i kwalifikacji zespołu. Sposób pracy, wynikający z praktycznie wdrożonej i sprawdzonej metodyki jest opisany w rozdz. 3.

Zespół audytowy składa się z dwóch części:

- składu stałego
- składu zmiennego („na telefon")

I. Skład stały zespołu

1. Audytorzy kwalifikujący – dwie osoby (symbole: AK_1 i AK_2)

Wymagania:

a) wykształcenie wyższe techniczne,
b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych, w szczególności w zakresie bezpieczeństwa teleinformatycznego,
c) co najmniej kilkuletnia praktyka w przeprowadzaniu audytów z zakresu bezpieczeństwa teleinformatycznego,
d) doświadczenie dydaktyczne oraz umiejętność prowadzenia negocjacji,
e) dopuszczenia do dostępu do informacji niejawnych (w rozumieniu ustawy „*o ochronie informacji niejawnych*").

Do podstawowych zadań audytorów kwalifikujących należy:

- wykonanie przedsięwzięć z etapu przygotowawczego audytu (por. rozdz. 3),
- we współdziałaniu ze specjalistami wymienionymi w punktach 2 i 3 niniejszego rozdziału, wykonanie przedsięwzięć ścieżki formalnej z etapu wykonawczego audytu,
- nadzór nad wykonywaniem przedsięwzięć ścieżki technicznej,
- opracowanie raportu końcowego z analiz technicznych,
- przekazanie stronie zleceniodawcy wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia",
- opracowanie dokumentu końcowego z audytu bezpieczeństwa teleinformatycznego w instytucji zleceniodawcy.

Audytorzy kwalifikujący podpisują się pod dokumentami poaudytowymi jako gwaranci rzetelności zawartych w nich informacji.

2. Specjalista od ochrony fizycznej i technicznej (symbol: SF–T)

Wymagania:

a) wykształcenie wyższe,

b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych, w szczególności w zakresie bezpieczeństwa teleinformatycznego,

c) praktyka w przeprowadzaniu audytów z zakresu bezpieczeństwa teleinformatycznego,

d) licencja pracownika zabezpieczenia technicznego II stopnia,

e) dopuszczenia do dostępu do informacji niejawnych (w rozumieniu ustawy „*o ochronie informacji niejawnych*").

Do zadań specjalisty od ochrony fizycznej i technicznej należy:

- współdziałanie z audytorami kwalifikującymi w wykonaniu przedsięwzięć ścieżki formalnej z etapu wykonawczego audytu,
- realizacja punktów 4.2.1 i 4.2.2 (por. rozdz.3) ścieżki technicznej z etapu wykonawczego audytu,
- opracowanie raportu z analizy systemów ochrony fizycznej i technicznej.

3. Specjalista od ochrony antypodsłuchowej i promieniowania ujawniającego (symbol: SA–PU)

Wymagania:

a) wykształcenie wyższe techniczne,

b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych oraz w zakresie instalacji i wykrywania urządzeń techniki specjalnej,

c) praktyka w przeprowadzaniu audytów z zakresu bezpieczeństwa teleinformatycznego,

d) dopuszczenia do dostępu do informacji niejawnych (w rozumieniu ustawy „*o ochronie informacji niejawnych*").

Do podstawowych zadań specjalisty od ochrony antypodsłuchowej i promieniowania ujawniającego należy:

- współdziałanie z audytorami kwalifikującymi (por. rozdz. 3) w wykonaniu przedsięwzięć ścieżki formalnej z etapu wykonawczego audytu,
- realizacja punktów 4.2.3 i 4.2.4 (por. rozdz.3) ścieżki technicznej z etapu wykonawczego audytu,
- opracowanie raportu z analizy technicznej.

4. **Specjalista od urządzeń sieciowych i sieci komputerowych** (symbol: SUS–SK)

Wymagania:

a) wykształcenie wyższe techniczne,
b) co najmniej kilkuletnie doświadczenie zawodowe w dziedzinie systemów komputerowych oraz w zakresie organizacji i obsługi sieci oraz budowy urządzeń sieciowych,
c) praktyka w przeprowadzaniu audytów z zakresu bezpieczeństwa teleinformatycznego,
d) dopuszczenia do dostępu do informacji niejawnych (w rozumieniu ustawy „*o ochronie informacji niejawnych*").

Do zadań specjalisty od urządzeń sieciowych i sieci komputerowych należy:

- współdziałanie z audytorami kwalifikującymi (por. rozdz. 3) w wykonanie przedsięwzięć ścieżki formalnej z etapu wykonawczego audytu,
- nadzór nad pracami ekspertów dziedzinowych (por. rozdz. 3),
- współudział w opracowaniu raportów z analizy technicznej.

5. **Personel pomocniczy** (symbol: PP)

Personel pomocniczy, zajmujący się np. kopiowaniem, oprawianiem etc. stosownych dokumentów musi posiadać dopuszczenia do dostępu do informacji niejawnych (w rozumieniu ustawy „*o ochronie informacji niejawnych*") w przypadku prac z takimi dokumentami. W szczególnych przypadkach (np. ankieterzy), personel taki musi posiadać odpowiednie upoważnienia zleceniodawcy do przeprowadzenia niezbędnych czynności na terenie jego Instytucji.

II. Skład zmienny zespołu (symbol: ED)

Skład zmienny zespołu stanowią dobierani w miarę potrzeb eksperci dziedzinowi. Eksperci dziedzinowi są dobierani przez audytorów kwalifikujących dla potrzeb konkretnego audytu, w zależności od systemów (sprzętu i oprogramowania) występujących w audytowanym systemie teleinformatycznym szczególnie licznie lub odgrywających w nim szczególnie ważną rolę. Na dobór ekspertów wpływają także wymagania osobowe dotyczące np. posiadania dopuszczeń do informacji niejawnych o odpowiednich klauzulach.

Rozdział 2. Wyposażenie narzędziowe zespołu audytowego

Do narzędzi, którymi dysponuje zespół audytowy należą:

1. Kwestionariusze ankietowe opracowane na podstawie zaleceń normy ISO/IEC 17799.
2. Szablony edycyjne dokumentów.
3. Narzędzia zautomatyzowane (programy), głównie:
   - skanery bezpieczeństwa,
   - skanery inwentaryzacyjne,
   - skanery konfiguracji.

2.1. Kwestionariusze ankietowe

Kwestionariusze ankietowe opracowane na podstawie normy ISO/IEC 17799 zawierają 913 szczegółowych pytań rozłożonych pomiędzy dziesięć następujących grup tematycznych normy (numeracja, rozpoczynająca się od 3, jest zgodna z numeracją normy ISO/IEC 17799):

3. Polityka bezpieczeństwa
4. Organizacja bezpieczeństwa
5. Klasyfikacja i kontrola aktywów
6. Bezpieczeństwo osobowe
7. Bezpieczeństwo fizyczne i środowiskowe
8. Zarządzanie systemami i sieciami
9. Kontrola dostępu do systemu
10. Rozwój i utrzymanie systemu
11. Zarządzanie ciągłością działania
12. Zgodność

Wypełniona i zweryfikowana na podstawie wywiadów i wizji lokalnych ankieta stanowi podstawę do wydawania sądów na temat stopnia spełnienia wymagań 139 punktów audytowych wynikających z normy ISO/IEC 17799.

2.2. Szablony edycyjne dokumentów

Dla większości dokumentów powstających podczas audytu wypracowano szablony dotyczące co najmniej ich redakcji, a w części przypadków ustalające rozmieszczenie merytorycznych treści.

2.3. Skanery bezpieczeństwa

Skaner to każdy mechanizm (np. urządzenie lub program) przeglądający pewien zbiór obiektów w ustalonym porządku. Skaner bezpieczeństwa to oprogramowanie (lub, szerzej, sterowany tym oprogramowaniem system komputerowy) przeglądający komputery należące do pewnego zadanego zbioru i sprawdzający czy występują w nich podatności.

Wynikiem działania skanera bezpieczeństwa jest raport, który w swym podstawowym wydaniu zawiera dla każdego komputera wykaz zidentyfikowanych (występujących w nim) podatności, a dla każdej podatności określa: identyfikator (według pewnej uznanej klasyfikacji, np. *bugtraq*), opis, stopień zagrożenia oraz sposób usunięcia.

Skaner bezpieczeństwa jest zbiorem procedur (czasem kolejno powoływanych programów lub skryptów) w praktyce przeprowadzających próby ataków, które w przypadku powodzenia są odnotowywane. Wykorzystywanie skanera bezpieczeństwa bez porozumienia z dysponentem systemu komputerowego jest przestępstwem z art. 267[3] K.K. („uzyskaną informacją" jest właśnie informacja o stanie zabezpieczeń).

Skanery bezpieczeństwa działają wykorzystując wymienne zbiory sygnatur podatności i wzorce ataków – dane te powinny być aktualizowane w miarę zmian stanu sztuki w tej dziedzinie. Subskrypcja tych danych jest ujęta w ofercie producentów komercyjnych skanerów bezpieczeństwa. Znane, historyczne

[3] Art. 267 Kodeksu Karnego

§1. Kto bez uprawnienia uzyskuje informację dla niego nie przeznaczoną, otwierając zamknięte pismo, podłączając się do przewodu służącego do przekazywania informacji lub przełamując elektroniczne, magnetyczne albo inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§2. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem specjalnym.

skanery bezpieczeństwa to np. *Satan*, *Tiger* i *Cops*, a obecnie (tzn. w roku 2003) najczęściej wykorzystywane to *Internet Security Scanner* (firmy ISS), *NetRecon* (Symantec, dawniej Axent) lub *Retina* firmy eEye.

2.4. Skanery inwentaryzacyjne

Skanery inwentaryzacyjne to grupa (wyróżniona przez autorów) ze względu na specyficzne zastosowanie: do identyfikacji i sporządzania spisów wszelkich usług występujących na poddanych przeglądaniu komputerach. Obecnie najskuteczniejszym skanerem tej klasy, użytecznym głównie w dużych sieciach biurowych Windows, jest *Languard Network Security Scanner* (firmy GFI Software Ltd.), przez producenta zaliczony do skanerów bezpieczeństwa i powoli ewoluujący w ich kierunku.

2.5. Skanery konfiguracji

Skaner konfiguracji to program służący do automatycznego, zdalnego badania ustawień konfiguracyjnych (w tym tzw. zasad zabezpieczeń) pewnego zbioru komputerów, generujący odpowiednie raporty. Wadą jest konieczność zdalnego dostępu do badanych komputerów z uprawnieniami administratora, co jest naturalne w sieciach domenowych Windows, ale jest niezgodne z zasadami bezpieczeństwa w większości sieci o innej organizacji.

Przykłady programów tej klasy to: *Microsoft Baseline Security Analyzer* (Microsoftu) lub *NetIQ Security Analyzer* (NetIQ Corporation). Skanery konfiguracji o szczególnym przeznaczeniu to np. *HFNetChkLT* (Shavlik Technologies), badający jakie aktualizacje zostały zaaplikowane w systemach Windows oraz *GASP* – wykorzystywany np. przez Business Software Alliance w poszukiwaniu nielegalnego oprogramowania.

Rozdział 3. Procesy audytowe

W dalszej części tego rozdziału opisano ogólnie, z komentarzami, procesy audytowe przyporządkowane do poszczególnych etapów audytu, oraz podano (tabela 3.1) kto z Zespołu Audytowego odpowiada za każdy proces i kto go nadzoruje.

I. Etap przygotowawczy audytu

1. Spotkanie wstępne z przedstawicielami zleceniodawcy:
   1.1. Prezentacja członków zespołu audytowego, przedłożenie dokumentów (poświadczeń bezpieczeństwa), ustalenie zakresu upoważnień audytorów do zbierania i dostępu do informacji zleceniodawcy; **ustalenie terminu wydania odpowiednich zarządzeń dopuszczających formalnie audytorów do działań w obszarze jurysdykcji zleceniodawcy**. Wydanie takich zarządzeń jest niezbędne do rozpoczęcia etapu wykonawczego audytu – w praktyce, etap ten może być realizowany dopiero **po** ich ogłoszeniu w instytucji zleceniodawcy.
   1.2. Ustalenie głównego konsultanta (osoby kontaktowej) oraz, w razie potrzeby, Zespołu Konsultantów ze strony zleceniodawcy. Główny konsultant (oraz odpowiednio członkowie Zespołu Konsultantów) musi być upoważniony do wyrażania opinii i składania wiążących oświadczeń w imieniu zleceniodawcy
   1.3. Wskazanie pracowników zleceniodawcy kompetentnych w poszczególnych zakresach tematycznych audytu. Audytorzy mogą formułować sądy na podstawie informacji zebranych z wszelkich dostępnych źródeł, w szczególności od każdego pracownika zleceniodawcy. Zleceniodawca powinien jednak wskazać pracowników szczególnie kompetentnych do udzielania informacji „o stanie rzeczy". W przeciwieństwie do konsultantów (patrz punkt 1.2), którzy mają prawo do interpretacji, zajmowania stanowiska i wyrażania woli w imieniu zleceniodawcy, wskazani pracownicy udzielają tylko informacji (prawdziwych w rozumieniu i najlepszej wierze zleceniodawcy).
   1.4. Uzgodnienie zasad komunikacji pomiędzy personelem zleceniodawcy i zespołem audytowym (w szczególności odpowiedzialności za opóźnienia i przesuwania terminu zakończenia prac), w tym:
      - zasad planowania konsultacji i autoryzacji dokumentów przez konsultantów,
      - zasad zbierania informacji wśród pracowników zleceniodawcy,
      - zasad prowadzenia prac audytowych – wykonywania zadań na rzecz audytorów przez personel zleceniodawcy (uprawnienia audytorów do samodzielnych działań, uprawnienia personelu zleceniodawcy do nadzoru, uprawnienia audytorów do żądania pomocy).
   1.5. Ustalenie harmonogramu prac audytowych.

2. Przeprowadzenie (w miarę potrzeby) seminarium kształtującego świadomość gremiów kierowniczych instytucji zleceniodawcy w zakresie audytu i bezpieczeństwa teleinformatycznego. Praktyka pokazuje, że seminarium takie pozwala kadrze kierowniczej zleceniodawcy oraz jego pracownikom współpracującym z audytorami wyrobić sobie pogląd na zakres prac audytowych oraz ujednolicić sposób rozumienia pojęć i terminów związanych z szeroko rozumianym bezpieczeństwem teleinformatycznym.

II. Etap wykonawczy audytu

3. Ścieżka formalna

W ramach działań wykonywanych na tej ścieżce postępowania audytorzy badają zarządzanie bezpieczeństwem teleinformatycznym w Instytucji zleceniodawcy na zgodność z określonym w umowie wzorcem audytowym (np. na zgodność z zaleceniami BS 7799 lub normą ISO/IEC 17799. Dla uproszczenia opisu w dalszej części opisu metodyki przyjęto, że tym wzorcem audytowym jest norma ISO/IEC 17799).

Podstawowe procesy ścieżki formalnej to:

3.1. Zebranie od zleceniodawcy i analiza dokumentacji ustanawiającej porządek prawny w badanej instytucji – podległość, odpowiedzialność i uprawnienia – w zakresie bezpieczeństwa teleinformatycznego (statut, regulaminy, stanowiskowe karty pracy, umowy, etc.).

3.2. Zebranie u zleceniodawcy i analiza dokumentacji ustanawiającej zależności między zleceniodawcą a podmiotami zewnętrznymi (umowy i inne dokumenty stanowiące), w szczególności:

- dokumentacji przenoszącej odpowiedzialność za zasoby teleinformatyczne zleceniodawcy na inne podmioty prawne, w tym umowy outsourcingowe i ubezpieczeniowe oraz umowy archiwizacji danych,
- dokumentacji ustanawiającej odpowiedzialność zleceniodawcy za zasoby obce (wszelkie umowy),
- umów między zleceniodawcą a innymi podmiotami, dopuszczających dostęp obcych pracowników do zasobów zleceniodawcy lub zasobów mu powierzonych (sprawdzenie pod kątem zapewnienia warunków należytej staranności w zakresie bezpieczeństwa teleinformatycznego).

3.3. Przekazanie do wypełnienia zidentyfikowanym w punkcie 1.3 osobom ze strony zleceniodawcy (kompetentnym w poszczególnych zakresach tematycznych audytu) tematycznych kwestionariuszy audytowych.

3.4. Wizje lokalne i wywiady w siedzibie zleceniodawcy (lub lokalizacjach ważnych z jakiegoś powodu dla zleceniodawcy) przeprowadzane przez audytorów w celu wyrobienia wstępnej opinii na stosowany w praktyce sposób zarządzania bezpieczeństwem teleinformatycznym w Instytucji zleceniodawcy.

3.5. Zebranie wypełnionych kwestionariuszy (przekazanych zgodnie z punktem 3.3) i ich analiza.

3.6. Spotkanie (w miarę potrzeby) z osobami, które wypełniły kwestionariusze w celu wyjaśnienia wątpliwości, uzupełnienia nieścisłości i braków, konfrontacja ustaleń z wynikami badań technicznych i powtórne (w miarę potrzeby) wizje lokalne i wywiady.

3.7. Końcowa analiza i opracowanie kwestionariuszy.

3.8. Opracowanie raportu końcowego zawierającego opinię o zgodności z normą ISO/IEC 17799.

4. Ścieżka techniczna

W ramach działań wykonywanych na tej ścieżce postępowania, w pierwszej fazie audytorzy analizują dokumentację techniczną sieci i systemów teleinformatycznych oraz systemów ochrony fizycznej i technicznej (w tym przeciwpożarowego i zasilania w energię elektryczną). Celem analizy jest:

- wykrycie braków w dokumentacji,
- przygotowanie testów penetracyjnych oraz badań za pomocą zautomatyzowanych narzędzi,
- przygotowanie (w razie potrzeby) pomiarów emisji ujawniającej,
- ujawnienie błędów koncepcyjnych w budowie sieci i systemów,
- przygotowanie danych do raportu końcowego z badań przeprowadzonych w ramach ścieżki technicznej.

W drugiej fazie działań audytorów i ekspertów dziedzinowych są przeprowadzane niezbędne (lub wynikające z umowy) pomiary i badania sieci i systemów. Ważnym produktem wynikowym działań prowadzonych w ramach ścieżki technicznej jest wykrycie podatności „do natychmiastowego usunięcia", tj. takich, których usunięcie w istotnym stopniu zmniejsza ryzyko utraty poufności, integralności lub dostępności informacji przetwarzanej, przechowywanej i przesyłanej przez zleceniodawcę.

Podstawowe procesy ścieżki technicznej to:

4.1. Analiza dostarczonej dokumentacji technicznej sieci i systemów (teleinformatycznych i technicznych) zleceniodawcy.

4.2. Badania stanu ochrony fizycznej i technicznej:

4.2.1. Przegląd zabezpieczeń fizycznych i technicznych, w tym zabezpieczeń przeciwpożarowych.

4.2.2. Przegląd systemu zasilania w energię elektryczną urządzeń i systemów zleceniodawcy.

4.2.3. Pomiar emisji ujawniającej (w razie potrzeby)[4].

4.2.4. Przeszukanie na obecność urządzeń podsłuchowych i przegląd środków ochrony osobistej (w razie potrzeby).

4.2.5. Opracowanie wstępnego raportu z badań systemów ochrony fizycznej i technicznej.

4.3. Badania stanu ochrony teleinformatycznej:

4.3.1. Wykonanie wyrywkowego badania konfiguracji wybranych komputerów w sieciach i systemach zleceniodawcy.

4.3.2. Badanie podatności zautomatyzowanymi narzędziami[5] w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy.

4.3.3. Badanie ustawień konfiguracyjnych zautomatyzowanymi narzędziami w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy.

4.3.4. Badanie zaaplikowanych aktualizacji zautomatyzowanymi narzędziami w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy.

4.3.5. Analiza otrzymanych w punktach 4.3.1–4.3.4 wyników badań i sporządzenie wykazu „Podatności do natychmiastowego usunięcia".

4.3.6. Wykonanie uzupełniających testów penetracyjnych.

4.3.7. Aktualizacja wykazu „Podatności do natychmiastowego usunięcia".

[4] W razie prowadzenia audytu na zgodność z wymaganiami ustawy „o ochronie informacji niejawnych" w zakresie informacji stanowiących tajemnice państwową, jest to punkt obligatoryjny audytu.

[5] Prace prowadzone w ścisłej współpracy z administratorami technicznymi zleceniodawcy.

4.3.7. Wykonanie, w miarę potrzeby, za pomocą zautomatyzowanych narzędzi inwentaryzacyjnych, inwentaryzacji składników sieci i systemów zleceniodawcy.

4.3. Przekazanie (za pisemnym potwierdzeniem odbioru) stronie zleceniodawcy wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia".

4.4. Opracowanie raportu końcowego z analiz technicznych.

III. Etap sprawozdawczy audytu

5. Opracowanie dokumentu końcowego z audytu bezpieczeństwa teleinformatycznego w Instytucji zleceniodawcy.

6. Przekazanie zleceniodawcy zbioru dokumentów audytowych (raporty, wydruki z narzędzi skanujących, etc.) – zdanie pracy pt. „Audyt bezpieczeństwa teleinformatycznego w (*nazwa instytucji zleceniodawcy*)". Oprócz formalnego przekazania dokumentów, w punkcie tym może zawierać się także spotkanie – prezentacja zleceniodawcy wyników audytu, wykonana przez audytora kwalifikującego.

Tabela 3.1. Zakresy odpowiedzialności i nadzoru procesów audytu

Numer procesu	Skrócony opis procesu	Odpowiedzialny	Nadzór
1.1	ustalenia wstępne	AK_1	AK_2
1.2	ustalenie konsultanta (–ów)	AK_1	AK_2
1.3	ustalenie informatorów	AK_1	AK_2
1.4	ustalenie zasad komunikacji	AK_1	AK_2
1.5	opracowanie harmonogramu	AK_1	AK_2
2	seminarium	AK_2	AK_1
3.1	zebranie i analiza dokumentacji o porządku prawnym	AK_2	AK_1
3.2	zebranie i analiza dokumentacji o zależnościach z podmiotami zewnętrznymi	AK_2	AK_1
3.3	przekazanie ankiet do wypełnienia	AK_2	AK_1
3.4	wizje lokalne i wywiady	AK_1	AK_2
3.5	zebranie i analiza ankiet	AK_2	AK_1
3.6	uzupełnianie ankiet	AK_2	AK_1
3.7	opracowanie ankiet	AK_2	AK_1
3.8	wykonanie raportu o zgodności z normą ISO/IEC 17799	AK_2	AK_1
4.1	analiza dokumentacji technicznej	SF–T, SA–PU, SUS–SK	AK_1
4.2.1	przegląd zabezpieczeń F–T	SF–T	AK_1
4.2.2	przegląd systemu zasilania	SF–T	AK_1
4.2.3	pomiar emisji ujawniającej	SA–PU	AK_1
4.2.4	poszukiwanie podsłuchów	SA–PU	AK_1
4.2.5	analiza notatek wewnętrznych Zespołu	AK_1	AK_2
4.3.1	wyrywkowe badania konfiguracji	SUS-SK lub ED	AK_1
4.3.2	badanie podatności (zautomatyzowane)	SUS-SK lub ED	AK_1
4.3.3	badanie konfiguracji (zautomatyzowane)	SUS-SK lub ED	AK_1
4.3.4	badanie uaktualnień (zautomatyzowane)	SUS-SK lub ED	AK_1
4.3.5	analiza wyników badań sieci teleinformatycznej	AK_1	AK_2
4.3.6	ręczne testy penetracyjne	ED	SUS-SK
4.3.7	aktualizacja wykazu podatności	AK_1	AK_2
4.3.8	inwentaryzacja zasobów (zautomatyz.)	SUS-SK lub ED	AK_1
4.4	przekazanie informacji o podatnościach	AK_1	AK_2
4.5	wykonanie raportu z badań technicznych	AK_1	AK_2
5	opracowanie dokumentu końcowego audytu	AK_1	AK_2
6	przekazanie wyników audytu zleceniodawcy	AK_1	AK_2

Rozdział 4. Specyfikacja dokumentów audytowych

W tym rozdziale metodą IPO (ang. *Input–Process–Output*) są wyspecyfikowane dokumenty związane z procesem audytu. Na końcu rozdziału w tabelach 4.1 i 4.2 są zebrane dokumenty niezbędne do prowadzenia prac audytowych oraz wytwarzane podczas audytu.

4.1. Tabele IPO

Objaśnienia do tabel IPO:

1. Symbol (*) przy numerze procesu oznacza, że proces ten jest dekomponowany na podprocesy.
2. Dokumenty określane w tabelach jako „notatka" dzielą się na dwa rodzaje:
   1) notatki służbowe Zespołu – zapisy autoryzowane, kopie przekazywane zleceniodawcy,
   2) notatki wewnętrzne Zespołu – zapisy nieautoryzowane, bez pozostawiania kopii u zleceniodawcy.
3. Linią przerywaną zaznaczone są krawędzie tabel z procesami opcjonalnymi (tzn. wykonywanymi na specjalne, zapisane w umowie, wymaganie zleceniodawcy).
4. Czcionką pogrubioną są zaznaczone podstawowe dokumenty wynikowe audytu, przekazywane zleceniodawcy.

Wejście	• dokumenty uwierzytelniające Zespołu • zapytanie ofertowe lub istotne warunki zamówienia • umowa
Nr procesu	1 (*)
Proces	Spotkanie wstępne z przedstawicielami zleceniodawcy
Wyjście	• zakres upoważnień • zarządzenia o audycie • zarządzenie o seminarium (opcjonalnie) • harmonogram • autoryzowana notatka służbowa 1 Zespołu

Wejście	• dokumenty uwierzytelniające Zespołu • zapytanie ofertowe lub istotne warunki zamówienia • umowa
Nr procesu	1.1
Proces	prezentacja członków zespołu audytowego, przedłożenie dokumentów (poświadczeń bezpieczeństwa), ustalenie zakresu upoważnień audytorów do zbierania i dostępu do informacji zleceniodawcy; ustalenie terminu wydania odpowiednich zarządzeń dopuszczających formalnie audytorów do działań w obszarze jurysdykcji zleceniodawcy
Wyjście	• zakres upoważnień • zarządzenia o audycie • zarządzenie o seminarium (opcjonalnie)

Wejście	zakres upoważnień
Nr procesu	1.2
Proces	ustalenie głównego konsultanta (osoby kontaktowej) ze strony zleceniodawcy – przedstawiciela upoważnionego do wyrażania opinii, składania oświadczeń i wyrażania woli w imieniu zleceniodawcy
Wyjście	autoryzowana notatka służbowa 1 Zespołu

Wejście	• zakres upoważnień • umowa
Nr procesu	1.3
Proces	ustalenie osób ze strony zleceniodawcy kompetentnych w poszczególnych zakresach tematycznych audytu
Wyjście	autoryzowana notatka służbowa 1 Zespołu

Wejście	• zakres upoważnień • umowa
Nr procesu	1.4
Proces	uzgodnienie zasad komunikacji pomiędzy personelem zleceniodawcy i zespołem audytowymi (w szczególności odpowiedzialności za opóźnienia i przesuwania terminu zakończenia prac)
Wyjście	autoryzowana notatka służbowa 1 Zespołu

Wejście	• zakres upoważnień • autoryzowana notatka służbowa 1 Zespołu • zapytanie ofertowe lub istotne warunki zamówienia • oferta • umowa
Nr procesu	1.5
Proces	opracowanie harmonogramu
Wyjście	harmonogram

Wejście	zarządzenie zleceniodawcy o miejscu i terminie przeprowadzenia seminarium
Nr procesu	2 (opcjonalnie)
Proces	Przeprowadzenie (w miarę potrzeby) seminarium kształtującego świadomość gremiów kierowniczych instytucji zleceniodawcy w zakresie audytu i bezpieczeństwa teleinformatycznego.
Wyjście	**materiały seminaryjne**

Wejście	• zakresy upoważnień • statut • regulaminy • zobowiązania indywidualne pracowników (stanowiskowe karty pracy, wykazy obowiązków etc.) • umowy przenoszące odpowiedzialność za zasoby teleinformatyczne zleceniodawcy na inne podmioty prawne (umowy outsourcingowe, ubezpieczeniowe) • dokumentacja ustanawiająca odpowiedzialność za zasoby obce (wszelkie **umowy)** • umowy między zleceniodawcą a innymi podmiotami dopuszczające dostęp obcych pracowników do zasobów zleceniodawcy lub zasobów mu powierzonych • kwestionariusze audytowe • zarządzenie o audycie • raport końcowy z analiz i badań technicznych
Nr procesu	3 (*)
Proces	badanie na zgodność z normą ISO/IEC 17799 (ścieżka formalna)
Wyjście	**raport końcowy o zgodności z normą ISO/IEC 17799**

Wejście	• statut • regulaminy • zarządzenia wewnętrzne dotyczące bezpieczeństwa • stanowiskowe karty pracy • umowy
Nr procesu	3.1
Proces	zebranie od zleceniodawcy i analiza dokumentacji ustanawiającej porządek prawny w badanej instytucji – podległość, odpowiedzialność i uprawnienia – w zakresie bezpieczeństwa teleinformatycznego
Wyjście	**pisemna opinia o dokumentacji organizacyjnej**

Wejście	• umowy przenoszące odpowiedzialność za zasoby teleinformatyczne zleceniodawcy na inne podmioty prawne (umowy outsourcingowe, ubezpieczeniowe) • dokumentacja ustanawiająca odpowiedzialność za zasoby obce (wszelkie umowy) • umowy między zleceniodawcą a innymi podmiotami dopuszczające dostęp obcych pracowników do zasobów zleceniodawcy lub zasobów mu powierzonych
Nr procesu	3.2
Proces	zebranie od zleceniodawcy i analiza dokumentacji ustanawiającej zależności między zleceniodawcą a podmiotami zewnętrznymi (sprawdzenie pod kątem zapewnienia warunków należytej staranności w zakresie bezpieczeństwa teleinformatycznego)
Wyjście	pisemna opinia o dokumentacji organizacyjnej

Wejście	• kwestionariusze audytowe • zakresy upoważnień
Nr procesu	3.3
Proces	przekazanie do wypełnienia zidentyfikowanym w procesie 1.3 osobom ze strony zleceniodawcy (kompetentnym w poszczególnych zakresach tematycznych audytu) tematycznych kwestionariuszy audytowych
Wyjście	notatka (wykaz z podpisami osób pobierających kwestionariusze) o wydanych kwestionariuszach z zaznaczonym terminem zwrotu

Wejście	• upoważnień zakresy
Nr procesu	3.4
Proces	wizje lokalne i wywiady w siedzibie zleceniodawcy (lub z wynikających z umowy lokalizacjach)
Wyjście	notatki wewnętrzne Zespołu z wizji lokalnych i wywiadów (wywiady autoryzowane w razie potrzeby)

Wejście	• wykaz osób którym wydano kwestionariusze audytowe • wypełnione kwestionariusze • notatki wewnętrzne Zespołu z wizji lokalnych i wywiadów • raport końcowy z analiz i badań technicznych
Nr procesu	3.5
Proces	zebranie przekazanych w procesie 3.3 kwestionariuszy i ich analiza
Wyjście	lista braków do uzupełnienia („dopytania") – notatka wewnętrzna Zespołu

Wejście	• zakres upoważnień • wypełnione kwestionariusze • lista braków do uzupełnienia („dopytania") – notatka wewnętrzna Zespołu
Nr procesu	3.6
Proces	spotkanie (w miarę potrzeby) z osobami, które wypełniły kwestionariusze w celu wyjaśnienia wątpliwości, uzupełnienia nieścisłości i braków, konfrontacja ustaleń z wynikami badań technicznych i powtórne (w miarę potrzeby) wizje lokalne i wywiady.
Wyjście	uzupełnione kwestionariusze

Wejście	• uzupełnione kwestionariusze ankietowe • notatki z wizji i wywiadów • opinia o dokumentacji (dokumenty wynikowe procesów 3.2, 3.2, 4.1) • raport końcowy z analiz i badań technicznych
Nr procesu	3.7
Proces	opracowanie kwestionariuszy ankietowych
Wyjście	opracowana ankieta

Wejście	• notatki z wizji i wywiadów • opinia o dokumentacji (dokumenty wynikowe procesów 3.2, 3.2, 4.1) • opracowana ankieta • raport końcowy z analiz i badań technicznych
Nr procesu	3.8
Proces	opracowanie raportu końcowego o zgodności z normą ISO/IEC 17799
Wyjście	**raport końcowy o zgodności z normą ISO/IEC 17799**

Wejście	• zakresy upoważnień • dokumentacja techniczna sieci i systemów (teleinformatycznych i technicznych) zleceniodawcy
Nr procesu	4 (*)
Proces	badanie systemów ochrony fizycznej i technicznej oraz systemów i sieci teleinformatycznych zleceniodawcy (ścieżka techniczna)
Wyjście	**raport końcowy z analiz i badań technicznych**

Wejście	dokumentacja techniczna sieci i systemów (teleinformatycznych i technicznych) zleceniodawcy
Nr procesu	4.1
Proces	analiza dostarczonej dokumentacji technicznej sieci i systemów (teleinformatycznych i technicznych) zleceniodawcy
Wyjście	pisemna opinia o dokumentacji technicznej

Wejście	dokumentacja techniczna systemów ochrony fizycznej i technicznej
Nr procesu	4.2 (*)
Proces	badania stanu ochrony fizycznej i technicznej
Wyjście	• raport z badań technicznych systemów ochrony fizycznej i technicznej • wyniki pomiarów

Wejście	dokumentacja techniczna systemów ochrony fizycznej i technicznej
Nr procesu	4.2.1
Proces	przegląd zabezpieczeń fizycznych i technicznych, w tym zabezpieczeń przeciwpożarowych
Wyjście	notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż.

Wejście	dokumentacja techniczna systemów ochrony fizycznej i technicznej
Nr procesu	4.2.2
Proces	przegląd systemu zasilania w energię elektryczną urządzeń i systemów zleceniodawcy
Wyjście	notatka wewnętrzna Zespołu z przeglądu systemu zasilania

Wejście	dokumentacja techniczna systemów ochrony fizycznej i technicznej
Nr procesu	4.2.3
Proces	pomiar emisji ujawniającej (opcjonalnie)
Wyjście	• notatka wewnętrzna Zespołu ze strefowania budynków i pomieszczeń • wyniki pomiarów emisji ujawniającej

Wejście	dokumentacja techniczna systemów ochrony fizycznej i technicznej
Nr procesu	4.2.4
Proces	przeszukanie na obecność urządzeń podsłuchowych i przegląd środków ochrony osobistej (opcjonalnie)
Wyjście	notatka wewnętrzna Zespołu z przeglądu na obecność urządzeń podsłuchowych i przeglądu środków ochrony osobistej

Wejście	• notatka wewnętrzna Zespołu z przeglądu na obecność urządzeń podsłuchowych i przeglądu środków ochrony osobistej • notatka wewnętrzna Zespołu ze strefowania budynków i pomieszczeń • wyniki pomiarów • notatka wewnętrzna Zespołu z przeglądu systemu zasilania • notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż.
Nr procesu	4.2.5
Proces	analiza notatek wewnętrznych Zespołu
Wyjście	raport z badań technicznych systemów ochrony fizycznej i technicznej

Wejście	dokumentacja techniczna sieci i systemów teleinformatycznych
Nr procesu	4.3 (*)
Proces	badania stanu ochrony teleinformatycznej
Wyjście	• raport z badań technicznych systemów i sieci teleinformatycznych zleceniodawcy • **wykaz „Podatności do natychmiastowego usunięcia”** • **spis inwentaryzacyjny** (opcjonalnie)

Wejście	dokumentacja techniczna sieci i systemów teleinformatycznych
Nr procesu	4.3.1
Proces	wykonanie wyrywkowego badania konfiguracji komputerów i urządzeń w sieci i systemach zleceniodawcy
Wyjście	notatka wewnętrzna Zespołu o wynikach wyrywkowych badań konfiguracji

Wejście	dokumentacja techniczna sieci i systemów teleinformatycznych
Nr procesu	4.3.2
Proces	badanie podatności zautomatyzowanymi narzędziami w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy
Wyjście	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności + raporty generowane przez narzędzia

Wejście	dokumentacja techniczna sieci i systemów teleinformatycznych
Nr procesu	4.3.3
Proces	badanie ustawień konfiguracyjnych zautomatyzowanymi narzędziami w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy
Wyjście	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji + raporty generowane przez narzędzia

Wejście	dokumentacja techniczna sieci i systemów teleinformatycznych
Nr procesu	4.3.4
Proces	badanie zautomatyzowanymi narzędziami zaaplikowanych aktualizacji w wybranych (lub, w zależności od szczegółowych ustaleń, we wszystkich) sieciach i systemach zleceniodawcy
Wyjście	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji + raporty generowane przez narzędzia

Wejście	• notatka wewnętrzna Zespołu o wynikach badań losowych konfiguracji • notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji • notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji • notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności • raporty generowane przez narzędzia
Nr procesu	4.3.5
Proces	analiza otrzymanych wyników badań systemów i sieci teleinformatycznych
Wyjście	• wytyczne do wykonania uzupełniających heurystycznych testów penetracyjnych • wstępny wykaz „Podatności do natychmiastowego usunięcia” • raport z badań technicznych systemów i sieci teleinformatycznych zleceniodawcy

Wejście	• wytyczne do wykonania uzupełniających heurystycznych testów penetracyjnych • dokumentacja techniczna sieci i systemów
Nr procesu	4.3.6
Proces	wykonanie uzupełniających heurystycznych testów penetracyjnych
Wyjście	raport z testów penetracyjnych

Wejście	• wyniki testów penetracyjnych • wstępny wykaz „Podatności do natychmiastowego usunięcia”
Nr procesu	4.3.7
Proces	aktualizacja wykazu „Podatności do natychmiastowego usunięcia”
Wyjście	**wykaz „Podatności do natychmiastowego usunięcia”**

Wejście	dokumentacja techniczna sieci i systemów
Nr procesu	4.3.8 (opcjonalnie)
Proces	wykonanie, w miarę potrzeby, za pomocą zautomatyzowanych narzędzi inwentaryzacyjnych, inwentaryzacji składników sieci i systemów zleceniodawcy
Wyjście	spis inwentaryzacyjny wykonany za pomocą zautomatyzowanych narzędzi inwentaryzacyjnych

Wejście	uzupełniony wykaz „Podatności do natychmiastowego usunięcia”
Nr procesu	4.4
Proces	przekazanie stronie zleceniodawcy wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia”
Wyjście	potwierdzenie przez zleceniodawcę przyjęcia wykazu „Podatności do natychmiastowego usunięcia”

Wejście	• pisemna opinia o dokumentacji technicznej • raport z badań technicznych systemów ochrony F–T • raport z badań technicznych systemów teleinformatycznych • wykaz „Podatności do natychmiastowego usunięcia”
Nr procesu	4.5
Proces	opracowanie raportu końcowego z analiz technicznych
Wyjście	**raport końcowy z analiz i badań technicznych**

Wejście	• raport końcowy z analiz i badań technicznych • raport końcowy o zgodności z normą ISO/IEC 17799
Nr procesu	5
Proces	Opracowanie dokumentu końcowego z audytu bezpieczeństwa teleinformatycznego w Instytucji zleceniodawcy
Wyjście	**dokument końcowy audytu**

Wejście	dokument końcowy audytu
Nr procesu	6
Proces	przekazanie zleceniodawcy zbioru dokumentów audytowych (raporty, wydruki z narzędzi skanujących, etc.) – odbiór wyników audytu
Wyjście	dokumenty odbioru pracy pt: „Audyt bezpieczeństwa teleinformatycznego w (*nazwa instytucji zleceniodawcy*)”

4.2. Specyfikacja zbiorcza dokumentów

Tab. 4.1. Wykaz dokumentów niezbędnych do przeprowadzenia prac audytowych

Lp.	Nazwa dokumentu	Dostarczany przez:
1	Umowa	zleceniodawca/Audytorzy
2	zapytanie ofertowe lub istotne warunki zamówienia	zleceniodawca/Audytorzy
3	dokumenty uwierzytelniające Zespołu Audytowego	Audytorzy
4	kwestionariusze audytowe	Audytorzy
5	dokumentacja techniczna systemów ochrony fizycznej i technicznej zleceniodawcy	zleceniodawca
6	dokumentacja techniczna sieci i systemów teleinformatycznych zleceniodawcy	zleceniodawca
7	statut instytucji zleceniodawcy	zleceniodawca
8	regulaminy obowiązujące w instytucji zleceniodawcy	zleceniodawca
9	obowiązujące zarządzenia w dziedzinie bezpieczeństwa	zleceniodawca
10	zobowiązania indywidualne pracowników (stanowiskowe karty pracy, wykazy obowiązków etc.)	zleceniodawca
11	dokumentacja przenosząca odpowiedzialność za zasoby teleinformatyczne zleceniodawcy (umowy outsourcingowe, ubezpieczeniowe itp.)	zleceniodawca
12	dokumentacja ustanawiająca odpowiedzialność za zasoby obce (wszelkie umowy)	zleceniodawca
13	umowy między zleceniodawcą a innymi podmiotami dopuszczające dostęp obcych pracowników do zasobów teleinformatycznych zleceniodawcy lub zasobów mu powierzonych	zleceniodawca

UWAGA

Opis zleceniodawca/Audytorzy w kolumnie „Dostarczany przez:” oznacza, że jest to dokument przygotowawczy do prowadzenie prac audytowych, którego uwierzytelnione kopie znajdują się w posiadaniu obu stron.

Tab. 4.2. Wykaz dokumentów wytwarzanych w procesie audytu

Lp.	Nazwa dokumentu	Status dokumentu	Wytwórca
1	autoryzowana notatka służbowa 1 Zespołu	wewnętrzny	Aud./Zlec.
2	zakres upoważnień	Oficjalny/ inicjujący	zleceniodawca
3	zarządzenia o audycie	oficjalny/ inicjujący	zleceniodawca
4	harmonogram prac audytowych	oficjalny	Aud./Zlec.
5	*zarządzenie o seminarium*	oficjalny	zleceniodawca
6	*materiały seminaryjne*	oficjalny/ przekaz.	Audytorzy
7	pisemna opinia o dokumentacji ustanawiającej porządek prawny w instytucji i ustanawiającej zależności między zleceniodawcą a podmiotami zewnętrznymi	oficjalny	Audytorzy
8	notatka (lista) o wydanych kwestionariuszach (z podpisami osób pobierających kwestionariusze)	oficjalny	Audytorzy
9	notatki wewnętrzne Zespołu z wizji lokalnych i wywiadów (wywiady autoryzowane w razie potrzeby)	wewnętrzny	Audytorzy
10	wypełnione kwestionariusze	wewnętrzny	Aud./Zlec.
11	lista braków do uzupełnienia („dopytania") w ankiecie – notatka wewnętrzna Zespołu	wewnętrzny	Audytorzy
12	uzupełnione kwestionariusze	wewnętrzny	Audytorzy
13	opracowana ankieta	wewnętrzny	Aud./Zlec.
14	pisemna opinia o dokumentacji technicznej	oficjalny	Audytorzy
15	notatka wewnętrzna Zespołu z przeglądu zabezpieczeń ochrony F–T i ppoż.	wewnętrzny	Audytorzy
16	notatka wewnętrzna Zespołu z przeglądu systemu zasilania	wewnętrzny	Audytorzy
17	*notatka wewnętrzna Zespołu ze strefowania budynków i pomieszczeń*	wewnętrzny	Audytorzy
18	*wyniki pomiarów emisji ujawniającej*	wewnętrzny	Audytorzy
19	*notatka wewnętrzna Zespołu z przeglądu na obecność urządzeń podsłuchowych i przeglądu środków ochrony osobistej*	wewnętrzny	Audytorzy

20	raport z badań technicznych systemów ochrony fizycznej i technicznej	oficjalny	Audytorzy
21	notatka wewnętrzna Zespołu o wynikach badań losowych konfiguracji	wewnętrzny	Audytorzy
22	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań podatności	wewnętrzny	Audytorzy
23	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań konfiguracji	wewnętrzny	Audytorzy
24	notatka wewnętrzna Zespołu o wynikach zautomatyzowanych badań zaaplikowanych aktualizacji	wewnętrzny	Audytorzy
25	wytyczne do wykonania uzupełniających ręcznych testów penetracyjnych	wewnętrzny	Audytorzy
26	wstępny wykaz „Podatności do natychmiastowego usunięcia”	wewnętrzny	Audytorzy
27	raport z badań technicznych systemów i sieci teleinformatycznych zleceniodawcy	wewnętrzny	Audytorzy
28	wyniki ręcznych testów penetracyjnych	wewnętrzny	Audytorzy
29	wykaz „Podatności do natychmiastowego usunięcia”	oficjalny/ przekaz.	Audytorzy
30	potwierdzenie przez zleceniodawcę przyjęcia wykazu zidentyfikowanych „Podatności do natychmiastowego usunięcia”	oficjalny	Aud./Zlec.
31	*spis inwentaryzacyjny wykonany za pomocą zautomatyzowanych narzędzi inwentaryzacyjnych*	oficjalny/ przekaz.	Audytorzy
32	wybrane raporty generowane przez narzędzia	oficjalny	Audytorzy
33	**raport końcowy z analiz i badań technicznych**	oficjalny/ końcowy	Audytorzy
34	**raport końcowy z audytu na zgodność z zaleceniami BS 7799 lub ISO/IEC 17799**	oficjalny/ końcowy	Audytorzy
35	**dokument końcowy audytu**	oficjalny/ końcowy	Audytorzy
36	**dokumenty odbioru pracy pt:** „Audyt bezpieczeństwa teleinformatycznego w (*nazwa instytucji zleceniodawcy*)”	oficjalny/końcowy	Aud./Zlec.

UWAGI

1. Nazwy dokumentów wypisane kursywą oznaczają, że są to dokumenty wytwarzane na specjalne życzenie zleceniodawcy (jako wyjście procesów opcjonalnych w tabelach IPO).

2. Opis Aud./Zlec. w kolumnie „Wytwórca" oznacza, że jest to dokument wytwarzany w wyniku wzajemnych uzgodnień pomiędzy audytorami i upoważnionymi przedstawicielami zleceniodawcy, autoryzowany przez obie strony.
3. Nazwy dokumentów wypisane pogrubioną czcionką oznaczają dokumenty końcowe (rozliczeniowe) audytu.
4. Status „oficjalny/przekaz." oznacza, że dokument ten zostaje przekazany zleceniodawcy w trakcie prac audytowych.
5. Status „oficjalny/inicjujący" oznacza, że jest to **dokument niezbędny do rozpoczęcia etapu wykonawczego audytu** – stanowi podstawę prawną wszelkich działań audytorów na terenie Instytucji zleceniodawcy.
6. Status „oficjalny" oznacza, ze dokument ten stanowi podstawę do opracowania dokumentów końcowych audytu lub zostaje do tych dokumentów włączony w całości.

Rozdział 5. Diagramy przepływu danych

Na podstawie zamieszczonych w dalszej części niniejszego rozdziału diagramów można:

1) ocenić złożoność procesów składających się na audyt;
2) prześledzić zależności pomiędzy dokumentami wytwarzanymi w procesie audytu;
3) ocenić na podstawie zależności pomiędzy procesami (oraz składu osobowego Zespołu) możliwości równoległego prowadzenia zadań audytowych.

Przedstawione diagramy są pomocne przy ustalaniu harmonogramu prowadzenia prac audytowych dla konkretnego zleceniodawcy oraz pozwalają uświadomić mu stopień złożoności przedsięwzięcia oraz niezbędny zakres jego zaangażowania w tym przedsięwzięciu (dostarczane dokumenty, konieczne rozporządzenia, konsultacje i szkolenia, udostępniane zasoby, etc.).

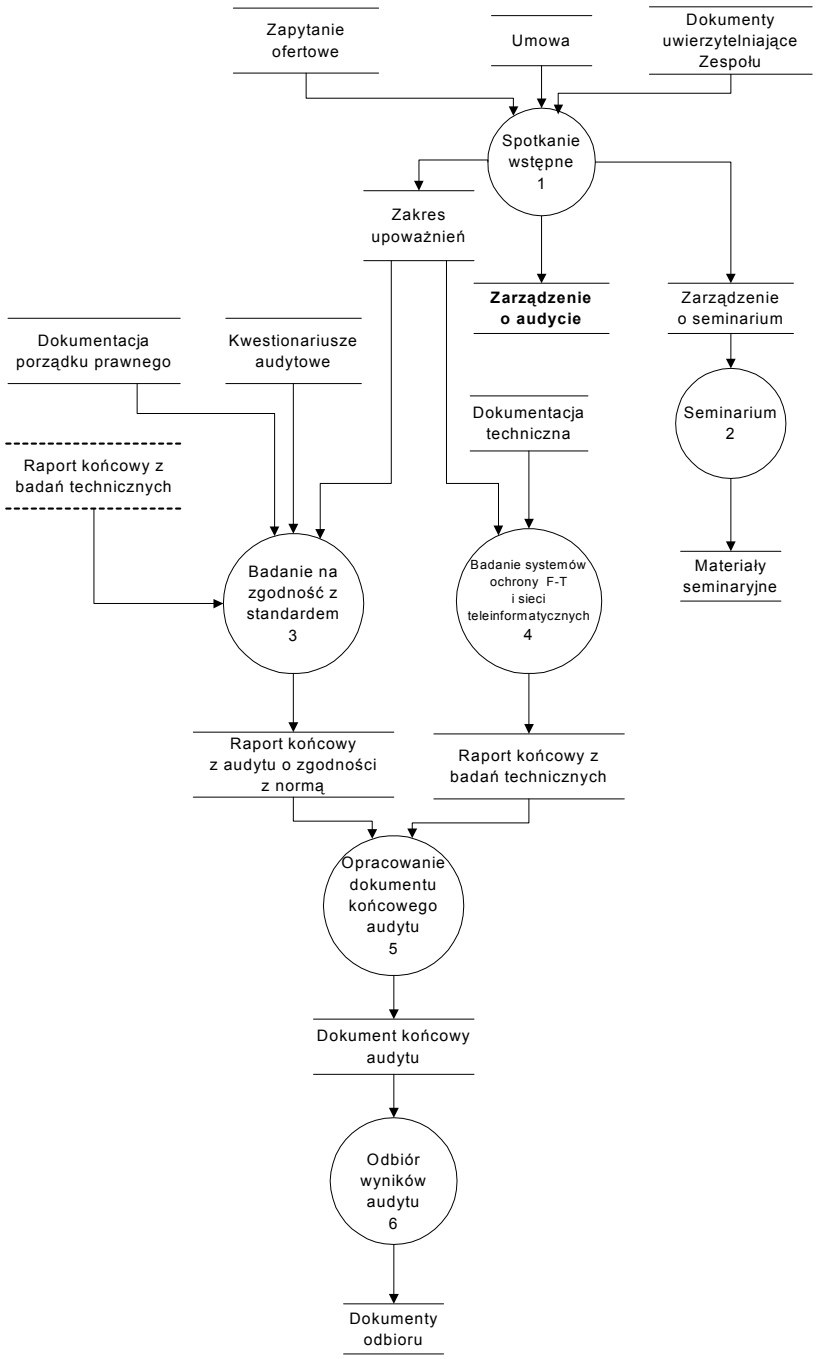

Diagram1: DFD_1 procesu audytu - schemat ogólny

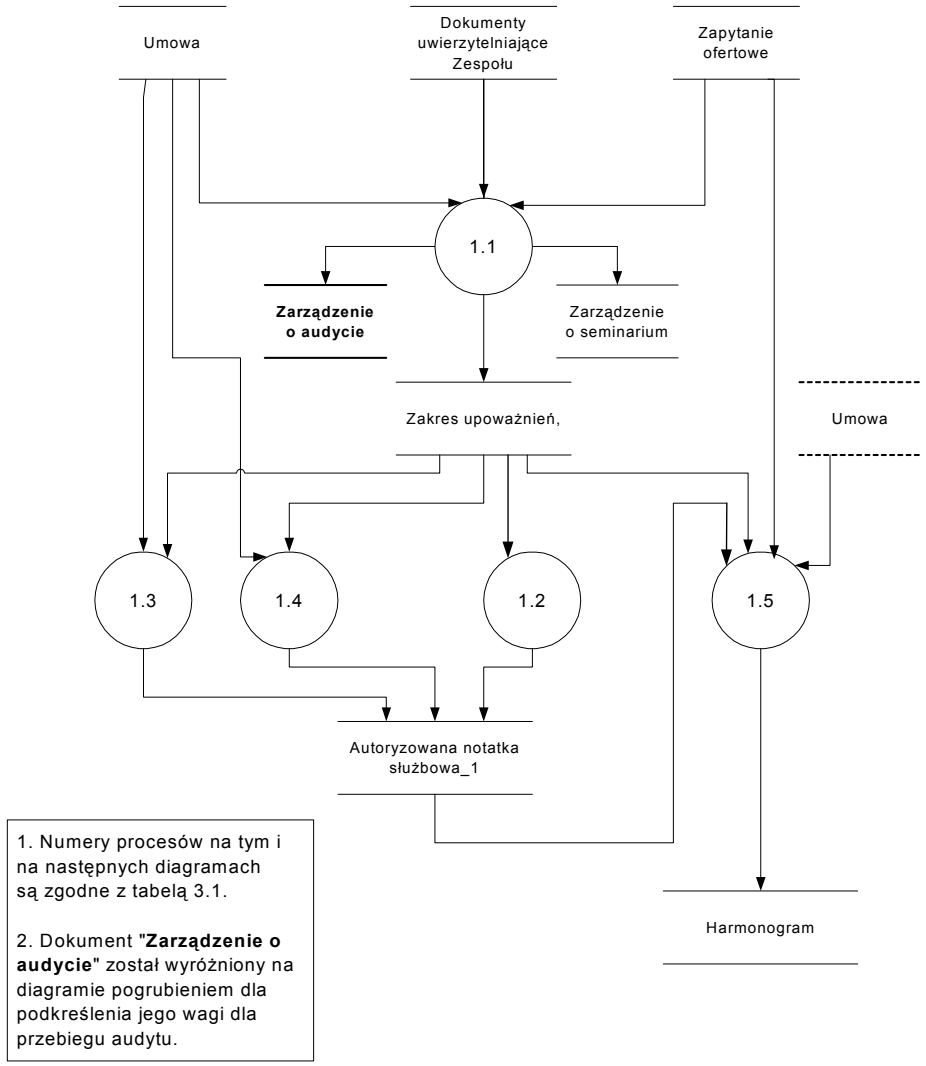

Diagram 2: DFD_2 - proces nr 1

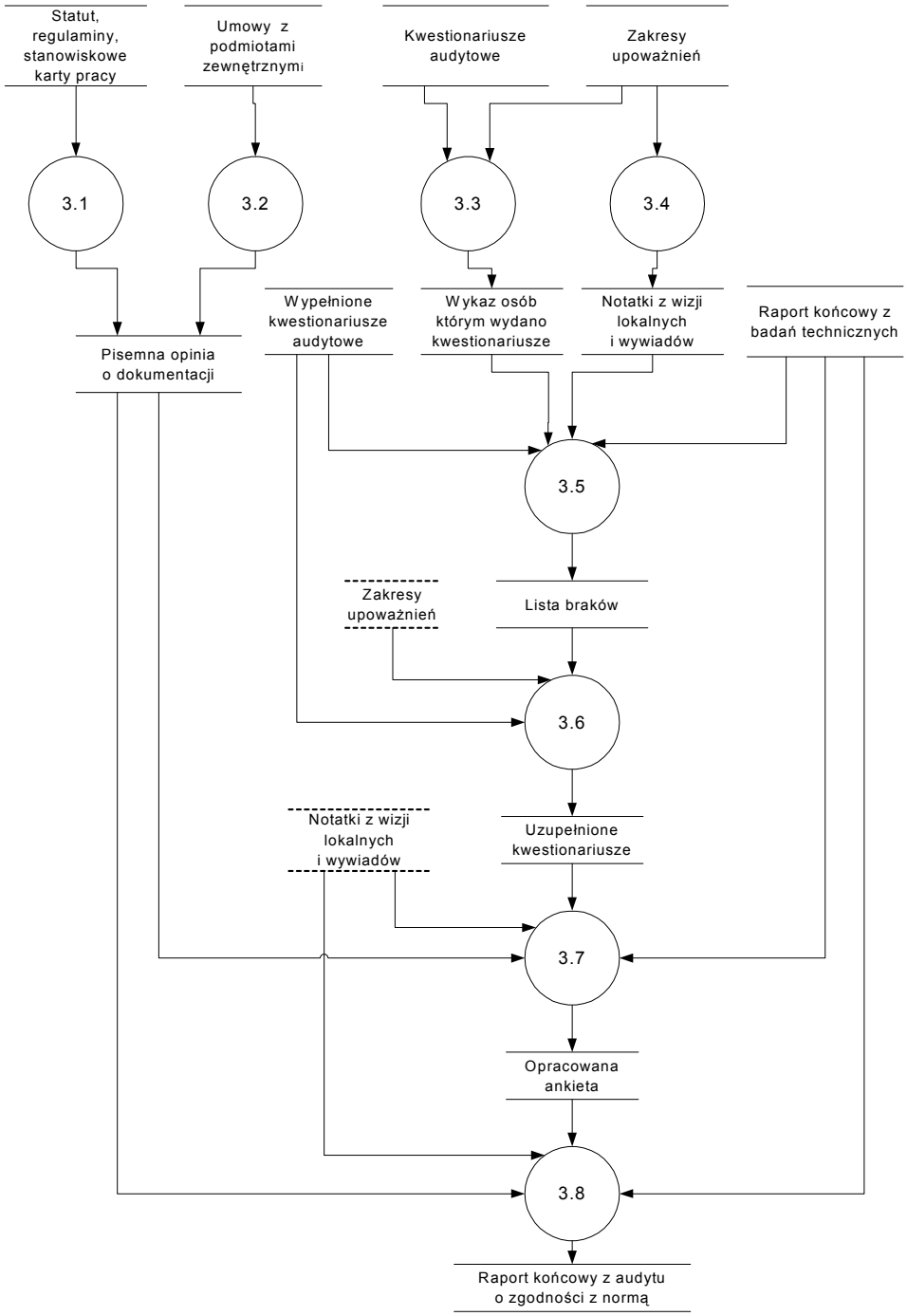

Diagram 3: DFD_2 - proces nr 3

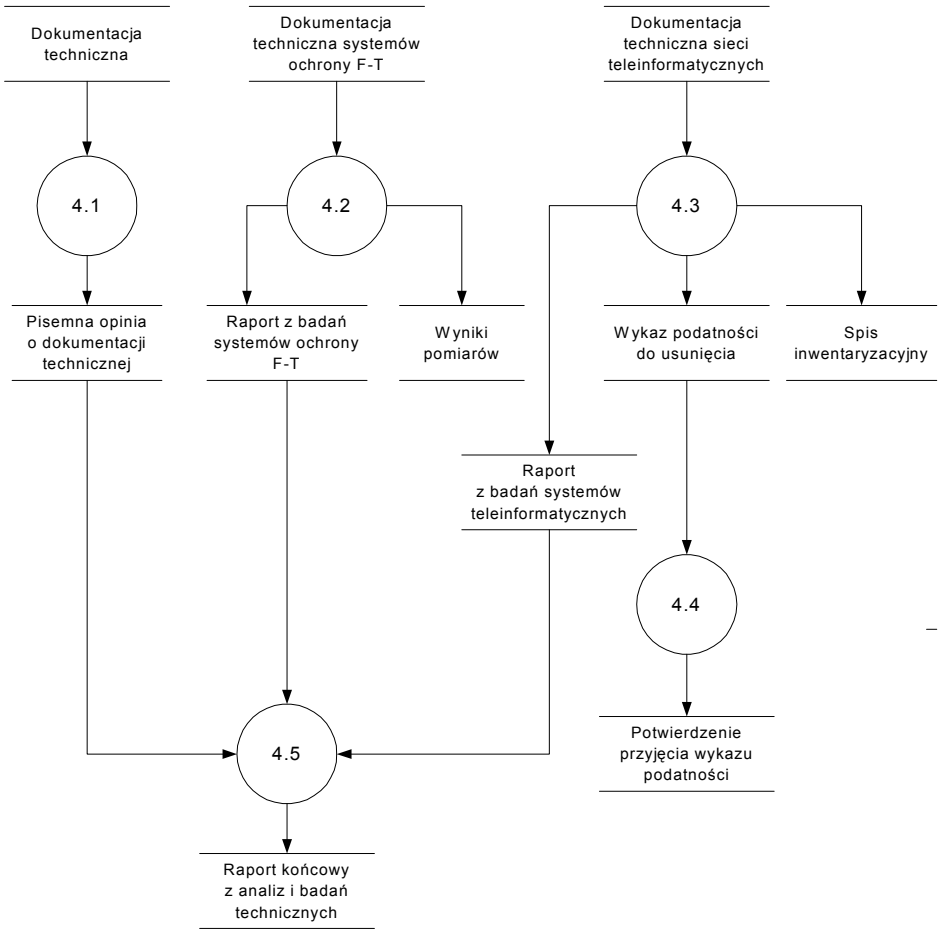

Diagram 4: DFD_2 - proces nr 4

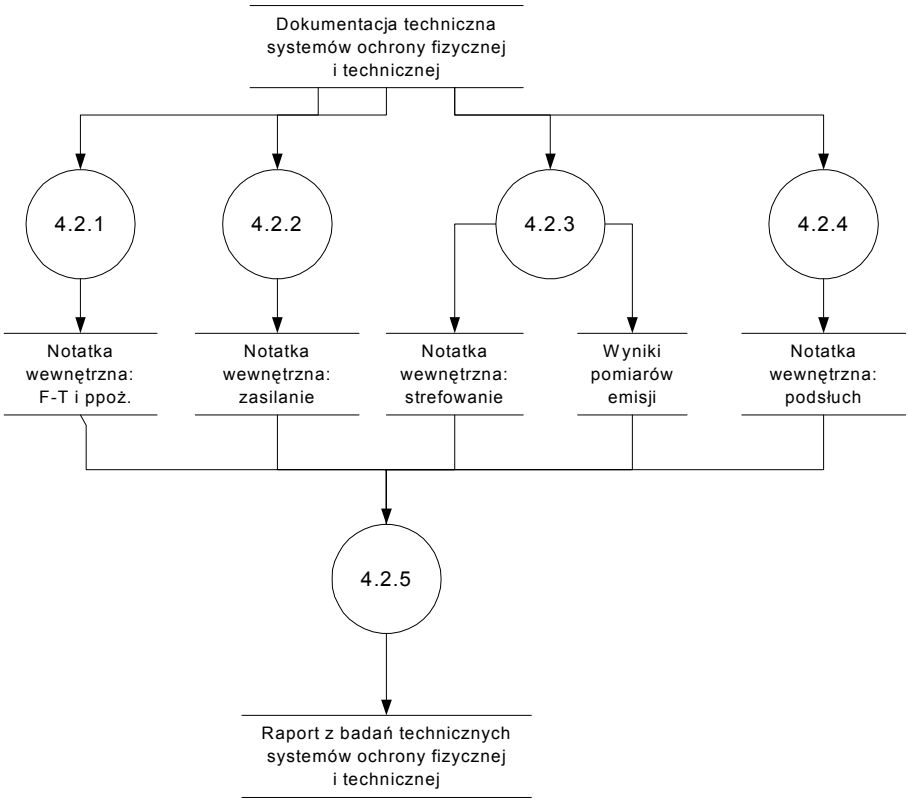

Diagram 5: DFD_3 - proces nr 4.2

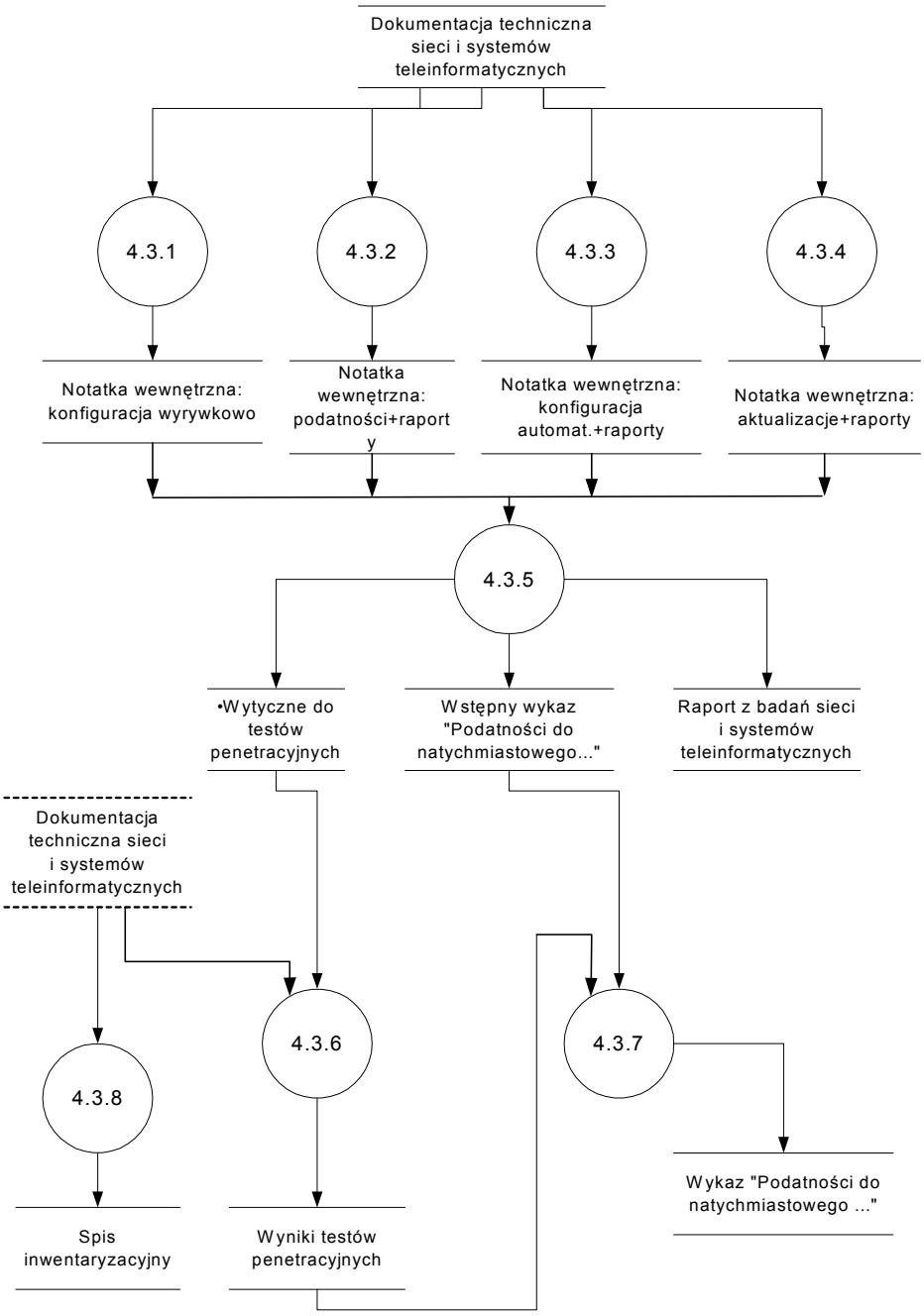

Diagram 6: DFD_3 - proces nr 4.3

Rozdział 6. Rzetelne praktyki

Niniejszy rozdział zawiera zapis tzw. „rzetelnych praktyk" (nazywanych też „najlepszymi praktykami" – z ang. *best practices*), tj. należących do kategorii know–how, heurystycznych metod postępowania, wypracowanych i sprawdzonych podczas dotychczasowej praktyki audytorskiej twórców metodyki.

Dwie podstawowe, ogólne zasady postępowania (praktyki) to:

1. Zespół audytorów bez zgody zleceniodawcy nie podaje żadnych informacji dotyczących audytu ani uzyskanych w związku z audytem, w szczególności nie umieszcza nazwy Instytucji zleceniodawcy na swoich listach referencyjnych.
2. Orientacja na klienta – w ramach etapu przygotowawczego dyskutowane są rzeczywiste oczekiwania klienta (być może niezapisane w jawnej formie w umowie), co pozwala na etapie wykonawczym odpowiednio rozłożyć akcenty, np. w ramach punktu 12 („Zgodność") normy ISO/IEC 17799 szczególnie dokładnie przeanalizować spełnienie wymogów formalnych wynikających z ustawy „*o ochronie danych osobowych*".

6.1. „Rzetelne praktyki" stosowane na ścieżce formalnej

1. Każda rozmowa, wizja lokalna etc. jest zawsze przeprowadzana przez dwóch członków Zespołu Audytowego.
2. Z każdej rozmowy, wizji lokalnej etc. jest sporządzana notatka wewnętrzna, która może być autoryzowana w razie potrzeby przez drugą stronę (w dokumentach Zespołu autoryzowane notatki wewnętrzne są nazywane notatkami służbowymi).

6.2. „Rzetelne praktyki" stosowane na ścieżce technicznej

1. Specjalista od sieci i urządzeń sieciowych (członek zespołu audytowego) prezentuje zespołowi audytowemu (szkolenie wewnętrzne) ogólny model przepływu informacji w sieci lub sieciach, w tym rozdział stref dystrybucji pakietów i zainstalowane mechanizmy separujące.

2. Wszelkie działania inwazyjne w systemach zleceniodawcy realizowane są przez uprawnionych pracowników zleceniodawcy pod kierunkiem audytorów. Audytorzy nie przejmują odpowiedzialności kompetentnych

pracowników zleceniodawcy w żadnym zakresie, nawet jeśli dla przyspieszenia prac zostaną dopuszczeni do występowania w roli operatora. Przy ortodoksyjnym traktowaniu tej zasady, podczas badań audytorzy fizycznie nie będą w ogóle dotykać żadnych urządzeń.

3. Wszelkie przeglądy (np. konfiguracji stacji roboczych) są wykonywane przez członków zespołu audytowego zawsze w asyście przedstawiciela zleceniodawcy (np. administratora stacji roboczych).

4. W przypadku wykrycia szczególnie groźnych podatności podczas badań technicznych zleceniodawca jest informowany o nich natychmiast po ich wykryciu, bez oczekiwania na zakończenie całości prac związanych z audytem. Działanie takie ma na celu umożliwienie zleceniodawcy podjęcie bezzwłocznych działań mających na celu ochronę informacji przetwarzanej, przechowywanej i przesyłanej w jego systemach i sieciach teleinformatycznych przed wykorzystaniem przez zagrożenia istniejących, wykrytych podatności.

5. Zasady badania konfiguracji stacji roboczych.

   Serwery, stacje robocze i urządzenia sieciowe dzielone są zwykle na trzy kategorie:

   - **kategoria I**: stacje–nosiciele informacji wrażliwej oraz urządzenia i łącza, których degradacja funkcji oznacza zagrożenie dla informacji wrażliwej;
   - **kategoria II**: stacje i koncentratory na których może pojawić się informacja wrażliwa;
   - **kategoria III**: stacje robocze i urządzenia na których nie jest przetwarzana i przechowywana informacja wrażliwa.

   Badanie konfiguracji obejmuje wszystkie stacje i urządzenia kat. I, oraz 2–5% stacji roboczych i urządzeń kat. II. Wybór stacji do badań wyrywkowych powinien być dokonany na podstawie racjonalnych przesłanek – najrozsądniej jest wybrać taki podzbiór stacji, który obejmuje stacje reprezentatywne dla pozostałych komputerów zaliczonych do kategorii II.

Podsumowanie

Opisana metodyka LP–A©, 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.

Literatura:

[1] Liderman K.: *Bezpieczeństwo teleinformatyczne*. IAiR WAT. Warszawa. 2001. ISBN 83–912747–8–0

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

[3] Liderman K.: *Analiza ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*. Biuletyn IAiR. Nr 16. WAT. Warszawa. 2001.

[4] Liderman K.: *O audycie raz jeszcze*... WinSecurity 6/02. Str. 39-44.

[5] Liderman K.: *System bezpieczeństwa teleinformatycznego*. Biuletyn IAiR. Nr 17. WAT. Warszawa. 2002.

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

[7] Materiały Bundesamt für Sichercheit in der Informationstechnik. IT-Grundschutzhandbuch. Niemcy. 2002.

[8] Common Criteria for Information Technology Security Evaluation. Part 1: Introduction and general model. May 1998. Version 2.0. CCIB-98-026.

[9] Common Criteria for Information Technology Security Evaluation. Part 2: Security functional requirements. May 1998. Version 2.0. CCIB-98-027

[10] Common Criteria for Information Technology Security Evaluation. Part 3: Security assurance requirements. May 1998. Version 2.0. CCIB-98-028.

[11] ITSEC. Version 1.2. June 1991.

[12] Trusted Computer System Evaluation Criteria. DoD. 15 August 1983. CSC-STD-001-83.

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

[14] BS 7799-1:1999: Part 1: Code of practice for Information Security Management. BSI.

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

[16] ISO/IEC 17799:2000. Information technology – Code of practice for Information Security Management.

[17] PN-I-02000: Technika informatyczna. Zabezpieczenia w systemach informatycznych. 1998.

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

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

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

[21] 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).

Recenzent: prof. dr hab. inż. Stanisław Paszkowski

Praca wpłynęła do redakcji 20.11.2003