BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 20, 2004

Zarys zastosowania metod sieciowych do wyznaczania czasu realizacji audytu bezpieczeństwa teleinformatycznego

Krzysztof LIDERMAN

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

STRESZCZENIE: W artykule została przedstawiona propozycja zastosowania metod sieciowych do wyznaczania czasu realizacji audytu bezpieczeństwa teleinformatycznego wykonywanego według metodyki LP-A oraz zostały przedyskutowane problemy występujące przy zbieraniu danych empirycznych.

1. Wprowadzenie

Już na etapie rozpatrywania ofert wykonania określonej pracy (np. audytu bezpieczeństwa teleinformatycznego) zamawiający zwykle żąda przedstawienia oszacowań kosztów planowanego przedsięwzięcia, ryzyka projektowego, a także harmonogramu. W przypadku przystąpienia do realizacji przedsięwzięcia, elementy te zostają uściślone w tzw. Planie Jakości Projektu (*ang.* ***P****roject* ***Q****uality* ***P****lan* – *PQP*)[1], którego pierwsza, obowiązująca wersja jest zwykle produktem realizacji pierwszego etapu pracy.

Plan Jakości Projektu jest dokumentem opisującym reguły, według których są przeprowadzane, nadzorowane i odbierane prace określone w przedsięwzięciu nazywanym potocznie „projektem". Przekazywane oficjalnie, jednorazowo zamawiającemu wyniki pracy noszą nazwę „dostawy", formalne

[1] Standardowo PQP jest elementem różnych metodyk prowadzenia projektów.

zaś ustosunkowanie się zamawiającego do dostawy nazywane jest „odbiorem". Cele PQP są następujące:

- określenie dla elementów dostaw przewidzianych w projekcie: zawartości merytorycznej, postaci (np. sposobu edycji i dostarczenia dokumentów), osób odpowiedzialnych oraz procedur i kryteriów odbioru;
- określenie ról i odpowiedzialności, zarówno po stronie wykonawcy jak i zamawiającego;
- osiągnięcie zaufania zamawiającego co do jakości pracy, która będzie wykonywana, dzięki prezentacji sposobu, w jaki będą wykonywane poszczególne zadania;
- określenie formalnych zasad rozwiązywania problemów, które mogą się pojawić podczas realizacji przedsięwzięcia;
- przedstawienie kluczowych środków, które będą stosowane w celu osiągnięcia uzgodnionej jakości produktów określonych w projekcie;
- jasne określenie uczestników projektu, procedur, reguł i stosowanych metod.

PQP jest przygotowywany przez wykonawcę i przedstawiony zamawiającemu do zatwierdzenia. W trakcie realizacji projektu, w przypadku zgody obu stron na wprowadzenie zmian w zapisach PQP, wykonawca wprowadza odpowiednie zmiany, generując nową wersję PQP, po czym przekazuje ją do zatwierdzenia zamawiającemu. PQP jest zatem narzędziem, przy pomocy którego wykonawca oraz zamawiający dbają o to, aby zostały osiągnięte cele określone w umowie, tj. PQP jest podstawą do stworzenia warunków, w których przedsięwzięcia przeprowadzane przez obie strony w ramach umowy powinny osiągnąć zamierzony stan kompletności oraz jakości.

Jednym z elementów PQP jest zwykle rozdział opisujący ryzyko związane z prowadzeniem przedsięwzięcia, którego dotyczy PQP, nazywane dalej „ryzykiem projektowym". W celu poprawnego oszacowania poziomu ryzyka projektowego niezbędne są ustalenia dotyczące:

- metodyki prowadzonego przedsięwzięcia (tutaj: LP-A),
- harmonogramu,
- zasobów zaangażowanych w projekt.

Trzeci z punktów, dotyczący zasobów, jest istotny dla ekonomicznej strony realizowanego przedsięwzięcia, ponieważ użyty tutaj termin „zasoby" w praktyce oznacza:

- ilość osób zaangażowanych w przedsięwzięcie (w szczególnych przypadkach również ze strony zamawiającego);

- budżet niezbędny do przeprowadzenia prac umownych na wymaganym poziomie jakości oraz, w razie potrzeby, jego podział, najczęściej w odniesieniu do etapów finansowania przedsięwzięcia;
- środki materialne – w przypadku audytu bezpieczeństwa teleinformatycznego głównie narzędzia programowe (np. skanery różnego typu) niezbędne do realizacji zadań audytowych.

W dalszej części artykułu jest przedstawiona propozycja wykonania oszacowań czasów wykonywania czynności wyspecyfikowanych w metodyce LP-A przeprowadzania audytu bezpieczeństwa teleinformatycznego [1], [2]. Podstawowe etapy procesu oszacowania, przedstawione w kolejnych rozdziałach, to:

1) przyjęcie konkretnej techniki opisu struktury projektu i wykonanie wykresu sieciowego dla metodyki LP-A,
2) zidentyfikowanie ograniczeń i przyjęcie założeń upraszczających,
3) oszacowanie czasów poszczególnych czynności w metodyce LP-A,
4) zidentyfikowanie ścieżki krytycznej na wykresie sieciowym,
5) oszacowanie czasu wykonania audytu.

Otrzymane w wyniku realizacji wymienionych punktów dane mogą stanowić podstawę dalszych oszacowań, np. zaangażowania zasobów.

2. PERT – technika opisu struktury projektu

Z technik opisu struktury projektu takich jak np. CPM (*ang. Critical Path Method* – metoda ścieżki krytycznej), MPM (*fr. Metra Potential Méthode*) oraz PERT (*ang. Program Evaluation and Review Technique*), do niniejszego artykułu została wybrana technika PERT. Technika ta wykorzystuje dwupunktowe modele sieciowe, tj. takie, w których czynności są reprezentowane za pomocą łuków grafu a zdarzenia za pomocą węzłów grafu.

Podstawowe etapy techniki PERT to:

- specyfikacja projektu i przygotowanie analizy jego struktury,
- określenie zależności pomiędzy poszczególnymi czynnościami wchodzącymi w skład projektu,
- sporządzenie wykresu sieciowego dla projektu,

- przypisanie poszczególnym czynnościom zakładanego czasu ich realizacji: optymistycznego, realnego, pesymistycznego,
- obliczenie oczekiwanego czasu wykonania czynności i odchylenia standardowego,
- określenie ścieżki krytycznej,
- analiza i zastosowanie praktyczne otrzymanych wyników.

Technika PERT daje możliwość statystycznego oszacowania czasu trwania poszczególnych czynności, co umożliwia wskazanie prawdopodobieństwa zrealizowania poszczególnych etapów projektu w założonych terminach[2]. Inne, wskazywane w literaturze [3], [4] zalety techniki PERT to:

- identyfikacja ścieżki krytycznej wskazuje na czynności wymagające szczególnej uwagi z punktu widzenia realizacji projektu,
- możliwość łatwego przypisania odpowiedzialności za poszczególne etapy projektu dzięki przejrzystemu wykresowi sieciowemu,
- możliwość sprawdzenia w dowolnym momencie projektu, czy projekt przebiega zgodnie z harmonogramem, czy jest opóźniony i czy może być wykonany z wyprzedzeniem.

W odmianie PERT-COST dodatkowo:

- w dowolnym momencie projektu możliwe jest sprawdzenie, czy dotychczas wydatkowane środki są zgodne z założeniami budżetu projektu,
- istnieje możliwość badania podczas realizacji projektu, czy posiadane zasoby są wystarczające do zakończenia projektu w terminie,
- w przypadku konieczności zakończenia projektu przed założonym terminem istnieje możliwość określenia, jak osiągnąć ten cel najniższym kosztem.

Formalnie sieć PERT musi być unigrafem skierowanym nie zawierającym dróg cyklicznych [3]. Ponieważ czynności, które technologicznie mogą być realizowane równolegle w czasie mogą spowodować że graf stanie się multigrafem, w sieciach PERT, w celu uniknięcia tego problemu, wprowadza się tzw. czynności pozorne o zerowym czasie trwania (na rys.1 i 2 łuki tych czynności są narysowane linią przerywaną) oraz dodatkowe węzły-zdarzenia. Dodatkowym postulatem jest istnienie dokładnie jednego węzła początkowego (bez poprzedników) i jednego węzła końcowego (bez następników) reprezentującego zdarzenie będące zakończeniem realizacji przedsięwzięcia [4].

[2] Jest to zatem jeden z elementów „zapewniania zaufania zamawiającego", o którym pisze się w PQP.

Jedną z głównych czynności w technice PERT jest **wyznaczenie ścieżki krytycznej**, tj. takiej ścieżki, którą tworzy ciąg czynności o najmniejszej rezerwie czasu łączący węzeł początkowy z końcowym. Zatem niezbędne w technice PERT jest:

- dokładne zdefiniowanie wszystkich zadań i czynności składających się na przedsięwzięcie projektowe (tutaj: wyznaczone w ramach metodyki LP-A), jednoznacznie wskazujących zakończenie projektu;
- w ramach poszczególnych ścieżek niezależność zadań i czynności: mogą być rozpoczynane, zatrzymywane i realizowane oddzielnie,
- uporządkowanie zadań i czynności (ustalenie kolejności).

Fakt skupiania się w technice PERT na ścieżce krytycznej w niektórych przypadkach może być przyczyną błędów – zawęża bowiem obszar analizy do jednej z wielu możliwych ścieżek realizacji projektu. Jeżeli czasy przejścia niektórych ścieżek niewiele różnią się od siebie, a szacowany czas wykonania poszczególnych czynności obarczony jest dużym odchyleniem standardowym, to może się okazać, że to inne ścieżki staną się ścieżkami krytycznymi. PERT bowiem korzysta z modeli losowych i nie można wskazać żadnej ścieżki krytycznej z całkowitą pewnością [3].

3. Wykresy sieciowe i zarys metody oszacowania czasów czynności

Wykres sieciowy dla metodyki LP-A został zbudowany drogą transformacji zamieszczonych w opisie metodyki (por. [1], [2]) diagramów przepływu danych (DFD), w których procesy zostały zamienione na czynności (por. tab. 1) i odwzorowane na łuki wynikowej sieci PERT.

Tabela 1 jest zbudowana na podstawie tabeli *„Zakresy odpowiedzialności i nadzoru procesów audytu”* zamieszczonej w [1] i [2]. Modyfikacji uległy jedynie początkowe wiersze tabeli, gdzie procesy 1.1–1.4 zostały scalone w czynność 1.# o nazwie „ustalenia wstępne”. Po prawej stronie tabeli powinien być podany dla każdej czynności czas jej wykonania.

Czas ten to w rzeczywistości wielkość losowa. W metodzie PERT wprowadza się pojęcie czasu optymistycznego t_a, czasu realnego t_m i czasu pesymistycznego t_b, gdzie:

- optymistyczny (t_a) – jest to najkrótszy, możliwy w praktyce, termin ukończenia danej czynności[3];

[3] Zwykle postuluje się (por. np. [4]), żeby czas ten był ustalony tak, aby prawdopodobieństwo, że czynność zostanie ukończona w krótszym czasie, nie przekraczało 0,01.

- realny (t_m) – jest to najpewniejszy w praktyce termin ukończenia danej czynności;
- pesymistyczny (t_b) – jest to najpóźniejszy, dopuszczalny w praktyce, termin ukończenia danej czynności[4].

Te trzy czasy, które powinny być podane przez ekspertów dziedzinowych (tutaj: doświadczonych audytorów pracujących według metodyki LP-A), służą do wyznaczenia czasu oczekiwanego t_{en} czynności n oraz odchylenia standardowego σ_n. W metodzie PERT (por. np. [3], [4]) wzory do obliczenia tych wielkości są następujące:

$$t_{en} = \frac{t_{an} + 4t_{mn} + t_{bn}}{6} \qquad \sigma_n = \frac{t_{bn} - t_{an}}{6} \quad \text{gdzie:}$$

- t_{an} to optymistyczny czas ukończenia czynności n;
- t_{mn} to realny czas ukończenia czynności n;
- t_{bn} to pesymistyczny czas ukończenia czynności n.

Zgodnie z tymi wzorami czas t_{en} jest średnią ważoną, w której największą wagę równą 4 przypisano do realnego czasu wykonania czynności, natomiast wagę równą 1 przypisano czasom: optymistycznemu i pesymistycznemu.

Uzasadnienie przyjęcia w metodzie PERT takiej a nie innej postaci wzoru do obliczenia czasu t_{en} jest następujące [4]: z praktyki zarządzania projektami wiadomo, że ze względu na zbytni optymizm w szacunkach[5], rzeczywiste czasy najczęściej przekraczają wartości podane jako realne.

Mając do dyspozycji wypełnioną tabelę 1 i wyznaczone ścieżki pełne (por. dalszą część niniejszego rozdziału) można wyznaczyć czasy realizacji tych ścieżek. Czasy te otrzymuje się, sumując czasy oczekiwane wykonania czynności składających się na daną ścieżkę pełną. Ścieżka pełna o najdłuższym czasie jest ścieżką krytyczną przedsięwzięcia audytowego, a uzyskany dla niej czas to czas oczekiwany T_e realizacji całego audytu.

Ponieważ czasy realizacji poszczególnych czynności, w tym czynności składających się na ścieżkę krytyczną, są obarczone niepewnością, to również oczekiwany czas realizacji całego audytu nie jest czasem pewnym. Z tego

[4] Zwykle postuluje się (por. np. [4]), żeby czas ten był ustalony tak, aby prawdopodobieństwo, że czynność zostanie ukończona w dłuższym czasie, nie przekraczało 0,01.

[5] Żeby „przebić" konkurencję uczestnicy przetargu, na przeprowadzenie prac (nie tylko) audytowych, często podają nierealne terminy wykonania pracy, nie mające nic wspólnego z omawianymi tutaj optymistycznymi szacunkami.

powodu w zastosowaniach praktycznych oblicza się zwykle odchylenie standardowe σ_{Te} czasu oczekiwanego T_e realizacji całego projektu (tutaj: audytu), zgodnie ze wzorem:

$$\sigma_{Te} = \sqrt{\sum \sigma_n^2}$$

Znając czas oczekiwany realizacji audytu oraz jego odchylenie standardowe, można obliczyć prawdopodobieństwo zakończenia audytu w dowolnym zadanym czasie $T_{\dot{z}}$. Algorytm postępowania umożliwiający obliczenie tego prawdopodobieństwa jest następujący:

1. Określenie żądanego czasu realizacji audytu $T_{\dot{z}}$ (np. na postawie zapisów oferty lub umowy).
2. Obliczenie parametru z będącego liczbą odchyleń standardowych między czasem żądanym $T_{\dot{z}}$ a oczekiwanym T_e realizacji audytu:

$$z = \frac{T_{\dot{z}} - T_e}{\sigma_{Te}}$$

3. Znalezienie na podstawie tabeli dystrybuanty rozkładu normalnego wartości prawdopodobieństwa odpowiadającej obliczonej wartości z.

Na wykresach sieciowych skonstruowanych dla metodyki LP-A i zamieszczonych na rys. 1 i rys. 2 można wskazać następujące pełne ścieżki czynności (dla lepszej czytelności do wyspecyfikowania ścieżek są używane są numery a nie symbole czynności – por. pierwsza kolumna tabeli 1):

a) dla wykresu na rysunku 1:

1. 1–2–4–7–9–10–11–28–29
2. 1–3–4–7–9–10–11–28–29
3. 1–2–5–7–9–10–11–28–29
4. 1–3–5–7–9–10–11–28–29
5. 1–2–6–7–9–10–11–28–29
6. 1–3–6–7–9–10–11–28–29
7. 1–2–4–8–9–10–11–28–29
8. 1–3–4–8–9–10–11–28–29
9. 1–2–5–8–9–10–11–28–29
10. 1–3–5–8–9–10–11–28–29
11. 1–2–6–8–9–10–11–28–29
12. 1–3–6–8–9–10–11–28–29
13. 1–2–12–13–14–15–16–17–27–28–29
14. 1–3–12–13–14–15–16–17–27–28–29
15. 1–2–12–18–19–20–21–22–23–24–26–27–28–29
16. 1–2–12–18–19–20–21–22–23–25–26–27–28–29

17. 1–3–12–18–19–20–21–22–23–24–26–27–28–29
18. 1–3–12–18–19–20–21–22–23–25–26–27–28–29

Biorąc pod uwagę fakt, że czynność oznaczona numerem 3 (seminarium) jest realizowana zwykle niezależnie od pozostałych czynności audytowych, zbiór ścieżek pełnych minimalizuje się do zbioru:

1. 1–2–4–7–9–10–11–28–29
2. 1–2–5–7–9–10–11–28–29
3. 1–2–6–7–9–10–11–28–29
4. 1–2–4–8–9–10–11–28–29
5. 1–2–5–8–9–10–11–28–29
6. 1–2–6–8–9–10–11–28–29
7. 1–2–12–13–14–15–16–17–27–28–29
8. 1–2–12–18–19–20–21–22–23–24–26–27–28–29
9. 1–2–12–18–19–20–21–22–23–25–26–27–28–29

b) dla wykresu na rysunku 2:

1. 1–2–4–7–9–10–11–28–29
2. 1–3–4–7–9–10–11–28–29
3. 1–2–5–7–9–10–11–28–29
4. 1–3–5–7–9–10–11–28–29
5. 1–2–6–7–9–10–11–28–29
6. 1–3–6–7–9–10–11–28–29
7. 1–2–4–8–9–10–11–28–29
8. 1–3–4–8–9–10–11–28–29
9. 1–2–5–8–9–10–11–28–29
10. 1–3–5–8–9–10–11–28–29
11. 1–2–6–8–9–10–11–28–29
12. 1–3–6–8–9–10–11–28–29
13. 1–2–12–13–17–27–28–29
14. 1–2–12–14–17–27–28–29
15. 1–2–12–15–17–27–28–29
16. 1–2–12–16–17–27–28–29
17. 1–3–12–13–17–27–28–29
18. 1–3–12–14–17–27–28–29
19. 1–3–12–15–17–27–28–29
20. 1–3–12–16–17–27–28–29
21. 1–2–12–18–22–23–24–26–27–28–29
22. 1–3–12–18–22–23–24–26–27–28–29
23. 1–2–12–18–22–23–25–26–27–28–29
24. 1–3–12–18–22–23–25–26–27–28–29

25. 1–2–19–20–21–22–23–24–26–27–28–29
26. 1–3–19–20–21–22–23–24–26–27–28–29
27. 1–2–19–20–21–22–23–25–26–27–28–29
28. 1–3–19–20–21–22–23–25–26–27–28–29

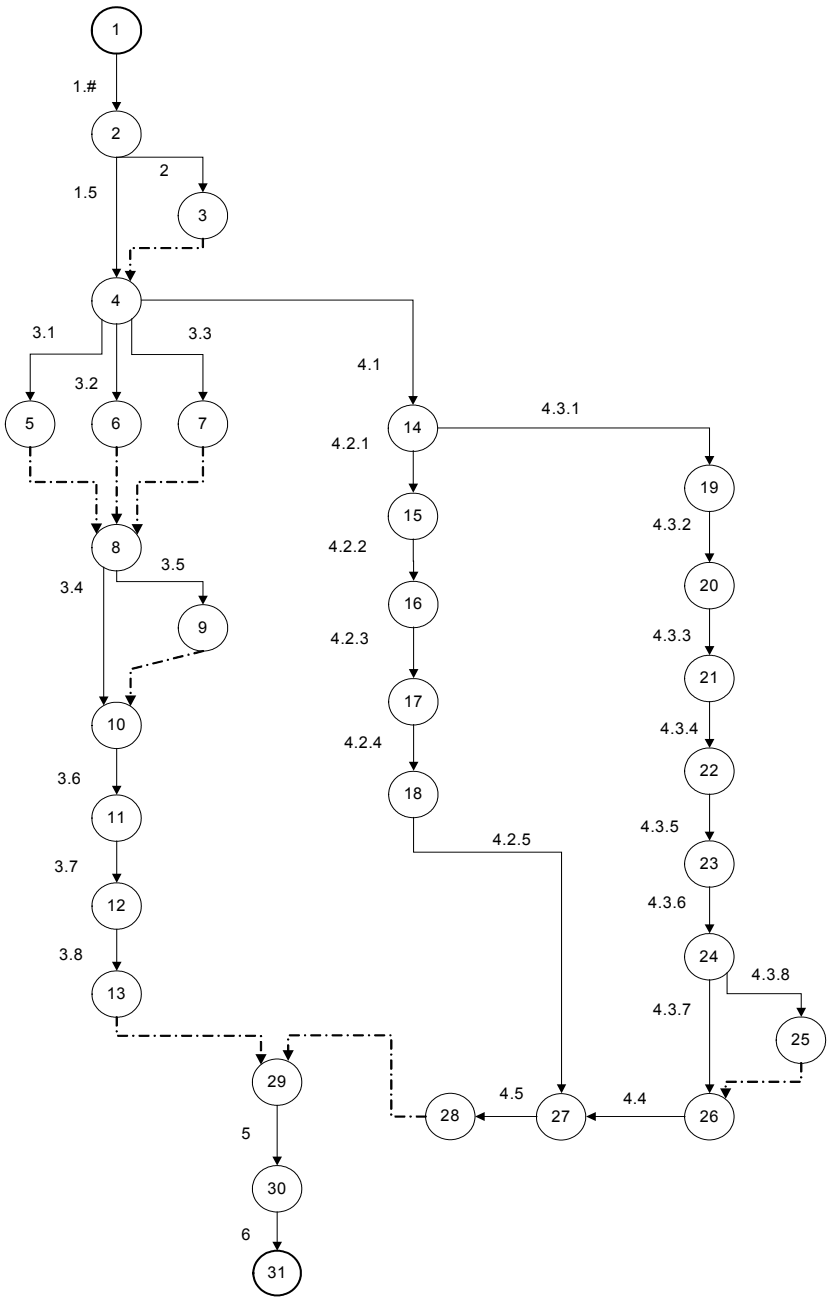
Biorąc pod uwagę fakt, że czynność oznaczona numerem 3 (seminarium) jest realizowana zwykle niezależnie od pozostałych czynności audytowych, zbiór ścieżek pełnych (podobnie jak w poprzednim przypadku) minimalizuje się do zbioru:

1. 1–2–4–7–9–10–11–28–29
2. 1–2–5–7–9–10–11–28–29
3. 1–2–6–7–9–10–11–28–29
4. 1–2–4–8–9–10–11–28–29
5. 1–2–5–8–9–10–11–28–29
6. 1–2–6–8–9–10–11–28–29
7. 1–2–12–13–17–27–28–29
8. 1–2–12–14–17–27–28–29
9. 1–2–12–15–17–27–28–29
10. 1–2–12–16–17–27–28–29
11. 1–2–12–18–22–23–24–26–27–28–29
12. 1–2–12–18–22–23–25–26–27–28–29
13. 1–2–19–20–21–22–23–24–26–27–28–29
14. 1–2–19–20–21–22–23–25–26–27–28–29

Z założeń metodycznych LP-A dotyczących składu zespołu audytowego [1], [2] wynika, że możliwe jest zrównoleglenie prac ścieżek: formalnej, badań technicznych i badań teleinformatycznych, co zostało uwidocznione na obu wykresach sieciowych. Natomiast zrównoleglenie wykonania prac składających się na ścieżkę (wymaga to modyfikacji prezentowanego modelu sieciowego) jest dyskusyjne, ponieważ zwykle np. badania wyrywkowe konfiguracji i pozostałe badania sieci teleinformatycznych wykonuje ta sama ekipa ekspertów – rzadko udaje się zgromadzić na tyle liczny zespół o wysokich kwalifikacjach, żeby można zrównoleglić prowadzenie badań.

Tabela 1. Przypisanie poszczególnym czynnościom metodyki LP-A czasu ich realizacji

Numer (symbol) czynności	Opis czynności	Szacunki czasów		
		t_a	t_m	t_b
1 (1.#)	ustalenia wstępne			
2 (1.5)	opracowanie harmonogramu			
3 (2)	seminarium			
4 (3.1)	zebranie i analiza dokumentacji o porządku prawnym			
5 (3.2)	zebranie i analiza dokumentacji o zależnościach z podmiotami zewnętrznymi			
6 (3.3)	przekazanie ankiet do wypełnienia			
7 (3.4)	wizje lokalne i wywiady			
8 (3.5)	zebranie i analiza ankiet			
9 (3.6)	uzupełnianie ankiet			
10 (3.7)	opracowanie ankiet			
11 (3.8)	wykonanie raportu o zgodności z normą ISO/IEC 17799			
12 (4.1)	analiza dokumentacji technicznej			
13 (4.2.1)	przegląd zabezpieczeń F–T			
14 (4.2.2)	przegląd systemu zasilania			
15 (4.2.3)	pomiar emisji ujawniającej			
16 (4.2.4)	poszukiwanie podsłuchów			
17 (4.2.5)	analiza notatek wewnętrznych Zespołu			
18 (4.3.1)	wyrywkowe badania konfiguracji			
19 (4.3.2)	badanie podatności (zautomatyzowane)			
20 (4.3.3)	badanie konfiguracji (zautomatyzowane)			
21 (4.3.4)	badanie uaktualnień (zautomatyzowane)			
22 (4.3.5)	analiza wyników badań sieci teleinformatycznych			
23 (4.3.6)	ręczne testy penetracyjne			
24 (4.3.7)	aktualizacja wykazu podatności			
25 (4.3.8)	inwentaryzacja zasobów (zautomatyzowana)			
26 (4.4)	przekazanie informacji o podatnościach			
27 (4.5)	wykonanie raportu z badań technicznych			
28 (5)	opracowanie dokumentu końcowego audytu			
29 (6)	przekazanie wyników audytu Zleceniodawcy			



Rys.1. Wykres sieciowy czynności bez zrównoleglenia prac (ograniczone zasoby) dla metodyki LP-A

Ta sama uwaga dotyczy zaznaczonej na rys. 2 możliwości zrównoleglenia prowadzonych prac w lokalizacjach w przypadku np. audytu organizacji składającej się z Centrali i rozproszonych po całej Polsce filii. Oznacza to, że w praktyce czas T_{tel} audytu dla ścieżki badań sieci teleinformatycznych należy pomnożyć przez n, gdzie n jest liczbą podlegających audytowi lokalizacji, czyli że badania w lokalizacjach odbywają się szeregowo a nie równolegle. Z przedstawionych względów, dalszej analizie zostanie poddany wykres sieciowy na rys. 1, czyli ścieżka krytyczna będzie poszukiwana w zbiorze dziewięciu ścieżek pełnych.

4. Klasyfikacja czynności i wzorce chronometrażowe

Przedstawione dotąd rozważania dają schemat postępowania dla określania czasu całkowitego audytu przy wykorzystaniu *ocen ekspertów* dotyczących czasów realizacji poszczególnych czynności audytowych, tj. czasów wpisywanych w kolumny t_a, t_m, t_b tabeli 1. Żeby móc rzetelnie podać te czasy, eksperci powinni dysponować odpowiednim materiałem empirycznym zgromadzonym podczas wykonywania audytów.

Rysunek 3 przedstawia propozycję budowy arkusza do zapisu empirycznych danych o czasach realizacji poszczególnych czynności audytowych. Pod tabelą na rys. 3 w „Uwagach" podane są przyjęte arbitralnie oceny opisowe i odpowiadające im oceny punktowe dla najważniejszych, związanych z głównymi ścieżkami schematu sieciowego metodyki, czynników mających wpływ na czas realizacji czynności audytowych. Czynniki te nazywane są dalej atrybutami.

Dla audytów prowadzonych zgodnie z metodyką LP-A można wyróżnić następujące klasy czynności:

1. **Klasa F** – dla ścieżki formalnej.

   Są to czynności: 1.5, 3.1, 3.2, 3.4, 3.5, 3.8, 3.7

   Na czas realizacji czynności ma wpływ:

   a) stopień zaangażowania (chęć do współpracy) pracowników audytowanej organizacji, przede wszystkim konsultantów;

   b) złożoność struktur organizacyjnych audytowanej organizacji, wpływająca na:

      - czas potrzebny audytorom na „nauczenie się" badanej organizacji;
      - łatwość identyfikacji informatorów, respondentów ankiet;

- ilość niezbędnych wywiadów oraz wizji lokalnych;
- ilość ankiet do opracowania i sam proces ankietowania (w tym w razie potrzeby szkoleń respondentów).

2. **Klasa BT** – dla ścieżki badań technicznych.

   Są to czynności: 4.1, 4.2.1, 4.2.2, 4.2.3, 4.2.4

   Na czas realizacji czynności ma wpływ:

   a) złożoność struktur organizacyjnych audytowanej organizacji i poszczególnych obiektów, w szczególności liczby pomieszczeń i stref;
   b) kompletność i jakość dostarczonej dokumentacji;
   c) ilość obiektów wymagających przeprowadzenia czynności 4.2.3 (pomiar emisji ujawniającej) i 4.2.4 (poszukiwanie podsłuchów);
   d) dostępność obiektów i systemów do przeprowadzenia badań wymienionych w punkcie c (np. tylko w jeden dzień w tygodniu).
   e) stopień zaangażowania (chęć do współpracy) pracowników audytowanej organizacji;

3. **Klasa BTE** – dla ścieżki badań teleinformatycznych.

   Są to czynności: 4.1, 4.3.1, 4.3.2, 4.3.3, 4.2.4, 4.3.5, 4.3.6, 4.3.7, 4.3.8

   Na czas realizacji czynności ma wpływ:

   a) stopień zaangażowania (chęć do współpracy) pracowników odpowiedzialnych za audytowane obiekty;
   b) złożoność struktury sieci teleinformatycznej i stref administracyjnych (odpowiedzialności) w tej sieci;
   c) kompletność i jakość dostarczonej dokumentacji technicznej;
   d) liczność skanowanego/sprawdzanego zbioru elementów;
   e) możliwość wyodrębnienia klas podobnych obiektów badanych, dla których badanie może zostać zrealizowane drogą badania reprezentantów;
   f) w przypadku badań automatycznych (np. skanerami bezpieczeństwa), strategia i głębokość badania poszczególnych elementów (np. pełen przegląd potencjalnych podatności wszystkich obiektów lub, dla poszczególnych klas obiektów, mniej czasochłonne przeglądy specyficznych podatności);
   g) dostępności obiektów i systemów do badań (np. tylko w jeden dzień w tygodniu).

4. **Klasa O** – czynności organizacyjne.

   Są to czynności: 1.#, 2, 3.8, 4.2.5, 4.4., 4.5, 5, 6

Na czas realizacji czynności ma wpływ:

a) przestrzeganie ustalonych i zapisanych w PQP procedur współpracy, w szczególności kompletność i terminowość dostarczenia przez audytowaną organizację wymaganej dokumentacji;
b) złożoność struktur organizacyjnych audytowanej organizacji i poszczególnych obiektów
c) stopień formalnej organizacji prac zespołu audytowego (ustalone standardy dokumentacyjne, procedury obiegu informacji, itp.)

Z analizy przedstawionych klas oraz zebranych podczas realizacji audytów bezpieczeństwa teleinformatycznego doświadczeń wynika, że na szczególną uwagę zasługują trzy atrybuty:

1) atr_1 – złożoność struktur organizacyjnych audytowanej organizacji i poszczególnych obiektów
2) atr_2 – kompletność i jakość dostarczonej dokumentacji
3) atr_3 – dostępności obiektów i systemów do badań.

Dane pokazujące wpływ tych atrybutów na czas całkowity audytu powinno się uzyskać na podstawie opracowania materiału empirycznego zebranego podczas audytów (por. tabela na rys. 3). Docelowo powinno się uzyskać dane do wpisania do kolumny (4) tabeli 2.

Pojawia się tutaj niestety poważna trudność – żeby dane były wiarygodne, nie można poprzestać na danych zebranych podczas jednego audytu. Dla wyznaczenia średnich czasów na zadowalającym poziomie wiarygodności liczba przeprowadzonych audytów, z których zebrano dane empiryczne, powinna wynosić co najmniej kilkanaście dla każdej wyróżnionej w tabeli 2 kombinacji[6].

Zawartość tabeli 2 to **wzorce chronometrażowe** dla metodyki LP-A, pozwalające na szybkie i w miarę precyzyjne oszacowanie czasu realizacji audytu jedynie na podstawie trzech wyodrębnionych tutaj atrybutów. Dysponowanie taką możliwością jest szczególnie pożądane podczas negocjacji oferty z zainteresowanym klientem, gdy dane o audytowanym obiekcie są stosunkowo skąpe i jednocześnie żąda się podania przez wykonawcę w miarę realnych czasów realizacji przedsięwzięcia. Dotychczasowe doświadczenia wskazują, że maksymalny czas realizacji audytu powinno się uzyskać dla kombinacji atrybutów z poz. 9 tabeli, a minimalny – kombinacji z poz. 19 (w tabeli 2 odpowiednie wpisy zostały wykonane pogrubioną kursywą).

[6] Dyskusja formalnego ujęcia problemu ilości wymaganych danych empirycznych do prognozowania czasów na zadanym poziomie ufności będzie przedmiotem odrębnego artykułu.

Średnie czasy audytu dla zadanej kombinacji atrybutów (tj. wartości do wpisania do kolumny (4) tabeli 2) można uzyskać na dwa sposoby:

1) uśredniając czasy z komórki *„Czas całkowity audytu”* tabeli na rys. 3;
2) uśredniając czasy każdej czynności audytowej i wyznaczając czas ścieżki krytycznej – czas ten będzie czasem realizacji audytu.

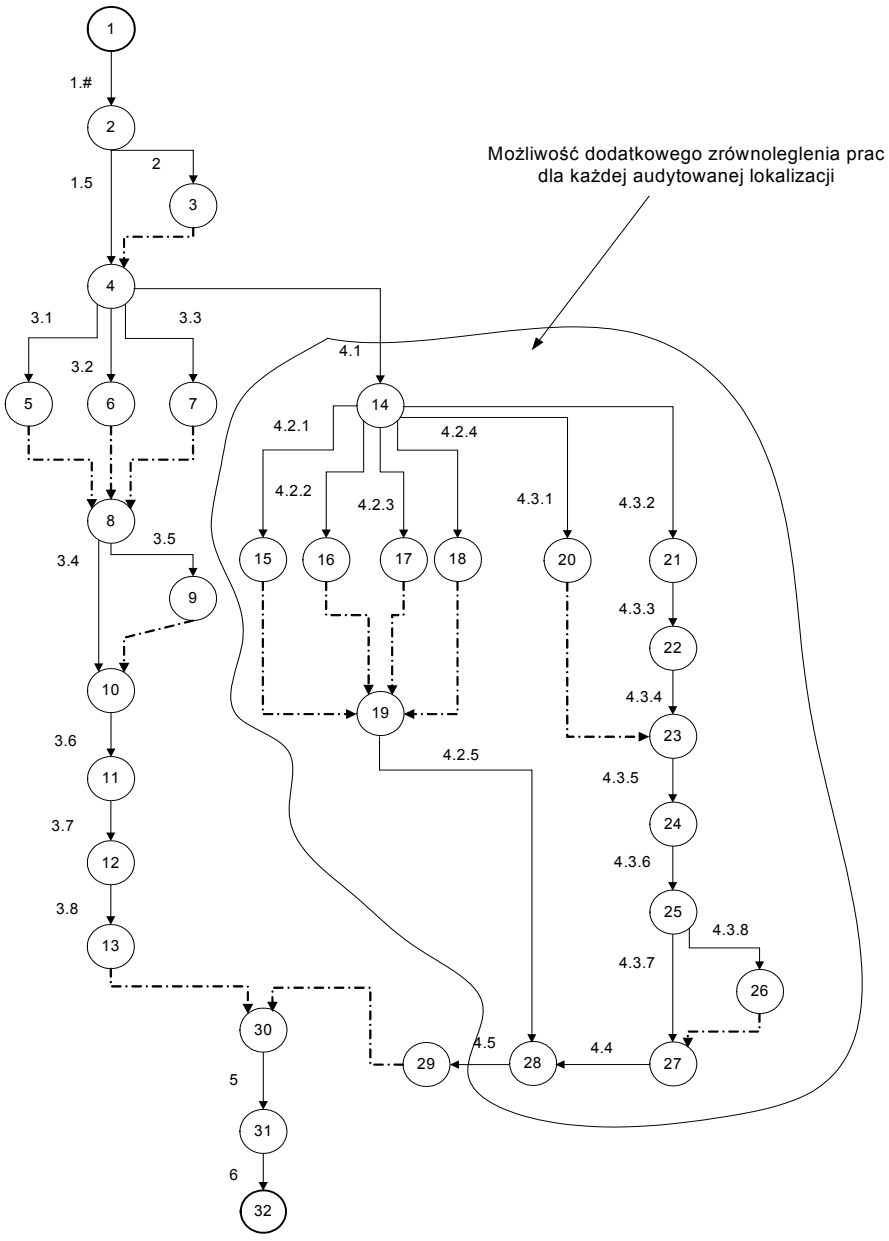
Precyzyjniejsze dane uzyskuje się dla drugiego przypadku. Wymaga on zbudowania dla każdej z wyodrębnionych 29 czynności audytowych (por. tab.1) tabeli analogicznych do tabeli 2 – w kolumnie (4) będą się wtedy znajdowały uśrednione czasy realizacji tych czynności w zależności od kombinacji trzech atrybutów[7]. Mając do dyspozycji takie czasy, można na wykresie sieciowym wyznaczyć ścieżkę krytyczną dla konkretnego typu (ze względu na atrybuty) audytu.

Kolejną trudnością jest zagwarantowanie powtarzalności warunków wykonywania pomiarów i dokładności podawania czasów czynności audytowych. Występujące w tym zakresie problemy to między innymi:

- czy np. czynność 4.3.1 *„wyrywkowe badania konfiguracji”* należy uznać za zakończoną w momencie wykonania przez eksperta ostatniego sprawdzenia na ostatnim poddawanym kontroli zasobie, czy też w momencie złożenia przez eksperta pisemnego sprawozdania z badań?
- czy otrzymane czasy będą takie same, jeżeli tę samą czynność w tych samych warunkach będą wykonywali różni eksperci (pojawia się tutaj problem różnego poziomu kwalifikacji i doświadczenia, a nawet zdolności adaptacyjnych ekspertów do różnych środowisk)?
- jaką przyjąć ziarnistość i jednostki pomiaru czasu: roboczogodziny, roboczodni (osiem godzin pracy eksperta?), osobodni i godziny, czas w jednostkach bezwzględnych?
- jak uwzględniać tzw. czasy logistyczne: przejazdu do miejsca badań, przesyłania wyników, edycji dokumentów pośrednich itd.?

Aby usunąć lub przynajmniej zminimalizować wymienione trudności, należy opracować metodykę zbierania danych chronometrażowych, gdzie zostałby zawarty szczegółowy algorytm postępowania dla osoby (lub osób) zbierającej te dane oraz zostałyby racjonalnie wybrane ujednolicone jednostki i metody pomiarowe.

[7] Docelowo zatem dokument „Wzorce chronometrażowe” powinien zawierać 30 tabel.



Rys. 2. Wykres sieciowy czynności ze zrównolegleniem prac dla metodyki LP-A

Nazwa audytu:			
Stopień złożoności audytowanej organizacji	1	2	3
Kompletność i jakość dostarczonej dokumentacji	1	2	3
Dostępność do badań obiektów i systemów audytowanej organizacji	1	2	3

Lp.	Numer/symbol czynności	Czas
1		
2		
3		
.....		

Data podpisania umowy:	Data odbioru pracy:	Czas całkowity audytu:
Arkusz wypełnił:		

Uwagi:

1. Czas jest podawany w roboczogodzinach (uwaga: roboczogodziny dotyczą zespołu ekspertów wykonujących opisywaną czynność – nie mylić z osobogodzinami!).
2. Dostępność do badań podawana jest trójstopniowo:
   1) **całkowita,** ocena punktowa 1 – oznacza, że audytowana organizacja nie nakłada ograniczeń
   2) **ograniczona,** ocena punktowa 2 – oznacza nałożenie ograniczeń przez audytowaną organizację na terminy badań
   3) **weekendy,** ocena punktowa 3 – oznacza dostępność obiektów do badań wyłącznie w weekendy.
3. Stopień złożoności audytowanej organizacji jest określany trójstopniowo:
   1) **wysoki,** ocena punktowa 3 – gdy efekt skali przejawia się co najmniej w dwóch wymiarach (np. duża liczba komputerów i rozproszenie terytorialne)
   2) **średni,** ocena punktowa 2 – gdy efekt skali dotyczy tylko jednego wymiaru
   3) **niski,** ocena punktowa 1 – nie występuje efekt skali.
4. Kompletność i jakość dostarczonej dokumentacji określana jest trójstopniowo:
   1) **zadowalająca,** ocena punktowa 1 – dostępna jest pełna i aktualna dokumentacja stanu przedmiotu audytu (rzeczywistego, pożądanego i ustanowionych reguł): organizacyjna (w tym prawna), techniczna, ewidencyjna itd.;
   2) **dostateczna,** ocena punktowa 2 – dokumentacja posiada niewielkie, łatwe do uzupełnienia braki;
   3) **niedostateczna,** ocena punktowa 3 – oznacza brak aktualnej dokumentacji lub szczątkową dokumentację. W praktyce oznacza to, że zespół audytorów w celu rzetelnego przeprowadzenia badań musi samodzielnie taką dokumentację wytworzyć lub skompletować.
5. Jako czas całkowity audytu należy podać czas pomiędzy dniem podpisania umowy a dniem odbioru przez klienta wyników audytu (zwykle nie odpowiada on czasowi będącemu sumą czasów poszczególnych czynności).

Rys. 3. Przykładowy arkusz zbierania danych do charakterystyk chronometrażowych audytu

Tabela 2. Średnie czasy audytu w zależności od kombinacji atrybutów procesu audytu.

Nr	Stopień złożoności audytowanej organizacji (1)	Kompletność i jakość dostarczonej dokumentacji technicznej (2)	Dostępność do badań obiektów audytowanej organizacji (3)	Średni czas audytu (4)
1	wysoki	zadowalająca	całkowita	
2	wysoki	zadowalająca	ograniczona	
3	wysoki	zadowalająca	weekendy	
4	wysoki	dostateczna	całkowita	
5	wysoki	dostateczna	ograniczona	
6	wysoki	dostateczna	weekendy	
7	wysoki	niedostateczna	całkowita	
8	wysoki	niedostateczna	ograniczona	
9	***wysoki***	***niedostateczna***	***weekendy***	
10	średni	zadowalająca	całkowita	
11	średni	zadowalająca	ograniczona	
12	średni	zadowalająca	weekendy	
13	średni	dostateczna	całkowita	
14	średni	dostateczna	ograniczona	
15	średni	dostateczna	weekendy	
16	średni	niedostateczna	całkowita	
17	średni	niedostateczna	ograniczona	
18	średni	niedostateczna	weekendy	
19	***niski***	***zadowalająca***	***całkowita***	
20	niski	zadowalająca	ograniczona	
21	niski	zadowalająca	weekendy	
22	niski	dostateczna	całkowita	
23	niski	dostateczna	ograniczona	
24	niski	dostateczna	weekendy	
25	niski	niedostateczna	całkowita	
26	niski	niedostateczna	ograniczona	
27	niski	niedostateczna	weekendy	

5. Podsumowanie

W artykule przedstawiono zarys metody prognozowania czasu wykonania audytu bezpieczeństwa teleinformatycznego prowadzonego według metodyki LP-A. Obecnie zbierane są, zgodnie z przedstawionym w tym artykule schematem postępowania, dane empiryczne z audytów. Już jednak tylko na podstawie przeprowadzonych rozważań można wyciągnąć pewne praktyczne wnioski.

Po pierwsze, sama metodyka audytu (tutaj: LP-A) nie wystarcza do rzetelnego podania *prognozowanych* czasów realizacji audytu i, w szczególności, pojedynczych czynności audytowych. Do tego celu niezbędne jest posiadanie przez Zespół Audytowy danych empirycznych ze zrealizowanych według zadanej metodyki audytów.

Po drugie, ze względu na niepowtarzalność przedsięwzięć audytowych, należy wyabstrahować takie cechy przedsięwzięcia audytowego (co zrobiono w rozdz. 4), które będą mogły być uznane za podstawowe i wspólne cechy audytu bezpieczeństwa teleinformatycznego dla dowolnej firmy.

Po trzecie, sam proces zbierania danych empirycznych w zakresie czasów realizacji poszczególnych czynności audytowych wymaga usystematyzowanego, metodycznego podejścia, ponieważ przy braku takowego nie zapewni się porównywalności otrzymanych wyników.

Przedstawiona w artykule problematyka i związane z nią trudności praktyczne skłaniają do przyjmowania z dużą dozą nieufności oszacowań wymaganych czasów realizacji audytu, zamieszczanych w ofertach na przeprowadzenie audytu z zakresu bezpieczeństwa teleinformatycznego. Trudności te powinny, zgodnie z dobrą praktyką inżynierską, skłonić potencjalnego zleceniodawcę do zapytania oferenta, w jaki sposób zostały wykonane przedstawione mu oszacowania.

Literatura:

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

[2] Liderman K.: *Podręcznik administratora bezpieczeństwa teleinformatycznego*. MIKOM. Warszawa. 2003. ISBN 83–7279–377–8.

[3] Korzan B .: *Elementy teorii grafów i sieci. Metody i zastosowania*. WNT. Warszawa. 1978.

[4] Trocki M. i in.: *Zarządzanie projektami*. PWE. Warszawa. 2003. ISBN 83–208–1429–4.

Recenzent: prof. dr hab. inż. Włodzimierz Kwiatkowski

Praca wpłynęła do redakcji 20.11.2004.