Metodyka LP-A – dziesięć lat później

Krzysztof LIDERMAN, Adam E. PATKOWSKI

Instytut Teleinformatyki i Automatyki WAT,
ul. Gen. S. Kaliskiego 2, 00-908 Warszawa
lider@ita.wat.edu.pl, aep@ita.wat.edu.pl

STRESZCZENIE: Artykuł jest próbą podsumowania „życia" metodyki LP-A w okresie minionych dziesięciu lat. Zawiera także ocenę aktualności metodyki i jej użyteczności we współczesnych warunkach. Uzasadniono wnioski o pomyślnym przejściu próby czasu przez metodykę oraz podstawy do zachowania jej obecnego kształtu. Zaprezentowano także współczesne wyzwania wobec metodyki wynikające ze zmian technologii.

SŁOWA KLUCZOWE: audyt, metodyka, ochrona informacji, zabezpieczenia

1. Wprowadzenie

W 2003 roku została opublikowana [16] metodyka LP-A prowadzenia audytu z zakresu bezpieczeństwa teleinformatycznego. Powstała ona na podstawie ponad dekady doświadczeń nieformalnego zespołu audytowego realizującego zamówienia różnych zleceniodawców, zwykle w jakimś stopniu dotyczące bezpieczeństwa. Praktycznie w każdym zleceniu występował element oceny bezpieczeństwa – realizowanej jako główne zadanie, gdy zlecenie dotyczyło audytu, albo jako element większej całości, gdy zamawiana była jakaś wersja „systemu bezpieczeństwa". Doświadczenia te wykazały, że prace prowadzące do oceny (zmierzające do jednoznacznego rozpoznania „stanu rzeczy") dość wyraźnie można było podzielić na badania „papierowe", dotyczące ludzi oraz regulaminów i zarządzeń, oraz na badania techniczne. Oczywiście zawsze dla ustalenia zakresu prac istotny był wzorzec, na zgodność z którym dokonywano oceny.

Zwykle jednym z najtrudniejszych problemów okazywała się komunikacja ze zleceniodawcą, który nienajlepiej orientował się, co może być wzorcem i jak należy go rozumieć. Od 2003 roku sytuacja w tej mierze się

poprawiła: wydana została pierwsza wersja normy PN-ISO/IEC 17799:2003, a przede wszystkim została ona mocno rozreklamowana.

Należy przypomnieć, że na początku obecnego wieku, do „bezpieczeństwa" przeszło wielu audytorów jakości, co wynikało z kurczącego się rynku i końca mody na ISO 9000 – duże i średnie firmy nabyły już tę usługę i certyfikat ISO 9000 przestał dawać przewagę marketingową. Wielu wysokiej klasy specjalistów w dziedzinie audytu zmieniło branżę. Niestety[1], większość z nich nie miała wykształcenia politechnicznego, a nawet informatycznego, co zaowocowało znaczną ofertą „papierowych" audytów i ucieczką od badań technicznych.

Na szczęście w pierwszej dekadzie obecnego wieku również marketingowcy zainteresowali się certyfikatami bezpieczeństwa jako narzędziem zwiększania konkurencyjności, co wynikało z mody i okresowego zainteresowania opinii publicznej mało dla niej zrozumiałymi wyczynami „hakerów" i opisami „wirusów" nagłaśnianymi przez szukających sensacji dziennikarzy. Związek między sensacyjnymi opisami ewidentnie technicznych środków ataku a zainteresowaniem ocenami czysto organizacyjnych „papierowych" certyfikatów wydaje się nieco irracjonalny, ale wyraża się w bardzo konkretnych pieniądzach. Jednak firmy, których „core biznes" jest realizowany w procesach stricte teleinformatycznych, ostatnio składają zamówienia na usługi wyłącznie ocen technicznych – najczęściej tzw. testów penetracyjnych aplikacji webowych. Według ocen (niestety niepopartych rzetelnymi badaniami ani źródłami) autorów niniejszej publikacji to obecnie najczęściej występujące zamówienie na rynku.

Norma 17799 nie zawsze jest wzorcem do badań bezpieczeństwa. Niezależnie jednak od wzorca pozostaje problem uzgodnienia ze zleceniodawcą zakresu badań i sposobu prowadzenia prac. To uzgodnienie musi dotyczyć zarówno warstwy zarządczej, jak i wykonawczej (operacyjnej). O ile zwykle w zakresie zarządczym dość łatwo uzgodnić ze zleceniodawcą sposób działania, wybierając jedną z uznanych metodyk (ostatnio modna[2] jest PRINCE 2), o tyle w zakresie operacyjnym w 2003 roku brakowało metodyki pozwalającej uwzględnić również specyfikę badań technicznych stanu bezpieczeństwa systemów teleinformatycznych. Panaceum miała być opracowana przez autorów niniejszej publikacji metodyka LP-A. Podkreślić należy, że powstała ona przede wszystkim w celu ułatwienia komunikacji między zleceniodawcami-menedżerami a wykonawcami-specjalistami w dziedzinie bezpieczeństwa. Aby osiągnąć sukces w tym zakresie, metodyka musiała przede wszystkim zdobyć

[1] Dalej wyrażony sąd (podobnie jak za innymi słowami „niestety" w tym tekście) świadczy o stanie rzeczy zdaniem autorów niepożądanym lub niewłaściwym.

[2] Zdaniem autorów w wielu przypadkach wybór tej metodyki wynika z jej popularności i nieznajomości rozwiązań konkurencyjnych.

pewną minimalną popularność. Metodyka, opracowana na podstawie najlepszych doświadczeń praktycznych, okazała się potem również użytecznym narzędziem wykonawców.

W roku 2013 minie 10 lat od upublicznienia metodyki LP-A w pracach [19] i [16]. Wydaje się[3], że jest to wystarczający okres, aby spróbować podsumować to, co się w tym czasie z metodyką LP-A działo. Wyniki pobieżnej kwerendy w sieci Internet pokazują następujące fakty:

1. LP-A znalazła się w Wikipedii[4] oraz w Polskim Serwisie Naukowym [25] (hasło „audyt informatyczny").
2. Wiele firm informuje w upublicznianych materiałach o stosowaniu metodyki LP-A do audytu stanu ochrony informacji przetwarzanej w systemach teleinformatycznych zarówno własnych (COMP Rzeszów S.A. [27], Asseco Poland [1]), jak i obcych (SecuRing [15]).
3. Informacje o metodyce są upowszechniane na portalach o tematyce bezpieczeństwa informacyjnego [12], [14].
4. LP-A jest przedmiotem szkoleń prowadzonych przez różne firmy szkoleniowe i doradcze [11], [4].
5. Informacje o metodyce LP-A są włączane do wykładów z zakresu audytu bezpieczeństwa teleinformatycznego na uczelniach (m.in. AGH [10]).
6. LP-A jest prezentowana w publikacjach autorów innych niż twórcy metodyki (por. np. [21]).
7. LP-A jest cytowana i analizowana w rozprawie doktorskiej [8] i jest tematem prac dyplomowych magisterskich (np. na Uniwersytecie Ekonomicznym w Katowicach [13] czy też, co wydaje się oczywiste, w WAT [30]).
8. LP-A była prezentowana na konferencjach naukowych [2], [18].
9. LP-A była podstawą wystawiania certyfikatów bezpieczeństwa [5].

Informacje nt. metodyki LP-A są przekazywane także podczas wykładów prowadzonych przez jej autorów w WAT i na Politechnice Warszawskiej.

Można stwierdzić, że metodyka osiągnęła niezbędny poziom popularności, by być użyteczną w uzgadnianiu przedsięwzięć audytowych ze zleceniodawcami. Okazała się także skuteczna w realizacji prac. Należy podkreślić, że użytkownicy metodyki – ci, którzy wykorzystywali ją w praktyce – nie formułowali radykalnych propozycji zmian.

[3] Ten zwrot oznacza, że dalej wyrażona opinia w przekonaniu autorów jest słuszna, chociaż nie potrafią (lub nie chcą) przedstawić wyczerpujących argumentów na jej rzecz.

[4] Przedstawiona lista nie jest listą argumentów za czymkolwiek – to wynik przeglądu świadczący o obecności metodyki LP-A w świadomości publicznej. Właśnie obecność „na Wiki" świadczy o tym dobitnie.

2. Przegląd celów opracowania metodyki LP-A

Opublikowana w 2003 roku metodyka była wynikiem doświadczeń i potrzeb związanych z pracami prowadzonymi w tamtym czasie przez jej autorów. Metodyka została opracowana dla sprecyzowania i skrócenia dyskusji pomiędzy zleceniodawcą a potencjalnymi wykonawcami na temat „co jest do zrobienia" w pracach, w których zamówienie opiewało na „audyt bezpieczeństwa" lub „sprawdzenie stanu bezpieczeństwa" całości lub części systemu teleinformatycznego. Istotne cele takich przedsięwzięć zwykle mieściły się w spektrum od uzyskania certyfikatu zgodności po wskazanie braków czy niedoskonałości zabezpieczeń istniejącego systemu. Stwierdzono, że do efektywnego uzgadniania i prowadzenia przedsięwzięć audytowych jest niezbędne opracowanie metodyki, która wspomagałaby osiąganie następujących celów:

1. Opracowanie modelu referencyjnego prac dla rozmów pomiędzy wykonawcami a zleceniodawcami o sposobie realizacji audytu z zakresu bezpieczeństwa informacyjnego.
2. Usystematyzowanie przedsięwzięcia audytowego w zakresie wzajemnej kolejności realizowanych czynności audytowych.
3. Usystematyzowanie przedsięwzięcia audytowego w zakresie zarówno generowanych w jego trakcie, jak i niezbędnych do jego przeprowadzenia, dokumentów.
4. Osiągnięcie komunikatywności i adaptowalności przez wykorzystanie takich mechanizmów formalnych, które:
   - Byłyby zrozumiałe dla osób nie posiadających wiedzy informatycznej (np. nie znających notacji graficznych typu UML i zasad obiektowości). Z doświadczeń autorów wynika, że takie właściwości mają diagramy DFD i tablice IPO, które po krótkich wyjaśnieniach są zrozumiałe nawet dla laików.
   - Byłyby proste w użyciu, w szczególności nie wymuszały stosowania narzędzi skomputeryzowanych. Kółka i linie oraz proste tabele można rysować chociażby na serwetce, prowadząc rozmowę przy kawie.
   - Byłyby łatwo skalowalne. Pierwotna wersja metodyki, opublikowana w pracach [19] i [16] została rozwinięta do poziomu trzech diagramów DFD, ponieważ z doświadczeń autorów wynikało, że jest to wystarczający poziom szczegółowości do rozmów z kierownictwem i menedżerami potencjalnego zleceniodawcy audytu. Większy poziom szczegółowości zaciemnia obraz przedsięwzięcia audytowego szczegółami technicznymi menedżerom (zleceniodawcy), natomiast mniejszy poziom szczegółowości nie pozwala wykonawcom przedstawić

zleceniodawcy potencjalnych problemów wynikających ze skali przedsięwzięcia i zaangażowanych po stronie zleceniodawcy zasobów mających istotny wpływ na czas i koszty prac.

Co prawda audyt, czyli badanie zgodności z pewnym wzorcem, nie odpowiada bezpośrednio na pytanie „czy jest bezpiecznie", ale rzetelne jego przeprowadzenie zwykle wymaga określenia jakości poszczególnych zabezpieczeń i ich wdrożenia. Ocena tej jakości może być prowadzona różnorako, ale autorzy uznają techniczne badania bezpieczeństwa za podstawowy element takiej oceny[5].

Z doświadczeń autorów wynika, że w poważnych przedsięwzięciach, zmierzających w perspektywie do działań dla podniesienia bezpieczeństwa, prace nad określeniem „stanu rzeczy" dzielą się na dwa rodzaje, różniące się zarówno specyfiką podejścia, jak i wymaganiami wobec realizujących je wykonawców. Wyraźnie daje się wyodrębnić prace odpowiadające realizacji tzw. papierowego audytu, sprowadzające się do badań formalnych dokumentacji i wywiadów, a dostarczające oceny ustanowienia i zarządzania szeroko pojętym bezpieczeństwem. Ten rodzaj prac w metodyce ujęto jako tzw. ścieżkę formalną. Prace należące do tzw. ścieżki technicznej dotyczą problemów najczęściej trudno wyobrażalnych dla zarządu i audytorów bez wykształcenia politechnicznego. Obejmują techniczne badania stanu bezpieczeństwa, gdzie wzorcem są zalecenia producentów zabezpieczeń i dobra praktyka inżynierska. Można zauważyć, że podstawą powodzenia obu grup prac jest dobór do nich osób o odpowiednich kwalifikacjach – „urzędniczych" dla ścieżki formalnej i „technicznych" dla ścieżki technicznej[6]. Metodyka LP-A zakłada generowanie raportów z obu grup badań, scalanych na końcu przedsięwzięcia w podsumowujący raport zbiorczy. Intencją było uzyskanie podejścia systemowego i efektu synergii, co jest szczególnie ważne w obszarze badań technicznych.

Metodyka LP-A jest uniwersalna – pozwala na regulowanie zarówno zakresu badań (zależnie od obiektu badań oraz od wzorca audytowego), jak i ich wnikliwości (zwykle zależy to od środków przeznaczonych przez zleceniodawcę audytu na badania).

Metodyka LP-A jest uniwersalna także w zakresie wielkości realizowanych przedsięwzięć. Warto jednak pamiętać, pomijając oczywiste problemy dotyczące znacznych sił i środków angażowanych w przypadku

[5] Zauważyć należy, że w przypadku badań certyfikacyjnych zainteresowany uzyskaniem certyfikatu zleceniodawca dąży do przeprowadzenia audytu „papierowego" – ograniczonego do badań poprawności formalnej dokumentacji. Oczywiście na tyle, na ile pozwala na to wybrany wzorzec. To znacznie tańsze niż kupowanie drogiej technologii i/lub usług.

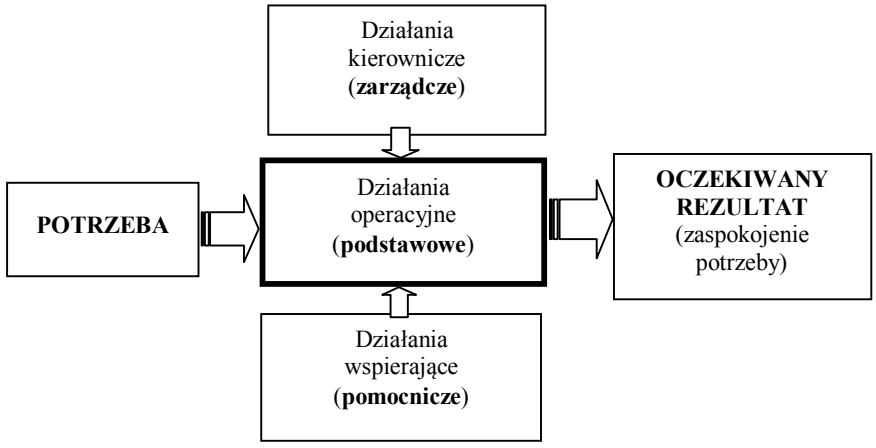
[6] Na marginesie warto wspomnieć, że w praktyce eksperci i audytorzy zatrudnieni w zadaniach należących do tzw. ścieżki technicznej są zdolni, bez większych trudności, realizować zadania ze ścieżki formalnej.

wieloelementowych i rozproszonych systemów, a wynikające po prostu z ich kosztów rosnących proporcjonalnie ze wzrostem wartości każdego z tych wymiarów, że pojawiają się problemy zarządzania przedsięwzięciem audytowym.

3. Umiejscowienie metodyki LP-A w procesie realizacji projektu

Audyt bezpieczeństwa informacyjnego, zgodnie z obowiązującymi trendami w zakresie zarządzania przedsięwzięciami, jest traktowany i zarządzany jako tzw. projekt. Rodzaje działań składających się na proces projektowania są przedstawione na rysunku 1 (za [17]). Metodyka LP-A należy do warstwy podstawowej – jest metodyką działań operacyjnych (wykonawczych).

W metodyce nie uwzględniono zatem hierarchizacji prac, harmonogramowania ani kosztorysowania etapów, a tym bardziej takich subtelności warstwy zarządczej, jak nadzór i korygowanie przebiegu realizacji przedsięwzięcia („projektu" w slangu zarządzania). Należy jednak zauważyć, że metodyka daje podstawy i dane do rzetelnego wykonania takich przedsięwzięć.



Rys. 2. Rodzaje działań związanych z wykonawstwem projektów (za [17] str. 178)

Metodykę sformułowano tak, aby realizowane zgodnie z nią przedsięwzięcia mogły być bez większych problemów zarządzane dowolną metodyką zarządzania projektem. W praktyce stwierdzono, że ortodoksyjnie stosowana metodyka PRINCE 2 jest zwykle metodyką zdecydowanie nadmiarową – wprowadza nieużyteczne obciążenie audytorów.

Jaka metodyka (PRINCE 2, MaXXIme itp.) zostanie wykorzystana do prowadzenia projektu – audytu bezpieczeństwa informacyjnego, zależy od preferencji wykonawców audytu i wymagań zleceniodawcy. Podczas realizacji audytów bezpieczeństwa informacyjnego autorzy metodyki LP-A (i ich zleceniodawcy) w zakresie działań zarządczych korzystali zwykle z elementów metodyki MaXXIme, takich jak PQP (ang. *Project Quality Plan*). W dużych projektach PQP, stanowiący element szablonu dokumentacyjnego większości metodyk zarządzania projektem, zapewnia niezbędne minimum nadzoru nad pracami.

4. Zmiany narzędzi ujętych w LP-A

W pierwotnej publikacji LP-A [16] wystąpiły, co prawda głównie w przypisach, informacje, które się zdezaktualizowały. Do wspomnianych informacji należą:

- cytaty z nieaktualnych obecnie źródeł, głównie z Kodeksu Karnego nieuwzględniające nowelizacji z ostatniego dziesięciolecia;
- przykłady narzędzi badań technicznych.

Ze względu na dążenie do uniwersalności, w LP-A nie wskazano wzorca audytowego i była to decyzja słuszna. Z praktycznych doświadczeń ostatniego dziesięciolecia wynika jednak, że zwykle przedmiot badania bezpieczeństwa określany jest przez wskazanie (terytorialnie i/lub funkcjonalnie) systemu teleinformatycznego stanowiącego obiekt badań oraz przez wybór zakresu badania drogą wskazania wybranych, odpowiednich punktów załącznika A (normatywnego) do normy PN ISO/IEC 27001:2007. Rzadkie na naszym rynku odstępstwa to zlecenia badania zgodności z PCI DSS (ang. PCI Data Security Standard [23]) czy Sarbanes–Oxley Act [28].

Obecnie zbiór sprawdzeń zwykle uzyskuje się, tworząc listę kontrolną literalnej zgodności z wymaganiami zakresów „bezpieczeństwa" zamieszczonych w normie PN ISO/IEC 17799:2007, odpowiadających numerami uzgodnionym (w ramach umowy ze zleceniodawcą) punktom załącznika A normy 27001:2007. Oczywiście dla każdego wymagania listę sprawdzanych elementarnych obiektów należy dla obiektu badań (systemu teleinformatycznego) sformułować oddzielnie. Dopiero kolejnym krokiem jest harmonogramowanie sprawdzeń, przydzielanie zadań itd.

Użytecznym narzędziem okazała się wspomniana już lista kontrolna literalnej zgodności ze zintegrowanymi wymaganiami normy 17799 oraz załącznika A normy 27001 sformułowana w postaci arkusza w Excelu (por. rysunek 2). Arkusz pozwala na łatwe integrowanie ocen przez podawanie dla każdego „zabezpieczenia" (w rozumieniu wymienionych norm) liczby zastosowanych zabezpieczeń niższego poziomu i liczby spełnionych „wytycznych do wdrożenia" (w rozumieniu normy 17799).

	Opis wymagania	Oc	Sug.
A	**6 Organizacja bezpieczeństwa informacji**		brak
A	**6.1 Organizacja wewnętrzna**		0,56
A	*Cel: Zarządzanie bezpieczeństwem informacji wewnątrz organizacji.*		---
	Zaleca się ustanowienie struktury organizacyjnej w celu inicjowania i kontroli wdrażania bezpieczeństwa informacji w organizacji.	n	oceń
	Zaleca się, aby kierownictwo zatwierdziło politykę bezpieczeństwa informacji, przypisało odpowiedzialność związaną z bezpieczeństwem, koordynowało i poddawało przeglądom wdrażanie bezpieczeństwa w organizacji.	n	oceń
	Jeśli zachodzi taka potrzeba, to zaleca się wskazanie i udostępnianie na potrzeby organizacji źródła specjalistycznej wiedzy z zakresu bezpieczeństwa informacji. Zaleca się wypracowanie kontaktów z zewnętrznymi specjalistami lub grupami, łącznie z odpowiednimi organami tak, aby mieć aktualną wiedzę o trendach rynkowych, zdolności monitorowania standardów i metod szacowania oraz zapewnienia odpowiednich punktów wymiany informacji w przypadku obsługi incydentu związanego z bezpieczeństwem informacji. Zaleca się też promowanie interdyscyplinarnego podejścia do bezpieczeństwa informacji.	s	oceń
A	**6.1.1 Zaangażowanie kierownictwa w bezpieczeństwo informacji**	s	S
A	Zabezpieczenie		---
A	Zaleca się, aby kierownictwo aktywnie wspierało bezpieczeństwo w organizacji przez wskazanie wyraźnego kierunku działania, demonstrowanie zaangażowania, jednoznaczne przypisanie i przyjmowanie odpowiedzialności w zakresie bezpieczeństwa informacji.	s	0,67
	Wskazówki do wdrożenia		---
	Zaleca się, aby kierownictwo:		---
	a) zapewniało, że cele bezpieczeństwa informacji są zidentyfikowane, spełniają wymagania organizacji i są włączone do odpowiednich procesów;	s	oceń
	b) określało, poddawało przeglądom i zatwierdzało politykę bezpieczeństwa informacji;	n	oceń
	c) poddawało przeglądom skuteczność wdrażania polityki bezpieczeństwa informacji;	n	oceń
	d) zapewniało jasne wskazania i widoczne wsparcie dla inicjatyw z zakresu bezpieczeństwa informacji;	s	oceń
	e) zapewniało środki potrzebne do zapewnienia bezpieczeństwa informacji;	s	oceń
	f) zatwierdzało w organizacji poszczególne role i zakresy odpowiedzialności związane z bezpieczeństwem informacji;	s	oceń
	g) inicjowało plany i programy utrzymujące właściwą świadomość problematyki bezpieczeństwa informacji;	n	oceń
	h) zapewniało, że wdrożenie zabezpieczeń informacji jest skoordynowane w całej organizacji (patrz 6.1.2).	s	oceń
	Zaleca się, aby kierownictwo określiło potrzebę, wewnętrznego lub zewnętrznego, specjalistycznego doradztwa z zakresu bezpieczeństwa informacji oraz dokonywało przeglądów i koordynowało wyniki takiego doradztwa w organizacji.	s	oceń
	W zależności od rozmiaru organizacji, obowiązki te mogą być wykonywane przez wyznaczone do tego celu forum kierownicze lub przez istniejące ciało zarządzające, takie jak zarząd.	nd	oceń
A	**6.1.2 Koordynacja bezpieczeństwa informacji**	s	S
A	Zabezpieczenie		---
A	Zaleca się, aby działania w zakresie bezpieczeństwa informacji były koordynowane przez reprezentantów różnych części organizacji pełniących odpowiednie role i funkcje.	s	0,8
	Zaleca się, aby te działania:		---
	a) zapewniały, że zadania z zakresu bezpieczeństwa są realizowane zgodnie z polityką bezpieczeństwa informacji;	nd	oceń
	b) określały postępowanie z przypadkami niezgodności;	nd	oceń
	c) zatwierdzały metodykę i procesy związane z bezpieczeństwem informacji, np. klasyfikację informacji lub szacowanie ryzyka;	nd	oceń
	d) rozpoznawały znaczące zmiany zagrożeń i stopień narażenia informacji lub środków do przetwarzania informacji na zagrożenia;	s	oceń
	e) szacowały adekwatność i koordynowały wdrożenie zabezpieczeń;	s	oceń
	f) skutecznie promowały w organizacji kształcenie, szkolenia i uświadamianie w zakresie bezpieczeństwa informacji;	n	oceń

Rys. 1. Fragment arkusza Excelowego: lista kontrolna literalnej zgodności z normą PN-ISO/IEC 17799 (opracowanie własne)

Za rozwojem systemów teleinformatycznych podąża niestety także rozwój zagrożeń, w szczególności ataków, rozwój rozwiązań technicznych zabezpieczeń i oczywiście rozwój narzędzi oceny bezpieczeństwa. O ile w niewielkim stopniu dotyczy to narzędzi ścieżki formalnej, o tyle w obszarze badań technicznych, a w szczególności testów penetracyjnych, postęp jest niezwykle dynamiczny. W ciągle użytecznym przewodniku badań technicznych bezpieczeństwa zalecanych przez NIST (SP-800-115 *Technical Guide to Information Security Testing and Assessment* [29]) wydanym w 2008 roku wskazano zastawy narzędzi, z których znaczna część nie jest już aktualizowana. Jednak BackTrack [2], [1] – zestaw narzędzi, który wytrzymał próbę czasu – jest stale aktualizowany. Nowa wersja BackTracka wydawana jest co pół roku[7], a aktualizacje narzędzi pojawiają się praktycznie co miesiąc. Otwarte narzędzie do wspomagania testów penetracyjnych o nazwie Metasploit [24], pozwalające na wykonywanie ataków według wzorców zapisanych w bazie danych, jest aktualizowane na bieżąco. Nowe wzorce ataków (tzw. potocznie exploity) wykorzystujące podatności pojawiają się praktycznie równocześnie z poprawkami (tzw. patchami) od producentów, eliminującymi te podatności w ich wyrobach.

Należy zauważyć, że narzędzia badań zależą od wielkości (rozmiaru) i metody szczegółowej badań obiektu: systemu teleinformatycznego. Jeśli system teleinformatyczny jest w jednej lokalizacji i nie zawiera wielu elementów – np. jest to centrum obliczeniowe świadczące usługi internetowe – to podstawowym narzędziem zarówno ścieżki formalnej, jak i technicznej będzie lista kontrolna literalnej zgodności z wzorcem, a badanie elementów systemu będzie wyczerpujące. W przypadku systemów rozproszonych terytorialnie lub obejmujących wielkie ilości różnorodnych elementów (np. wielkie sieci biurowe) badanie będzie dotyczyć wybranych elementów (np. reprezentatywnych), zaś listy kontrolne (porządek realizacji badań) zostaną zoptymalizowane w celu minimalizacji wyjazdów ekspertów i audytorów „w teren" i czasu badań.

5. Możliwości rozszerzenia metodyki LP-A na systemy SCADA

Jedną z modyfikacji metodyki LP-A w ciągu minionych 10 lat było przystosowanie jej do audytu bezpieczeństwa sieci teleinformatycznych połączonych z systemami przemysłowymi. Szczegółowo sposób modyfikacji został opisany w pracy [18]. Składają się na niego cztery podstawowe działania:

[7] Napisane w 2012 roku.

1. Identyfikacja norm i standardów z zakresu bezpieczeństwa sieci teleinformatycznych połączonych z systemami przemysłowymi, które mogą stanowić tzw. wzorzec audytowy. W pracy [18] zaproponowano[8]:
   - NIST Special Publication 800-82 (SECOND PUBLIC DRAFT): *Guide to Industrial Control Systems (ICS) Security*.
   - NIST Special Publication 800-53: *Recommended Security Controls for Federal Information Systems.*
   - zalecenia zawarte w *21 Steps to Improve Cyber Security of SCADA Networks*.
2. Przełożenie zaleceń z ww. dokumentów na zestawy pytań ankietowych. Opracowana ankieta, mająca za podstawę SP 800-82, zawiera 165 pytań (patrz przykład na rysunku 3).

   Takie ankiety są wykorzystane do badań ankietowych prowadzonych w ramach realizacji ścieżki formalnej metodyki LP-A oraz stanowią podstawę do opracowania wytycznych dla zespołów prowadzących badania techniczne.
3. Wyspecyfikowanie wymagań stawianych zespołom prowadzącym badania techniczne. Wymagania te określają specjalną wiedzę i umiejętności członków zespołów prowadzących badania techniczne. Wymagana wiedza dotyczy m.in. specyficznych dla SCADA/ICS protokołów, np. ICCP (ang. *Inter-Control Center Communication Protocol*[9]) czy MODBUS oraz tzw. maszynowych systemów bezpieczeństwa (nie mających swojego odpowiednika w tradycyjnych systemach informatycznych). Natomiast wspomniane wcześniej umiejętności mogą dotyczyć np. obsługi specjalizowanych przyrządów pomiarowych, nie używanych w audytach zwykłych sieci informatycznych.
4. Określenie wyposażenia zespołu prowadzącego badania techniczne w odpowiednie, do badanej sieci przemysłowej i planu audytu, przyrządy pomiarowe. Element ten zwykle nie jest istotny w badaniach zwykłych sieci informatycznych.

Dodatkowo należy mieć na uwadze konieczność dopracowania metodyki samych badań technicznych, w szczególności testów penetracyjnych. Dostępne, nieliczne publikacje na ten temat, kładą szczególny nacisk na nadanie właściwego priorytetu badaniom technicznym w całym audycie.

[8] Należy jednak zauważyć, że wymienione dokumenty zawierają zalecenia dotyczące *budowy zabezpieczeń* połączonych sieci, a nie zalecenia dotyczące oceny ich stanu bezpieczeństwa.

[9] Jest to międzynarodowy standard International Electrotechnical Commission (IEC) Std 870-6 Telecontrol Application Service Element Two (TASE.2), opisujący zasady komunikacji w czasie rzeczywistym pomiędzy centralami sterowniczymi.

6.2.2.3 Okablowanie

Pytania kontrolne:

1. Czy projekt okablowania sieci przemysłowej jest ujęty w firmowym planie bezpieczeństwa?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
2. Czy stosowane są odpowiednie kable sieciowe, przystosowane do środowiska przemysłowego (np. kable typu UTP są odpowiednie do środowiska biurowego, a nie przemysłowego) odporne na zakłócenia spowodowane polami magnetycznymi, falami radiowymi, zwiększoną temperaturą, wilgocią, pyłem, wibracjami?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
3. Czy są stosowane przemysłowe łącza RJ45 (w celu ochrony przed wilgocią, pyłem i wibracjami) zamiast złączy zwykłych?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
4. Czy zostało rozważone zastosowanie, odporniejszych na różne czynniki środowiskowe, kabli optycznych lub koncentrycznych?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
5. Czy kable i złącza sieci przemysłowej są odpowiednio oznakowane kolorem i etykietowane w celu ich wyraźnego wyróżnienia i zminimalizowania nieodpowiednich połączeń pomiędzy sieciami ICS i IT?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
6. Czy, w celu zminimalizowania nieuprawnionego dostępu fizycznego, kable są układane w specjalnych kanałach?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
7. Czy, w celu zminimalizowania nieuprawnionego fizycznego dostępu, urządzenia sieciowe są umieszczone w zamkniętych szafach?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
8. Czy szafy z urządzeniami sieciowymi mają odpowiednią wentylację?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**
9. Czy powietrze dopływające do wnętrza szaf z urządzeniami sieciowymi jest filtrowane?
   ☐ **TAK** ☐ **NIE** ☐ **NIE DOTYCZY** ☐ **POTRZEBNY KOMENTARZ**

Rys. 2. Przykład arkusza ankietowego (opracowanie własne)

6. Zakończenie

Można chyba stwierdzić, że metodyka zaczęła „żyć własnym życiem”, co bardzo cieszy jej autorów, bo osiągnięcie takiego stanu zakładali podczas opracowywania i publikowania LP-A.

Ponadto należy podkreślić, że w osobistych kontaktach z pracownikami firm i organizacji wykorzystujących metodykę, autorzy nie odnotowali żądań, ani nawet sugestii wprowadzenia istotnych zmian w metodyce. Większość uwag praktyków sprowadzała się do oczekiwania większej dokładności metodyki. Niestety, zastosowanie się do tej sugestii spowodowałoby zmniejszenie uniwersalności metodyki i ograniczenie zakresu możliwych wzorców audytowych.

Rozważano możliwość opracowania oczekiwanego przez wykonawców szablonu dokumentacyjnego, ale bez zwiększenia szczegółowości metodyki wydaje się nieosiągalne uzyskanie użytecznego wzorca. Poza tym większość średnich i dużych firm ma własne wzorce edycyjne i wymóg sporządzania dokumentów audytowych zgodnie z takim wzorcem jest częstym wymaganiem zleceniodawcy.

Autorzy metodyki dostrzegają, że w ciągu minionych dziesięciu lat pojawiły się w dziedzinie przetwarzania informacji dwa nowe elementy, istotnie rzutujące na praktykę prowadzenia badań audytowych. Te elementy to wirtualizacja zasobów i przetwarzanie w chmurze (ang. *cloud computing*). Pierwszy z nich ma wpływ przede wszystkim na rzetelną inwentaryzację zasobów teleinformatycznych, bez której trudno mówić o utrzymaniu odpowiedniego stopnia ochrony zasobów informacyjnych. Drugi z nich, oprócz trudności związanych z wirtualizacją, wnosi dodatkowe zagadnienia związane z właściwym przygotowaniem umów SLA i jurysdykcją, której podlegają zasoby w „chmurze". Wydaje się, że te dwa elementy, patrząc na problem z perspektywy metodyki LP-A, powinny znaleźć swoje odzwierciedlenie głównie w modyfikacji wagi sprawdzeń na ścieżce formalnej oraz dopracowaniu zbioru tzw. rzetelnych praktyk audytowych. Inaczej mówiąc, nie dotyczą treści metodyki, a doboru wzorca audytowego i/lub interpretacji jego zapisów.

W najbliższym czasie całkowicie nowym wyzwaniem dla służb bezpieczeństwa będzie niewątpliwie radykalnie nowa koncepcja zarządzania sprzętem teleinformacyjnym nazwana BYOD (ang. *Bring Your Own Device*), polegająca na wykorzystywaniu prywatnych urządzeń pracowników do realizacji zadań służbowych. Zarówno dziennikarskie prognozy (np. [9]), jak i poważne analizy (np. Gartnera, m.in. [32]) wskazują, że BYOD zajmie istotne miejsce wśród rozwiązań organizacyjnych firm. Co ważniejsze, stanowić będzie radykalną zmianę stosunków prawnych dotyczących zasobów informacyjnych, a przynajmniej tych zasobów, które do tej pory podlegały inwentaryzacji w ewidencji środków trwałych (licencje w ewidencji wartości niematerialnych i prawnych). Dla porządku odnotować należy i przeciwną koncepcję – *inverse BYOD* – polegającą na akceptowaniu przez pracodawcę prywatnego wykorzystywania służbowych urządzeń i licencji. Do tej pory użytkowe opracowania dotyczące BYOD dotyczą przede wszystkim urządzeń mobilnych, takich jak telefony komórkowe czy smartfony, w mniejszym stopniu czytników

i tabletów [32]. Obecne wymagania, czy to normy grupy 27000, czy inne uznane regulacje (np. lista kontrolna [6] stanowiąca zalecenia dla systemów informacyjnych administrowanych przez DoD lub podłączonych do sieci DoD) uwzględniają tzw. urządzenia mobilne i pracę zdalną, jednak nie uwzględniają faktu, że nosicielem zasobu informacyjnego (informacji) pracodawcy staje się zasób, do którego prawa własności i zarządzania należą do pracownika. Zapewne zostanie to uwzględnione w kolejnych wydaniach norm, obecnie jednak zmuszać będzie audytorów do innowacyjnego stosowania zapisów wymagań dotyczących tzw. strony trzeciej i zobowiązań pracowniczych. Przedwcześnie jest jeszcze rozstrzygać, czy rozsądne będzie wprowadzenie jakichś specjalnych zapisów w metodyce, autorzy jednak uważnie śledzą zmiany w tym zakresie.

Warto na koniec wspomnieć, że metodyka LP-A była wzorcem do opracowania metodyki L-RAC (ang. *Risk Analysis and Control*) [19] oraz metodyki prowadzenia testów penetracyjnych P-PEN [22]. Prowadzono także prace nad zastosowaniem metod sieciowych do szacowania czasu audytu na podstawie metodyki LP-A [20], ale prace te zostały zawieszone.

Ascetyczną formę metodyki, pomijającą zarówno modne obecnie deklaracje o wysokich kwalifikacjach moralnych, jak i formułowanie kodeksów etyki audytorów, autorzy uznają za właściwą. Oczekiwanie rzetelnych kwalifikacji inżynierskich zastępuje wszystkie te, niepewne[10] w praktyce, deklaracje.

Literatura

[1] Asseco Poland: *Roczne sprawozdanie finansowe Asseco Poland S.A. za 2005 rok (01.01.2005-3.12.2005),* http://i.wp.pl/a/f/espi/0603/0767253_Roczne_sprawozdanie_finansowe_Asseco_Poland_SA_za_2005_rok.pdf (stan z 15.12.2012).

[2] *BackTrack Linux – Penetration Testing Distribution*, http://www.backtrack-linux.org/ (stan z 21.12.2012).

[3] BARBIER J., BRADLEY J., MACAULAY J., MEDCALF R., REBERGER CH., *BYOD and Virtualization Top 10 Insights from Cisco IBSG Horizons Study*, Survey Report, CISCO IBSG Horizons, CISCO IBSG 2012.

[4] *Bezpieczeństwo informacji. Systemy/Procedury*, 2Business Consulting Group, http://www.2business.pl/uploads/prezentacje/2BCG%20-%20informacja%20bezpieczenstwo.pdf (stan z 21.12.2012).

[10] Trawestując Ralpha Emersona: „Im żarliwiej zapewniali nas o swej uczciwości, tym staranniej liczyliśmy potem srebrne łyżeczki" (ang. „The louder he talked of his honor, the faster we counted our spoons").

[5] *Certyfikat Audytu Bezpieczeństwa*, Informator Banku Spółdzielczego w Brańsku nr 58, styczeń – marzec 2009, http://www.bsbransk.pl/informator/2009s-m/strona5.pdf (stan z: 21.12.2012).

[6] *Checklist Details for General Mobile Device (Non-Enterprise Activated) STIG Version 1, Release 2*, NVD Checklist Id.: 417. Publ. date: 02/26/2012 (under review), http://web.nvd.nist.gov/view/ncp/repository/checklistDetail?id=417.

[7] CYRA Ł., GORSKI J., *Standards Conformity Framework in Comparison with Contemporary Methods Supporting Standards Application*, In: The Proceedings of International Conference of Dependability of Computer Systems DepCoS-RELCOMEX, Szklarska Poręba, 2008, pp 95-102.

[8] CYRA Ł., *A Method of Trust Case Templates to Support Standards Conformity Achievement and Assessment*, PhD Thesis. Gdańsk University of Technology, 2008.

[9] DIX J., *The approaching BYOD wave*, Network World December 03, 2012. http://www.networkworld.com/columnists/2012/120312-edit.html

[10] home.agh.edu.pl/~szymon/pbi/Wyklad%205%20Audyt.pdf (stan z 12.12.2012).

[11] http://isecman.org/audyt-wewnetrzny-bezpieczenstwa-informacji-pazdziernik (stan z 15.12.2012).

[12] http://www.centrum.bezpieczenstwa.pl/ (stan z 21.12.2012).

[13] http://www.ue.katowice.pl/?contentid=6660 (stan z 21.12.2012).

[14] KRAWCZYK P., *Audyt wewnętrzny w zakresie bezpieczeństwa,* prezentacja do zajęć PSZBI na SGH, 2009, portal ipsec.pl (stan z 21.12.2012).

[15] LIDERMAN K., PATKOWSKI A. E., *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, http://www.securing.pl/upload/File/metodykapracaudytowych.pdf (stan z 15.12.2012).

[16] LIDERMAN K., PATKOWSKI A.E., *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego,* Biuletyn IAiR, nr 19, str. 3-49, WAT, Warszawa, 2003.

[17] LIDERMAN K., *Analiza ryzyka i ochrona informacji w systemach komputerowych.* PWN, Warszawa, 2008.

[18] LIDERMAN K., *Audyt bezpieczeństwa sieci teleinformatycznych połączonych z systemami przemysłowymi – wytyczne do modyfikacji metodyki LP-A*, w: Zieliński Z. (red.): *Systemy czasu rzeczywistego. Postępy badań i zastosowania,* str. 299-308, WKŁ, Warszawa, 2009.

[19] LIDERMAN K., *Podręcznik administratora bezpieczeństwa teleinformatycznego.* MIKOM, Warszawa, 2003.

[20] LIDERMAN K., *Zarys zastosowania metod sieciowych do wyznaczania czasu realizacji audytu bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 20, str. 55-74, WAT, Warszawa, 2004.

[21] MOLSKI M. ŁACHETA M., *Przewodnik audytora systemów informatycznych*, Helion, Gliwice, 2006.

[22] PATKOWSKI A.E., *Metodyka P-PEN przeprowadzania testów penetracyjnych systemów teleinformatycznych*, Biuletyn IAiR, nr 24, str. 63-96, WAT, Warszawa, 2007.

[23] PCI DSS (PCI Data Security Standard) https://www.pcisecuritystandards.org/ security_standards /documents.php

[24] *Penetration Testing Software | Metasploit*, http://www.metasploit.com/

[25] Polski Serwis Naukowy, hasło *Audyt informatyczny,* www.naukowy.pl

[26] *Program konferencji*, XVI Krajowa Konferencja, Systemy Czasu Rzeczywistego, Pułtusk, 14-17 września 2009, http://zti.inf.polsl.pl/scr/Upload/SCR09 programv2c.pdf

[27] *Prospekt Emisyjny Akcji COMP Rzeszów S.A.*, Millennium Dom Maklerski Spółka Akcyjna 2004, www.millenniumdm.pl/pobierz/komunikaty/comp5.pdf (stan z 15.12.2012).

[28] Sarbanes–Oxley Act: *An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes,* 107th Congress Public Law 204, July 30, 2002, [H.R. 3763].

[29] SCARFONE K., MURUGIAH SOUPPAYA M., CODY A., OREBAUGH A., *Technical Guide to Information Security Testing and Assessment*, NIST Special Publication 800-115, NIST Sep. 2008, http://csrc.nist.gov/publications/nistpubs/800-115/SP800115.pdf

[30] SKWARA W., *Implementacja wytycznych BSI IS Audit do metodyki LP-A*, praca magisterska, Wydział Cybernetyki, WAT, Warszawa, 2012.

[31] Wikipedia, hasło *Audyt informatyczny*. (stan z dn. 22.11.2012) pl.wikipedia.org/wiki/Audyt_informatyczny

[32] WILLIS A. D., *Bring Your Own Device: New Opportunities, New Challenges*. Gartner ID G00238131, Gartner 16 August 2012, http://www.gartner.com/ resources/238100/238131/bring_your_own_device_new_op_238131.pdf (stan z 15.12.2012).

LP-A methodology – ten years later

ABSTRACT: This paper is an attempt to summarize the „life" of the LP-A methodology within the space of ten recent years. It presents an assessment of topicality and usefulness of the methodology in the present-day world. This justifies the conclusion that the considered methodology successfully stood the test of time and should retain its current form. Some modern challenges to the methodology resulting from technological changes are also presented.

KEY WORDS: audit, methodology, information security, safety

Praca wpłynęła do redakcji: 3.01.2013