BIULETYN INSTYTUTU AUTOMATYKI I ROBOTYKI
NR 22, 2005

Zarys projektowania systemu bezpieczeństwa teleinformatycznego

Krzysztof LIDERMAN

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

STRESZCZENIE: W artykule przedstawiono problematykę projektowania systemu bezpieczeństwa teleinformatycznego. Opis jest ukierunkowany przede wszystkim na działania operacyjne, przedstawione na tle liniowego modelu cyklu życia takiego systemu i dotyczy: projektowania koncepcyjnego, projektowania architektury, stosowania wzorców projektowych, testowania systemu oraz szczegółów działań na etapie analizy i projektowania. Działania związane z zarządzaniem procesem projektowania systemu bezpieczeństwa teleinformatycznego są przedstawione w skrócie w rozdziale 3.

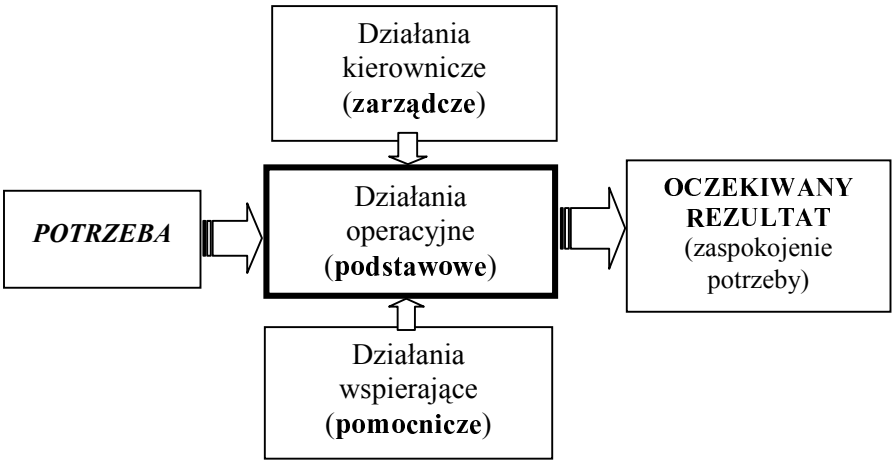
1. Wstęp

Projektowanie jest szczególnym rodzajem przedsięwzięcia. Termin „przedsięwzięcie" oznacza *złożone działanie, wielopodmiotowe, przeprowadzone zgodnie z planem, który ze względu na skomplikowanie bywa sporządzany przy pomocy specjalnych metod*[1]. Z kolei „projekt" to *celowe, niepowtarzalne (realizowane jednorazowo), złożone przedsięwzięcie zawarte w skończonym przedziale czasu – z wyróżnionym początkiem i końcem – realizowane zespołowo, w sposób względnie niezależny od powtarzalnej działalności przedsiębiorstwa, za pomocą specjalnych metod oraz technik*. „Celowość" oznacza, że projekt jest działaniem podejmowanym w celu osiągnięcia rezultatów oczekiwanych przez zleceniodawcę takiego projektu.

[1] T. Kotarbiński, *Sprawność i błąd*, PZWS, Warszawa, 1970.

Rodzaje działań składających się na proces projektowania są przedstawione na rysunku 1.1 (za [12]). Artykuł dotyczy przede wszystkim działań operacyjnych. Zagadnienia związane z zarządzaniem procesem projektowania i wytwarzania przedstawiono w rozdziale 3 tylko w zarysie. Przedmiotem projektowania, opisywanym w artykule, jest system bezpieczeństwa teleinformatycznego, czyli system ochrony informacji przetwarzanej, przesyłanej i przechowywanej w systemach teleinformatycznych przed utratą tajności, integralności oraz dostępności [1], [4].

Od zarządzania procesem projektowania należy odróżnić System Zarządzania Bezpieczeństwem Informacji (SZBI) [14], który z perspektywy projektowania systemu bezpieczeństwa jest składową ochronnych przedsięwzięć organizacyjnych (por. wyjaśnienia w rozdz. 5 – perspektywa zarządzania). Warto w tym miejscu zwrócić uwagę, że błędem jest utożsamianie SZBI z „bezpieczeństwem" informacji lub teleinformatycznym (nawet wtedy, gdy na ten SZBI jest wydany certyfikat bezpieczeństwa), tzn. zakładanie, że: *mamy SZBI = jesteśmy bezpieczni*.



Rys. 1.1. Rodzaje działań związanych z wykonawstwem projektów

2. Cykl życia systemu bezpieczeństwa teleinformatycznego

Termin „cykl życia" systemu określa koncepcję rozłożenia w czasie głównych czynności wykonywanych podczas pracy nad opracowaniem i wyprodukowaniem systemu określonego typu oraz podczas jego eksploatacji. Podstawowe elementy składowe cyklu życia systemu to: *cykl rozwojowy* i *cykl eksploatacyjny*, a podstawowe uszeregowanie etapów w cyklu to uszeregowanie kaskadowe (nazywane też liniowym lub wodospadowym). Przyjęcie określonej koncepcji cyklu rozwojowego pomaga:

- zdefiniować czynności, które trzeba wykonać podczas projektowania i budowy systemu,
- ujednolicić (w ramach firmy) sposób realizacji przedsięwzięć,
- zaplanować punkty kontroli stopnia realizacji systemu.

Sekwencyjny model liniowy cyklu życia systemu opisuje systematyczne podejście do wytwarzania systemu, polegające na przechodzeniu kolejno przez etapy: analizowania, projektowania, wytwarzania (w przypadku systemów programowych: kodowania), testowania i pielęgnacji. W informatyce jest to najstarszy oraz najpopularniejszy model procesu wytwórczego, stanowiący szablon, w którym można umieszczać konkretne metody analizowania, projektowania, programowania, testowania i pielęgnacji. Obecnie jest stosowany przede wszystkim jako pewien ogólnie uznany wzorzec do akademickiego wyjaśniania problemów wytwarzania systemów informatycznych.

W takiej roli model ten jest użyty w przedstawionym w tabeli 2.1 cyklu życia systemu bezpieczeństwa teleinformatycznego. Oprócz tradycyjnych dla takiego modelu etapów, grupujących określone czynności projektowe i wytwórcze, w tabeli są wyspecyfikowane czynności z zakresu zapewniania jakości oraz dokumenty wytwarzane w ramach każdego z etapów. Dokładny opis czynności etapu analizy i projektowania jest zawarty w rozdziale 6 niniejszego artykułu. Z przedstawionej tabeli wynika, że główne czynności etapu analizy i projektowania pokrywają się z czynnościami wykonywanymi na potrzeby bezpieczeństwa teleinformatycznego [1], [3], [6] w ramach procesu nazywanego analizą ryzyka. Wyróżnione kursywą czynności w kolumnie „Analiza" należy traktować jako dodatkowe, niezbędne do wykonania rzetelnego projektu takiego systemu. Są one praco- i czasochłonne, a ich włączenie (lub nie) do cyklu rozwojowego zależy od umowy z konkretnym zleceniodawcą takiego projektu – a dokładniej: od tego, czy np. zleceniodawca posiada rzetelnie wykonany (por. [1] i rozdz. 3) spis inwentaryzacyjny.

Tab. 2.1. Cykl życia systemu bezpieczeństwa teleinformatycznego

ETAPY:	**ANALIZA** (część I analizy ryzyka)	**PROJEKTOWANIE** (część II analizy ryzyka)	**WYTWARZANIE**	**TESTOWANIE**	**EKSPLOATACJA**
Czynności podstawowe:	*Inwentaryzacja zasobów teleinformatycznych.* *Ocena wstępna.* Identyfikacja kluczowych procesów biznesowych. Identyfikacja zagrożeń. Identyfikacja podatności. Określenie wymaganego poziomu ochrony (dla każdego z podstawowych atrybutów bezpieczeństwa informacji). Identyfikacja ograniczeń.	Projektowanie zarządzania bezpieczeństwem teleinf. (struktur i procedur organizacyjnych). Dobór technicznych i programowych środków ochronnych. Projektowanie sposobu zastosowania środków ochronnych (architektury). Ocena ryzyka szczątkowego.	Instalacja sprzętu i oprogramowania w sieci/systemie teleinf. oraz systemów ochrony fizycznej i technicznej. Rekonfiguracja sieci/systemów. Spisanie polityki, planu i instrukcji bezpieczeństwa teleinformatycznego. Spisanie planów zapewniania ciągłości działania. Wdrożenia i **szkolenia**.	**Testy penetracyjne** lub ocena na zgodność z ustalonym profilem kryterialnym/normą lub **audyt** bezpieczeństwa teleinformatycznego.	Nadzór i kontrola w zakresie bezpieczeństwa teleinformat. (w tym audyty i różnicowa analiza ryzyka). Likwidacja luk w systemie ochrony. **Szkolenia** podstawowe i doskonalące z zakresu bezpieczeństwa teleinf. Przeglądy i aktualizacje procedur i dokumentów. Testowanie planów zapewniania ciągłości działania.
Czynności zapewniania jakości:	Uzgodnienie podstawy oceny. Formalna akceptacja dok. wynikowych.	Formalna akceptacja ryzyka szczątkowego i dokumentów wynikowych.	Formalna akceptacja. dokumentów wynikowych. Testy regresyjne.	Formalna akceptacja raportów z testów/oceny lub audytu.	Nadzór ze strony zespołu ds. zarządzania bezpieczeństwem teleinformatycznym.
Wytwarzane dokumenty:	*Spis inwentaryzacyjny zasobów teleinformat.* Lista kluczowych procesów biznesowych i wspierających je procesów przetwarzania informacji. Listy: zagrożeń, zasobów i podatności, ograniczeń.	Wyniki analizy ryzyka. Projekty zalecanych struktur i procedur organizacyjnych.	Dokumentacja powykonawcza sieci i systemów teleinformat. Dokumentacja szkoleń. **Dokumenty opisujące system bezpieczeństwa teleinf.**: polityka, plan, instrukcje i plan zapewniania ciągłości działania.	Raporty z testów/oceny lub audytu.	Aktualizacja istniejącej dokumentacji.

3. Zarządzanie przedsięwzięciem projektowania i budowy systemu bezpieczeństwa teleinformatycznego

Warunkami niezbędnymi do opracowania i pomyślnego wdrożenia systemu bezpieczeństwa teleinformatycznego, od strony zarządzania przedsięwzięciem, jakim jest projektowanie i budowa systemu bezpieczeństwa teleinformatycznego, są:

1) świadomość najwyższej kadry kierowniczej zleceniodawcy znaczenia bezpieczeństwa teleinformatycznego dla działalności biznesowej firmy;
2) chęć i jawna deklaracja najwyższej kadry kierowniczej wsparcia działań podnoszących poziom bezpieczeństwa teleinformatycznego;
3) sformułowanie celu budowy i wdrożenia systemu bezpieczeństwa;
4) powołanie zespołu ds. zarządzania bezpieczeństwem teleinformatycznym, który będzie opracowywał (bądź nadzorował opracowanie) politykę bezpieczeństwa teleinformatycznego dla swojej firmy[2];
5) podjęcie decyzji co do sposobu budowy (lub zmiany) systemu bezpieczeństwa teleinformatycznego:
   - własnymi siłami firmy *lub*
   - zlecenie wykonania tej pracy wyspecjalizowanemu zespołowi z zewnątrz (rozwiązanie częściej spotykane[3]);
6) wskazanie kluczowych dla działania firmy procesów biznesowych (i związanych z nimi systemów teleinformatycznych);
7) wskazanie grup informacji, których ochrona jest szczególnie pożądana i określenie wymaganego poziomu ich ochrony (również w kontekście spełnienia wymagań ustawowych);
8) oszacowanie możliwych kosztów strat w przypadku utraty poufności, integralności lub dostępności informacji (również w aspekcie naruszenia przepisów prawnych państwowych lub resortowych, takich jak naruszenia przepisu o ochronie danych osobowych).

Należy zwrócić uwagę, że punkty 1–5 muszą być zrealizowane samodzielnie przez ścisłe kierownictwo firmy zleceniodawcy. W realizację punktów 6–8 (są one elementem etapu analizy), wykonywanych najczęściej pod kierunkiem zewnętrznych ekspertów, zaangażowani są także przedstawiciele ścisłego kierownictwa firmy, jako osoby najbardziej kompetentne do udzielenia wymaganych wyjaśnień.

---

[2] Powołanie takiego zespołu zalecają normy z zakresu bezpieczeństwa teleinformatycznego, np. PN-ISO/IEC-17799. Por. także [1].

[3] Dla dalszych rozważań w tym artykule przyjmuje się, że ten wariant został wybrany przez zleceniodawcę.

Do elementów zarządzania przedsięwzięciem należy również ustalenie składu zespołu projektującego i budującego system zabezpieczeń. Nie wchodząc w szczegóły organizacji pracy takiego zespołu, można jego podstawowe elementy wyspecyfikować następująco[4]:

1. Zespół analityków:
   - eksperci ds. bezpieczeństwa teleinformatycznego, wykonujący analizę ryzyka na potrzeby bezpieczeństwa teleinformatycznego,
   - audytorzy bezpieczeństwa teleinformatycznego,
   - *wyższa kadra kierownicza zleceniodawcy*,
   - *wskazani konsultanci ze strony zleceniodawcy*.
2. Zespół projektantów:
   - eksperci ds. bezpieczeństwa teleinformatycznego,
   - eksperci od wybranych technicznych i programowych środków ochronnych,
   - eksperci i konsultanci dziedzinowi, np. prawnicy.
3. Zespół wdrożeniowy:
   - eksperci ds. bezpieczeństwa teleinformatycznego, nadzorujący całość prac,
   - inżynierowie-eksperci od konkretnych platform sprzętowych i programowych,
   - szkoleniowcy,
   - *administratorzy techniczni* (systemów, serwerów, urządzeń sieciowych, stacji roboczych) *ze strony zleceniodawcy*,
   - *kadra kierownicza zleceniodawcy, wdrażająca zaprojektowane rozwiązania organizacyjne*.

Podstawowe czynniki warunkujące od strony technicznej wykonanie poprawnego projektu (planu) systemu bezpieczeństwa teleinformatycznego, ale ściśle związane z warstwą zarządzania przedsięwzięciem, to posiadanie przez zleceniodawcę:

1) schematu obiegu informacji w firmie z zaznaczoną klauzulą tajności każdej informacji (gdzie informacja zmienia swoją postać, jakie są miejsca potencjalnego wycieku informacji itp.),
2) spisu posiadanych zasobów teleinformatycznych (ile i jakie zasoby musimy chronić, kto za nie odpowiada itp.)

[4] Kursywą są wyróżnieni pracownicy zleceniodawcy, których współpraca z przedstawicielami zleceniobiorcy jest niezbędna do osiągnięcia celu – zbudowania skutecznego systemu bezpieczeństwa teleinformatycznego.

oraz ustalenie, czy przetwarzanej w firmowych systemach teleinformatycznych informacji dotyczą obowiązujące regulacje prawne (jeśli tak, to jakie?).

Termin „zasób teleinformatyczny", np. według normy PN-ISO/IEC-17799, obejmuje:

1) bazy danych, kartoteki, dokumentacje systemu, podręczniki użytkownika, materiały szkoleniowe, procedury biurowe, umowy partnerskie, serwisowe, dokumentacje typu *know-how* sklasyfikowane jako *informacje*;
2) oprogramowanie użytkowe, systemowe oraz narzędziowe sklasyfikowane jako *oprogramowanie*;
3) komputery, urządzenia telekomunikacyjne, drukarki, zasilacze awaryjne, meble itp. sklasyfikowane jako *zasoby fizyczne*;
4) urządzenia zapewniające: łączność, oświetlenie, zasilanie w energię elektryczną, klimatyzację itp. sklasyfikowane jako *urządzenia usługowe*.

Spis inwentaryzacyjny zasobów teleinformatycznych[5] powinien obejmować nie tylko wykaz zasobów według ww. typów, ale także:

1) precyzyjną lokalizację każdego zasobu;
2) adres IP (o ile posiada);
3) właściciela każdego zasobu.

4. System bezpieczeństwa teleinformatycznego – koncepcja

System bezpieczeństwa teleinformatycznego powinien być skuteczny, co oznacza, że:

- przełamanie nawet części środków ochronnych nie powinno prowadzić do naruszenia tajności, integralności lub dostępności chronionej informacji,
- każda próba penetracji systemu powinna być rozpoznana i sygnalizowana.

Skuteczny system bezpieczeństwa to system kompleksowy, wykorzystujący w spójny sposób (tzn. niesprzeczny i niepozostawiający dziur) środki ochronne:

- organizacyjne (w tym kadrowe),
- fizyczne i techniczne,
- sprzętowo-programowe,

[5] Z przedstawionego zakresu spisu wynika, że tzw. *skanery inwentaryzacyjne* mogą co najwyżej wspomóc wykonanie spisu inwentaryzacyjnego, ale na pewno go nie zastąpią.

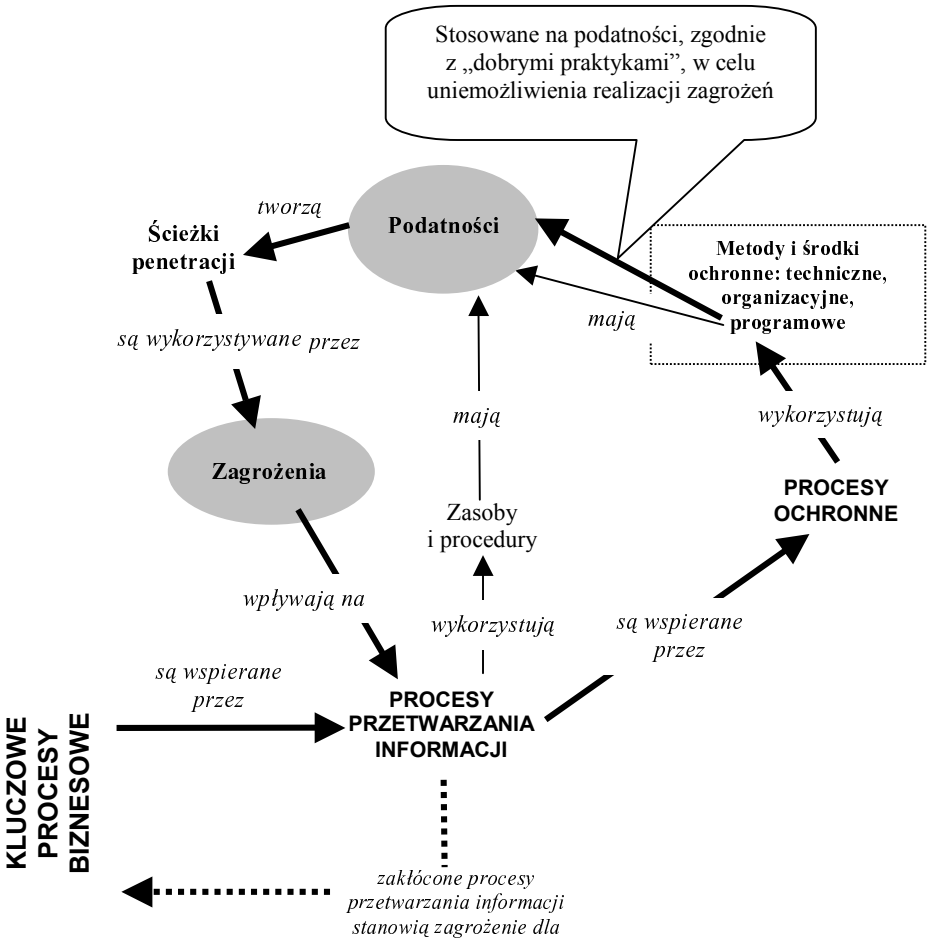
zorganizowane w taki sposób, że zapewnią wykrycie naruszenia bezpieczeństwa i próby takich działań oraz skuteczną ochronę, pomimo przełamania niektórych z nich, co oznacza ich zastosowanie według zasady *obrony „w głąb”* (szczegółowa i formalna definicja tej zasady została podana w [4]).

Środki ochronne, o których mowa, są stosowane do systemów teleinformatycznych wspierających kluczowe (lub krytyczne, szczegóły por. rozdz. 6.1) procesy biznesowe. Zadaniem środków ochronnych jest zapewnienie tajności, integralności i dostępności przetwarzanej w chronionych systemach teleinformatycznych informacji, ponieważ ma ona wpływ na przebieg procesów biznesowych. Zagrożenia dla informacji mogą wykorzystać podatności związane z zasobami wykorzystywanymi zarówno w procesach przetwarzania informacji, jak i w procesach ochronnych. Poglądowo zależności te przedstawia rysunek 4.1. Jak z niego wynika, przedstawione tam *metody i środki ochronne: techniczne, organizacyjne, programowe* są to te elementy, którymi można manipulować w procesie budowania systemu bezpieczeństwa, tzn. w zakresie których są podejmowane **decyzje projektowe**.

4.1. Kompleksowość i dekompozycja

Kompleksowe podejście do zagadnienia bezpieczeństwa teleinformatycznego ma swoje implikacje w postaci złożoności procesu projektowania środków ochronnych, szczególnie tych związanych z infrastrukturą i ochroną fizyczną, na przykład:

- zapewnienie odpowiedniego poziomu bezpieczeństwa dla takiego parametru informacji, jak tajność może wymagać umieszczenia całego systemu teleinformatycznego lub jego wybranych elementów w tzw. strefach bezpieczeństwa. Budowa stref bezpieczeństwa (w tym kancelarii tajnych), spełniających wymagania ustawy o ochronie informacji niejawnych wymaga zaangażowania nie tylko znacznych środków pieniężnych, ale także specjalistów z dziedziny budownictwa, kompatybilności elekromagnetycznej, ochrony technicznej itp.
- zapewnienie odpowiedniego poziomu dostępności informacji przetwarzanej w systemach teleinformatycznych może wymagać zastosowania systemów zasilania wyposażonych w spalinowe agregaty prądotwórcze (por. przykład 4.1). To z kolei zwykle wymaga rozwiązania problemu odprowadzania spalin i wybudowania/zaadaptowania pomieszczeń na agregat. Projektowanie systemu zasilania awaryjnego stanowi zwykle podprojekt w ramach projektowania systemu ochrony fizycznej i technicznej (por. rys. 4.3).



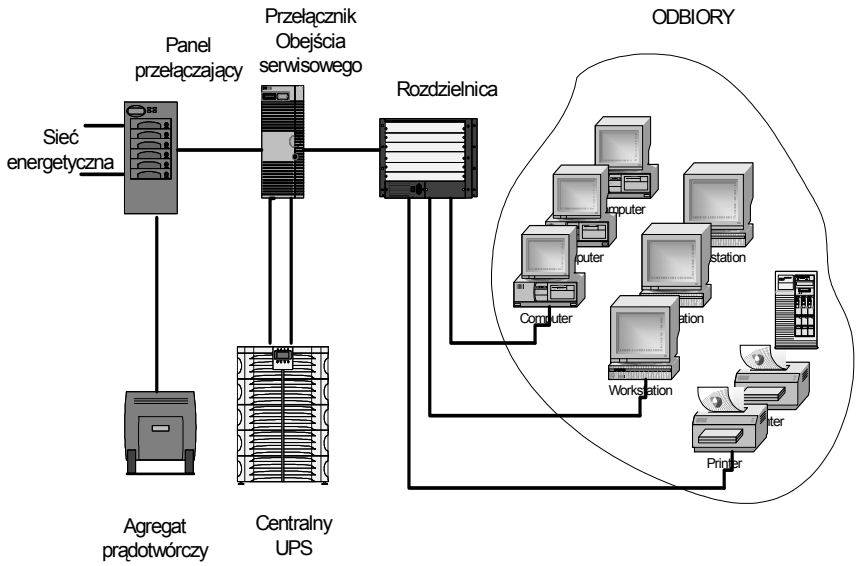
Rys. 4.1. Zależności przyczynowo-skutkowe w procesie identyfikacji i doboru środków ochronnych

Przykład 4.1.

W celu przeciwdziałania zakłóceniom zasilania, stosuje się systemy zasilania awaryjnego (nazywane też systemami zasilania gwarantowanego), na które składają się:

- redundantne, niezależne linie doprowadzające energię elektryczną (zasilania),
- panel przełączający,

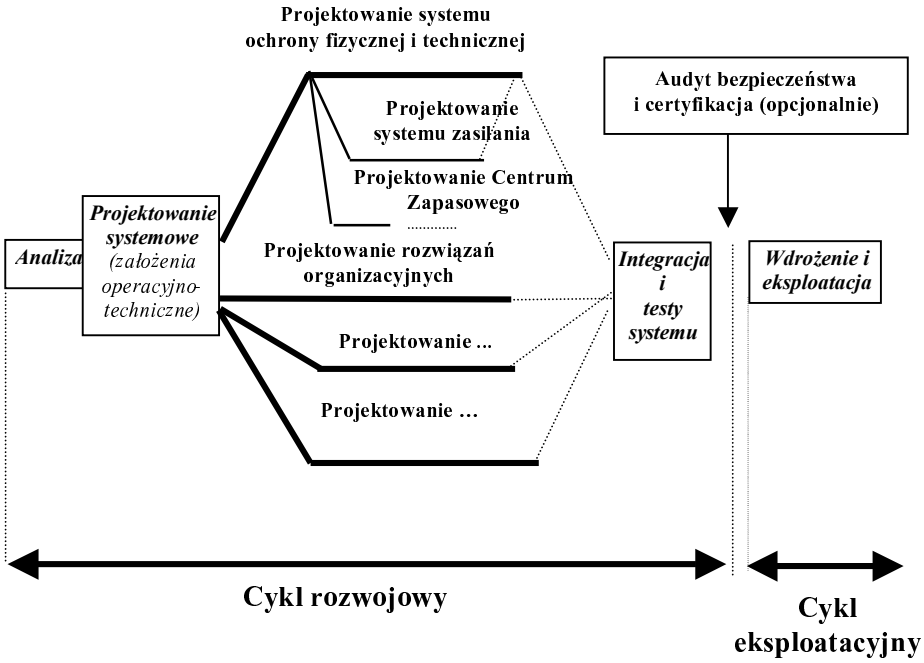
- przełącznik obejścia serwisowego,
- zasilacze bezprzerwowe,
- rozdzielnice,
- szafy montażowe,
- sieć linii zasilających,
- sieć linii logicznych (nadzór i sterowanie),
- konsola operatora i oprogramowanie,
- *agregaty prądotwórcze* (opcjonalnie, gdy wymagany czas zasilania awaryjnego wynosi więcej niż 40 min.),
- *urządzenia odprowadzające wydzielane ciepło* (opcjonalnie),
- wyłącznik awaryjny (dla systemu zasilania centralnego).



Rys. 4.2. Zasilanie systemu teleinformatycznego z centralnego UPS-u z wykorzystaniem agregatu prądotwórczego (przykład)

koniec_przykładu 4.1

W celu opanowania problemu złożoności procesu projektowania, należy zastosować **dekompozycję** – proces projektowania systemu bezpieczeństwa teleinformatycznego można zdekomponować do podprocesów projektowania wybranych środków ochronnych, realizowanych często w ramach odrębnie kontraktowanych przedsięwzięć (por. rys. 4.3).



Rys. 4.3. Schemat cyklu życia systemu bezpieczeństwa z zaznaczonymi odrębnymi przedsięwzięciami (ścieżkami) projektowymi (przykład)

4.2. Przesłanki budowy „w głąb" systemu obrony

Dobrą wizualizacją zasady obrony „w głąb" jest średniowieczny zamek odpowiednio umiejscowiony w terenie, otoczony fosami i kilkoma pasami murów obronnych wzmocnionych wieżami. Pokonanie fosy i przerwanie zewnętrznego pasa murów obronnych przez napastników zwykle nie prowadziło do utraty zamku, ponieważ obrońcy wycofywali się za drugi, wewnętrzny pas murów obronnych i bronili się dalej.

W przypadku zastosowania tej zasady do środków ochronnych, składających się na system bezpieczeństwa teleinformatycznego, oznacza to tyle, że po przełamaniu jednego środka ochronnego, na drodze do celu potencjalny intruz powinien natknąć się na kolejny środek ochronny. Najlepiej, żeby był on z innej grupy (te grupy tworzą środki: organizacyjne, programowo-sprzętowe oraz ochrony fizycznej i technicznej) – warto bowiem na ścieżce penetracji stosować dywersyfikację środków ochronnych.

Przesłankę do budowy systemu bezpieczeństwa w taki sposób dają badania Niemieckiego Federalnego Urzędu ds. Bezpieczeństwa Informacyjnego (szczegóły por. www.bsi.bund.de), przedstawione w tabeli 4.1.

Tab. 4.1. Statystyka zagrożeń i możliwości przeciwdziałania zagrożeniom zidentyfikowanym przez Niemiecki Federalny Urząd ds. Bezpieczeństwa Informacyjnego (stan na listopad 2002)

Oznaczenie katalogowe	Nazwy klas zagrożeń	Liczba zagrożeń w klasie
G1	Siły wyższe	13
G2	Skutki błędów w organizacji pracy	71
G3	Szkodliwe działania ludzi	53
G4	Awarie lub złe wykorzystanie urządzeń technicznych	44
G5	Błędy w obsłudze systemu komputerowego	104
	RAZEM:	**285**

Oznaczenie katalogowe	Nazwy grup metod przeciwdziałania zagrożeniom	Liczba przedsięwzięć w metodzie
M1	Infrastruktura	29
M2	Organizacja	241
M3	Personel	30
M4	Sprzęt i oprogramowanie komputerowe	160
M5	Komunikacja	98
M6	Obsługa zdarzeń kryzysowych	81
	RAZEM:	**639**

Liczby znajdujące się w kolumnie „RAZEM" pokazują, że liczba możliwych przedsięwzięć ochronnych jest ponad dwukrotnie większa niż liczba zagrożeń. Oznacza to, że każdemu zagrożeniu można przeciwstawić średnio co najmniej dwa środki ochronne. Tabela 4.1 pokazuje jeszcze inną istotną zależność: najwięcej zagrożeń, ale i najwięcej możliwości przeciwdziałania im, leży w zakresie organizacji. Stąd, przy projektowaniu systemu bezpieczeństwa, ważne jest włączenie do projektu przygotowania ludzi korzystających z systemów teleinformatycznych. To przygotowanie powinno prowadzić do:

- właściwej eksploatacji systemu teleinformatycznego i zbiorów informacji,
- właściwego rozumienia i użycia zaimplementowanych środków ochronnych,
- właściwych reakcji na incydenty z zakresu bezpieczeństwa teleinformatycznego (w tym na ataki socjotechniczne).

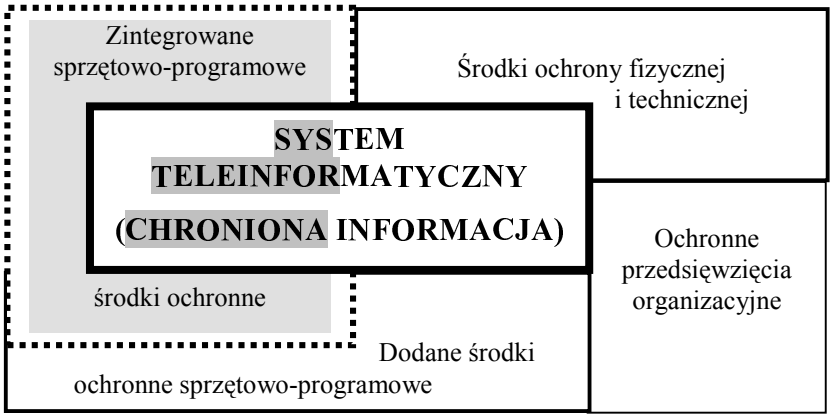
5. Architektura systemu bezpieczeństwa teleinformatycznego

W informatyce termin „architektura" to słowo-klucz na określenie schematu ogólnej budowy systemu z użyciem składników zidentyfikowanych podczas opracowywania koncepcji (projektu systemowego). Oznacza on zatem **ogólny opis systemu** z wykorzystaniem:

- podstawowych, na określonym poziomie szczegółowości, składników systemu, uwidocznionych jedynie przez ich cechy zewnętrzne,
- ich organizacji w bardziej złożone struktury,
- sposobów ich współdziałania w celu wykonania określonych zadań.

Ze względu na kompleksowość systemu bezpieczeństwa, przydatne jest rozpatrywanie jego architektury w różnych perspektywach, np.:

a) konstrukcyjnej



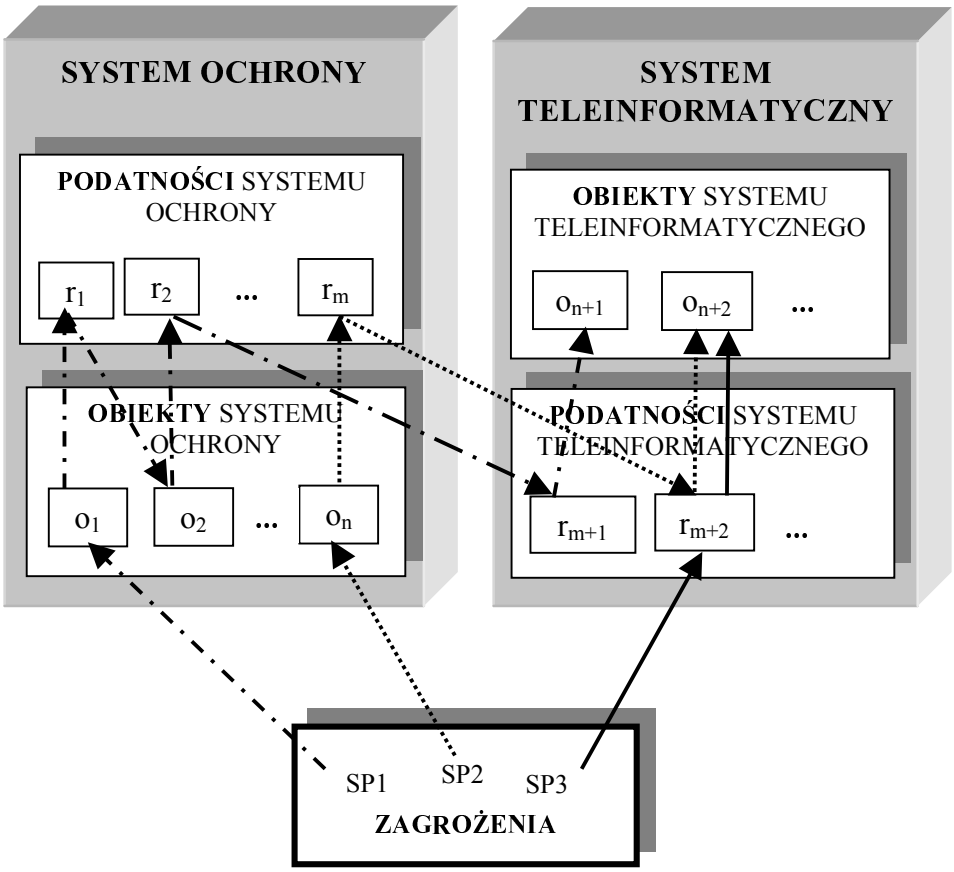
Rys. 5.1. Architektura systemu bezpieczeństwa teleinformatycznego: perspektywa konstrukcyjna

Perspektywa konstrukcyjna pokazuje:

- rodzaj i dywersyfikację zastosowanych środków ochronnych,
- spójność (symbolizowaną zamkniętym obszarem wokół systemu teleinformatycznego) systemu ochrony.

Model architektoniczny w perspektywie konstrukcyjnej można, w zależności od potrzeb, poddać dekompozycji w celu uwidocznienia detali. Szczególną uwagę należy zwrócić na właściwe zaprojektowanie i przedstawienie rozwiązań znajdujących się na styku poszczególnych grup środków ochronnych.

b) ścieżek penetracji

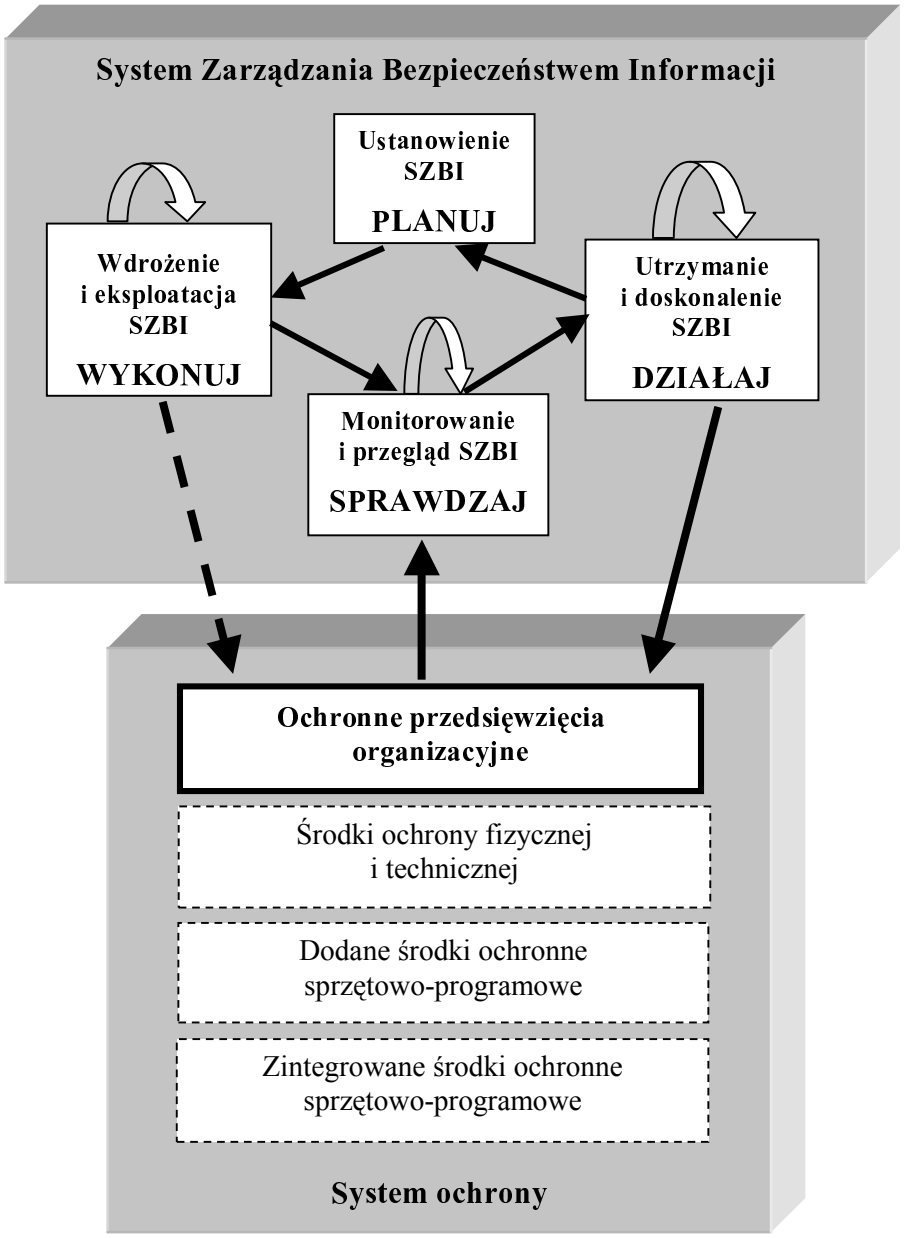


Rys. 5.2. Architektura systemu bezpieczeństwa teleinformatycznego: perspektywa ścieżek penetracji

Interpretacja rysunku 5.2 może być następująca:

- ścieżka penetracji **SP1**: zagrożenie wykorzystuje podatność r_1 w obiekcie o_1, będącym elementem systemu ochrony, co z kolei umożliwia wykorzystanie podatności r_2 obiektu o_2 stanowiącego także element systemu ochrony. Umożliwia to wykorzystanie podatności r_{m+1} obiektu $o_{n+1,}$ będącego elementem systemu teleinformatycznego przetwarzającego (przechowującego, przesyłającego) konkretną informację.
- ścieżka penetracji **SP3**: zagrożenie wykorzystuje bezpośrednio podatność r_{m+2} w obiekcie o_{n+2}, będącym elementem systemu teleinformatycznego przetwarzającego (przechowującego, przesyłającego) konkretną informację.

c) zarządzania bezpieczeństwem



Rys. 5.3. Architektura systemu bezpieczeństwa teleinformatycznego: perspektywa zarządzania bezpieczeństwem

Perspektywa zarządzania bezpieczeństwem informacji pokazuje związki pomiędzy SZBI a systemem ochrony. Ogólnie uznawany model zarządzania bezpieczeństwem, w modnym obecnie wydaniu procesowym, jest wprowadzony w normie PN-I-7799-2 [14]. Norma ta jest zharmonizowana z innymi normami systemów zarządzania, takimi jak BS EN ISO 9001:2000 oraz BS EN ISO 14001:1996, tak aby.*zapewnić spójne i zintegrowane wdrożenie i działanie systemów zarządzania*[6]. Norma wprowadza model „Planuj-Wykonuj-Sprawdzaj-Działaj" (ang. PDCA) jako podejście do tworzenia, wdrażania i zwiększania skuteczności systemu zarządzania bezpieczeństwem informacji, stanowiącego część systemów zarządzania organizacji. Wdrożenie modelu PDCA odzwierciedla ponadto zasady określone w wytycznych OECD (2002), odnoszące się do bezpieczeństwa systemów informacyjnych i sieci.

Na rysunku 5.3 strzałki wstęgowe pokazują, że działania PDCA odnoszą się także do czynności systemu zarządzania (SZBI) jako takiego. Oprócz tego, czynności „Działaj", „Wykonuj", „Sprawdzaj" mają związki z przedsięwzięciami organizacyjnymi systemu ochrony (strzałki zwykłe pogrubione).

6. Analiza i projektowanie na potrzeby budowy systemu bezpieczeństwa teleinformatycznego

Etapy analizy i projektowania w cyklu życia systemu bezpieczeństwa teleinformatycznego zawierają czynności analizy ryzyka (por. [1], [3], [6]). Specyfikacja tych czynności jest zawarta w rozdziałach 6.1. i 6.2.

6.1. Etap analizy

Rzetelna realizacja czynności na etapie analizy wymaga ścisłej współpracy konsultantów (ze strony klienta) z analitykami. Konsultantami powinny być osoby:

- najwyższego szczebla kierowniczego firmy (dla której jest wykonywana analiza) posiadające wiedzę na temat kluczowych procesów biznesowych firmy,
- posiadające pełnomocnictwa najwyższego kierownictwa firmy do wiążącego wypowiadania się w imieniu firmy na tematy będące przedmiotem analizy.

Podstawowe czynności procesu analizy obejmują:

[6] W załączniku informacyjnym C normy [13] przedstawiono (w tablicy C.1) powiązanie między BS EN ISO 9001:2000, BS EN ISO 14001:1996 a BS 7799-2:2002.

1) identyfikowanie procesów kluczowych. Dla różnych typów organizacji (finansowe, naukowe, handlowe, produkcyjne) różne będą procesy kluczowe;
2) określenie dla zidentyfikowanych procesów kluczowych dopuszczalnych czasów przestoju;
3) określenie dla zidentyfikowanych procesów kluczowych ich wrażliwości na zakłócenia we wspierających je procesach przetwarzania informacji;
4) znalezienie wśród procesów z punktu 1 procesów krytycznych. Krytyczność procesu określa:
   - czas jego dopuszczalnego przestoju – im mniejszy, tym proces bardziej krytyczny[7],
   - wrażliwość na utratę tajności, integralności lub dostępności informacji wykorzystywanej w procesie kluczowym;
5) dla procesów krytycznych zidentyfikowanie wspierających je procesów przetwarzania informacji w systemach teleinformatycznych;
6) dla każdego z procesów zidentyfikowanych w punkcie 5 zidentyfikowanie zagrożeń, które mogą doprowadzić do utraty tajności, integralności i dostępności przetwarzanych w nich informacji;
7) zidentyfikowanie wymaganych poziomów ochrony informacji przetwarzanej, przesyłanej i przechowywanej w procesach wspierających (punkt 5) w odniesieniu do atrybutów: tajności, integralności, dostępności. Im silniejsza wrażliwość zidentyfikowana w punkcie 3, tym silniejsza powinna być ochrona;
8) dla procesów zidentyfikowanych w punkcie 5 zidentyfikowanie zasobów w nich wykorzystywanych;
9) dla każdego zasobu każdego procesu z punktu 5 zidentyfikowanie podatności, które mogą być wykorzystane przez zagrożenia zidentyfikowane w punkcie 6;
10) w zbiorze zasobów (punkt 8) i zbiorze podatności (punkt 9) wyznaczenie ścieżek penetracji (por. [4]) dla procesów wspierających. Ścieżkę penetracji, w zasobach będących nośnikami informacji i zasobach uczestniczących w procesach ochronnych (zabezpieczeniach) oraz procedurach organizacyjnych, wyznaczają podatności niezabezpieczone i podatności, których zabezpieczenia zostały przełamane.

[7] Przykładem procesu kluczowego dla przedsiębiorstwa produkcyjnego jest proces dostaw części do produkcji. Staje się on procesem krytycznym ze względu na czas, jeżeli jest on organizowany według metody *just-in-time*, co oznacza, że nie ma magazynowania części do produkcji. Koszty produkcji się obniżają (nie trzeba utrzymywać magazynów), ale jednocześnie wzrasta wrażliwość procesu produkcyjnego na zakłócenia w procesie dostaw.

11) zidentyfikowanie ograniczeń w zakresie potencjalnych decyzji projektowych wynikających np. z przepisów prawnych, budżetu zleceniodawcy lub czasu przeznaczonego na projekt i wykonanie systemu bezpieczeństwa.

Wzajemne zależności czynności wymienionych w punktach 1-10 są pokazane na rysunku 4.1.

Dokumenty wynikowe procesu analizy to:

- lista kluczowych procesów biznesowych,
- lista procesów krytycznych i wspierających je procesów przetwarzania informacji,
- listy: zagrożeń, zasobów i podatności,
- specyfikacja wymaganych poziomów ochrony informacji,
- zidentyfikowane ograniczenia w zakresie potencjalnych decyzji projektowych (por. rozdz. 6.4),
- wstępny zbiór ścieżek penetracji.

6.2. Etap projektowania

Celem etapu projektowania jest zaprojektowanie procesów ochronnych dla procesów przetwarzania informacji wspierających krytyczne procesy biznesowe. Podstawowe czynności procesu projektowania procesów ochronnych obejmują:

1) zaprojektowanie zarządzania bezpieczeństwem teleinformatycznym (struktur, dokumentów i procedur organizacyjnych);
2) dobór technicznych i programowych środków ochronnych do podatności;
3) zaprojektowanie sposobu zastosowania środków ochronnych na ścieżkach penetracji. Projektowany sposób zastosowania środków ochronnych (architektury) musi uwzględniać:
   - wymagany poziom ochrony,
   - rodzaj atrybutu informacji, który podlega ochronie (tajność, integralność, dostępność),
   - aplikację według zasady obrony „w głąb”,
   - niesprzeczność działania środków ochronnych na ścieżce penetracji;
4) zidentyfikowanie potencjalnych podatności w zaprojektowanych środkach ochronnych;
5) uzupełnienie ścieżek penetracji zidentyfikowanych w punkcie 10 etapu analizy o podatności zaprojektowanych środków ochronnych;

6) ponowne przejrzenie zmodyfikowanych ścieżek penetracji i uzupełnienie ich o dodatkowe środki ochronne;
7) ocenę ryzyka szczątkowego;
8) w zależności od wyników oceny z punktu 7 – przeprojektowanie systemu ochrony lub przejście do kolejnego etapu – wytwarzania.

Realizację punktów 1 i 2 listy może wspomóc tabela 6.1, w której są wyspecyfikowane podstawowe procesy ochronne oraz możliwości wykorzystania w nich środków ochronnych.

Tabela 6.1. Dobór środków ochronnych do procesów ochronnych

Lp.	ŚRODKI OCHRONY: / PROCESY OCHRONNE:	Fizyczne i techniczne	Programowe	Sprzętowe	Organizacyjne
1	**Uwierzytelniania:**				
	– w systemach dostępu logicznego do systemu teleinformatycznego		1		2
	– w systemach dostępu fizycznego do obiektów	3			4
	– danych		5		6
2	**Wykrywania:**				
	– nieuprawnionych działań	7	8		9
	– podatności	10	11		12
	– zagrożeń środowiskowych (np. pożar, zalanie)	13			
3	**Wykrywania i filtrowania niepożądanych kodów i treści:**		14		
4	**Minimalizowania podatności:**				
	– „utwardzanie" konfiguracji		15		16
	– uaktualnianie oprogramowania (np. baz sygnatur) oraz likwidowanie podatności poprzez aplikację poprawek		17		18
5	**Minimalizowania przestojów sprzętu komputerowego:**	19		20	21
6	**Utajniania informacji:**	22	23	24	25
7	**Zapewniania integralności informacji:**		26		27
8	**Autoryzacji osób (procesów):**	28	(29)		30

Stosowane techniki i narzędzia (por. liczby w tab. 6.1.):

1: integralne procesy uwierzytelniania w systemach operacyjnych, autonomiczne systemy kontroli dostępu do danych

2: procedury nadawania i odbierania praw dostępu do informacji

3: służby nadzoru i prewencji, elektroniczne systemy kontroli WE/WY

4: procedury nadawania i odbierania praw dostępu do pomieszczeń i urządzeń

5: podpisy cyfrowe

6: podpisy ręczne

7: służby nadzoru i prewencji

8: zastosowanie IPS, analiza zapisów w dziennikach zdarzeń systemów operacyjnych i urządzeń

9: procedury nadzoru i kontroli, procedury działania służb nadzoru i prewencji, szkolenia

10: służby nadzoru i prewencji

11: zastosowanie skanerów bezpieczeństwa

12: testy penetracyjne, audyty

13: systemy ppoż., systemy wykrywania wilgoci, służby nadzoru i prewencji

14: zapory sieciowe i osobiste, AV, filtry antyspamowe

15: zastosowanie programów utwardzających

16: procedury i zalecenia na temat konfiguracji oprogramowania i sprzętu

17: mechanizmy wgrywania poprawek i uaktualnień

18: procedury testowania i wgrywania poprawek oraz uaktualnień

19: redundancje elementów i zasilania systemów ochrony technicznej

20: redundancje elementów sprzętowych sieci i systemów teleinformatycznych, macierze RAID, systemy zasilania awaryjnego.

21: umowy z dostawcami sprzętu komputerowego, biurowego i oprogramowania opracowanie i testowanie planów zapewniania ciągłości działania

22: strefy bezpieczeństwa, mechaniczne środki ochronne

23: szyfrowanie, steganografia

24: szyfrowanie, ochrona przed wyciekiem informacji przez promieniowanie ujawniające

25: klasyfikacja informacji i dopuszczenia dla personelu, procedury pracy w strefach bezpieczeństwa, szkolenia

26: podpisy cyfrowe

27: szkolenia

28: służby nadzoru i prewencji, elektroniczne systemy kontroli WE/WY

29: (integralne procesy w systemach operacyjnych, autonomiczne systemy kontroli dostępu do danych)

30: procedury autoryzacji.

Dokumenty wynikowe procesu projektowania to:

- lista technicznych i programowych środków ochronnych,
- projekt sposobu implementacji ww. środków (architektura),
- projekty zalecanych struktur i procedur organizacyjnych,
- lista zasobów i podatności (dla procesów ochronnych),
- uzupełniony zbiór ścieżek penetracji,
- wyniki oceny ryzyka szczątkowego.

6.3. Wzorce projektowe

Wzorzec jest uogólnionym rozwiązaniem pewnego powracającego problemu konstrukcyjnego. Uznaje się powszechnie, że wzorce są ulepszeniem w stosunku do opisów sporządzanych ad hoc lub rutynowo. Poza tym, stosowanie wzorców wpływa na przyspieszenie i podniesienie jakości procesu projektowania. Wśród wzorców projektowych wyróżnia się:

- *wzorce ogólne*[8] (niezależne od technologii), które znajdują zastosowanie w budowie każdego dobrze zaprojektowanego systemu informatycznego;
- *wzorce specyficzne* dla technologii zastosowanej przy tworzeniu aplikacji, budowane na bazie wzorców ogólnych (np. wzorce J2EE).

W dziedzinie bezpieczeństwa teleinformatycznego takimi *wzorcami ogólnymi* są konstrukcje zawarte w trzyczęściowej normie międzynarodowej ISO/IEC 15408: *Information technology – Security techniques – Evaluation Criteria for IT Security*, która została opracowana przez Wspólny Komitet Techniczny ISO/IEC JTC 1 (Technika Informatyczna) we współpracy z organizacjami sponsorującymi Projekt Wspólnych Kryteriów[9].

Na podstawie ww. normy, Polski Komitet Normalizacyjny wydał normę (jako tłumaczenie wersji angielskiej):

PN-ISO/IEC 15408: *Technika informatyczna – Techniki zabezpieczeń. Kryteria oceny zabezpieczeń informatycznych:*

- Część 1: *Wprowadzenie i model ogólny* ([15], opublikowana w sierpniu 2002)

[8] Najbardziej znane i stosowane są tzw. **wzorce GoF** (***G**ang **o**f **F**our*, Banda Czworga, por. książkę Gamma E., Helm R., Johnson R., Vlissides J.: *Design Patterns. Elements of Reusable Object-Oriented Software*, Addison-Wesley, 1995).

[9] Tekst identyczny z ISO/IEC 15408 jest publikowany przez Organizacje Sponsorujące Projekt Wspólnych Kryteriów jako *Common Criteria for Information Technology Security Evaluation*.

– Część 2: *Wymagania funkcjonalności zabezpieczeń* (dotąd nieopublikowana)
– Część 3: *Wymagania uzasadnienia zaufania do zabezpieczenia* ([16], opublikowana w październiku 2002).

W normie wprowadzono koncepcję profili i zadań zabezpieczeń, gdzie:

– **Profil Zabezpieczeń** (ang. *Protection Profile*, PP) **–** niezależny od implementacji zbiór wymagań na zabezpieczenia dla pewnej kategorii Przedmiotów Oceny (TOE), spełniających potrzeby odbiorców;
– **Zadanie Zabezpieczeń** (ang. *Security Target*, ST) **–** zestaw wymagań na zabezpieczenia i specyfikacji, które będą używane jako podstawa do oceny określonego Przedmiotu Oceny (TOE).

Zarówno PP, jak i ST są dokumentowane według ustalonego (w normie) szablonu dokumentacyjnego (por. [5]) i za pomocą specyficznych elementów konstrukcyjnych. Norma definiuje bowiem zbiór elementów konstrukcyjnych, które składają się na zestawy wymagań na zabezpieczenia o znanej przydatności i mogą być wykorzystywane przy ustalaniu wymagań na zabezpieczenia dla planowanych produktów i systemów.

Uporządkowanie przez normę wymagań na zabezpieczenia w hierarchię klas, rodzin i komponentów ma na celu ułatwienie odbiorcom zlokalizowania konkretnych wymagań na zabezpieczenia. Specyfikację wzorców wraz z ich oznaczeniami symbolicznymi przedstawia tabela 6.2. Podstawowym elementem (nieujętym w tab. 6.2) jest tzw. *element uzasadnienia zaufania*, stanowiący pojedyncze, niepodzielne wymaganie dotyczące bezpieczeństwa[10]. Każdy z takich elementów należy do jednego z trzech zbiorów:

– elementów działania konstruktora, np.:

  ADV_FSP.1.1**D** Konstruktor powinien dostarczyć specyfikację funkcjonalną.

– elementów określających zawartość i prezentację elementów dowodu, np.:

  ADV_FSP.1.1**C** Specyfikacja funkcjonalna powinna opisywać TSF i ich zewnętrzny interfejs w nieformalny sposób.

  ADV_FSP.1.2**C** Specyfikacja funkcjonalna powinna być spójna wewnętrznie.

– elementów działania osoby oceniającej, np.:

  ADV_FSP.1.1**E** Oceniający powinien potwierdzić, że dostarczona informacja spełnia wszystkie wymagania co do zawartości i prezentacji dowodu.

  ADV_FSP.1.2**E** Oceniający powinien określić, czy specyfikacja funkcjonalna jest dokładną i kompletną konkretyzacją wymagań na funkcjonalność zabezpieczeń TOE.

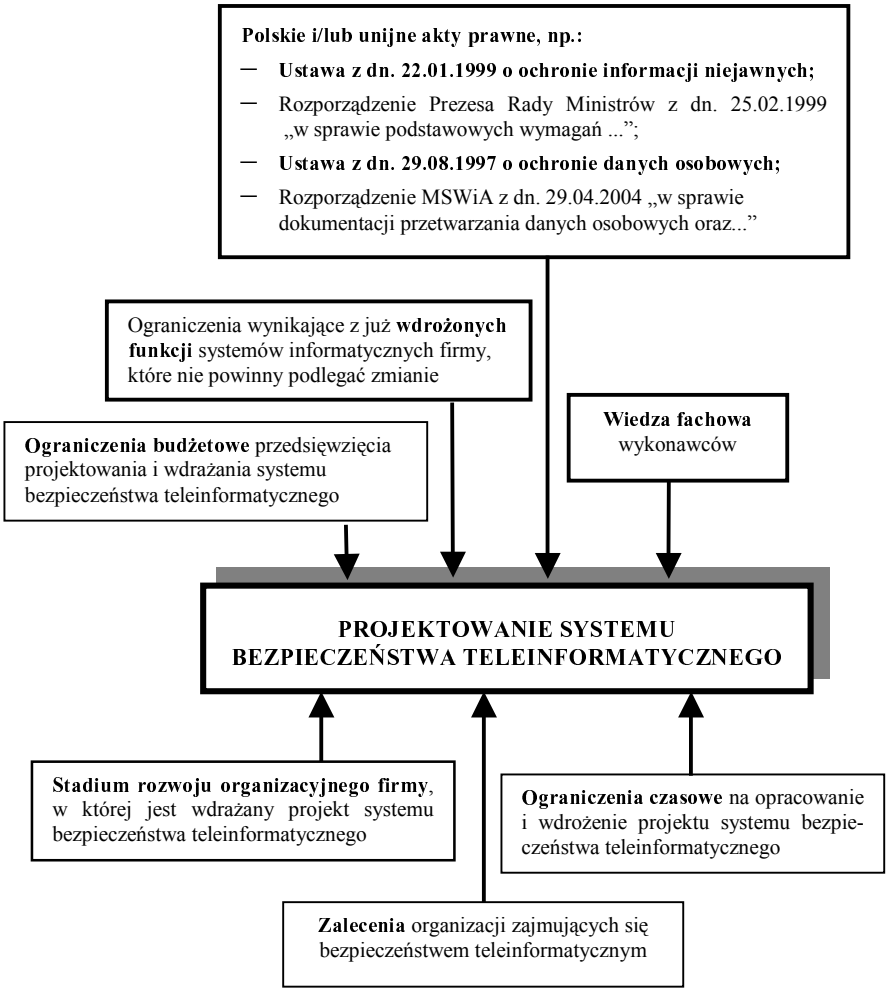
[10] Używając terminologii projektowania, można powiedzieć, że element ten jest ostatnim elementem w łańcuchu dekompozycji koncepcji projektu.

Tabela 6.2. „Klocki lego" normy PN-ISO/IEC 15408

Klasa uzasadniająca zaufanie	Rodzina uzasadniająca zaufanie	Nazwa skrócona
Klasa ACM: Zarządzanie konfiguracją	Automatyzacja CM	ACM_AUT
	Możliwości CM	ACM_CAP
	Zakres CM	ACM_SCP
Klasa ADO: Dostawa i eksploatacja	Dostawa	ADO_DEL
	Instalacja, generacja i uruchomienie	ADO_IGS
Klasa ADV: Konstruowanie	Specyfikacja funkcjonalna	ADV_FSP
	Projekt wysokiego poziomu	ADV_HLD
	Reprezentacja implementacji	ADV_IMP
	Organizacja wewnętrzna TSF	ADV_INT
	Projekt niskiego poziomu	ADV_LLD
	Zgodność reprezentacji	ADV_RCR
	Modelowanie polityki bezpieczeństwa	ADV_SPM
Klasa AGD: Dokumentacja eksploatacyjna	Instrukcja administratora	ADV_ADM
	Instrukcja użytkownika	ADV_USR
Klasa ALC: Wsparcie w czasie cyklu życia	Bezpieczeństwo konstruowania	ALC_DVS
	Naprawa usterek	ALC_FLR
	Definicja cyklu życia	ALC_LCD
	Narzędzia i techniki	ALC_TAT
Klasa ATE: Testy	Pokrycie	ATE_COV
	Głębokość	ATE_DPT
	Testy funkcjonalne	ATE_FUN
	Testowanie niezależne	ATE_IND
Klasa AVA: Szacowanie podatności	Analiza ukrytych kanałów	AVA_CCA
	Niewłaściwe używanie	AVA_MSU
	Siła funkcji zabezpieczających TOE	AVA_SOF
	Analiza podatności	AVA_VLA

6.4. Ograniczenia procesu projektowania

Każdy proces projektowania (a dokładniej: podejmowane w jego trakcie decyzje) podlega różnym ograniczeniom. Podstawowe ograniczenia związane z projektowaniem systemu bezpieczeństwa teleinformatycznego są przedstawione na rysunku 6.2 (najbardziej istotne zaznaczono pogrubieniem ramki).



Rys. 6.2. Czynniki ograniczające decyzje projektowe w procesie projektowania systemu bezpieczeństwa teleinformatycznego

7. Testowanie systemu bezpieczeństwa teleinformatycznego

Testowanie systemu bezpieczeństwa teleinformatycznego jest przedsięwzięciem kompleksowym i unikalnym – ze względu na niejednorodność (współpracujących w ramach systemu) obiektów podlegających testowaniu. Są to obiekty:

- organizacyjne (procedury i struktury organizacyjne),
- fizyczne (zamki, płoty itp.),
- techniczne (systemy ppoż., systemy nadzoru wizyjnego, elektroniczne systemy uwierzytelniania dostępu do obiektów itp.),
- programowe (IPS, zapory sieciowe, systemy uwierzytelniania logicznego),

oraz ludzie jako obiekty szczególnie wrażliwe z tego powodu, że wykonywane (lub zaniechane) przez nich działania mogą stanowić elementy ścieżki penetracji.

7.1. Przegląd rodzajów badań

Wśród podstawowych rodzajów badań (testów) mających na celu wykrycie błędów i zapewnienie o poprawności działania systemu można wyróżnić następujące:

1. **Zgodności** (ang. *validation test*) – jest to badanie systemu wykonywane w celu sprawdzenia, czy produkt spełnia określone wymagania, np. narzucone przez regulacje i standardy państwowe. Pomyślne przejście takich testów może być podstawą do wydania *certyfikatu* dla systemu, np. certyfikatu zgodności z wymaganiami PN-I-07799-2.
2. **Systemu** – jest to szczególny przypadek badania zgodności, wykonywany w celu sprawdzenia, czy wykonany system spełnia wymagania funkcjonalne określone przez użytkowników. Zwykle składa się z:
   1) **testowania wznowień** – polega na wywoływaniu różnych awarii i sprawdzaniu zdolności systemu do dalszego działania (pożądany jest tzw. stopniowy „upadek" systemu);
   2) **testowania bezpieczeństwa** – polega na przeprowadzaniu formalnych audytów bezpieczeństwa, których częścią są tzw. *testy penetracyjne* oraz, w szczególnych przypadkach, badania kodu na podatność na ataki. Cechą charakterystyczną jest testowanie rozwiązań organizacyjnych i badanie personelu na odporność na ataki socjotechniczne;

3) **testowania obciążeniowe, testowania wrażliwości, testowania efektywności** – zwykle niewykonywane w ramach budowy systemu bezpieczeństwa (są natomiast elementem procesu testowania chronionego systemu).

3. **Odbiorcze** (ang. *acceptance test*) – jest to badanie systemu lub jednostki funkcjonalnej, wykonywane zwykle przez nabywcę, na jego żądanie, po zainstalowaniu w środowisku docelowym, z udziałem dostawcy, w celu sprawdzenia, czy są spełnione wymagania zawarte w kontrakcie.
4. **Scalania** (ang. *integration test*) – jest to badanie polegające na stopniowym konstruowaniu struktury systemu i wykrywania błędów związanych z niepożądanymi zależnościami pomiędzy elementami konstrukcyjnymi. Celem jest zbudowanie z oddzielnych, przetestowanych elementów, systemu działającego zgodnie z projektem architektury. W przypadku budowy systemu bezpieczeństwa teleinformatycznego, dotyczy np. scalania elementów sprzętowych i programowych, wykorzystywanych w procesach ochronnych, z chronionym systemem teleinformatycznym.
5. **Regresyjne** – jest to badanie polegające na powtórnym wykonaniu niektórych testów, w celu upewnienia się, że nowo wprowadzone zmiany (np. zainstalowanie elementów sprzętowych i programowych wykorzystywanych przez procesy ochronne) nie wywołały niepożądanych skutków ubocznych.

7.2. Uwagi o testowaniu systemu bezpieczeństwa

W odróżnieniu od testowania np. systemu programowego, testowanie systemu bezpieczeństwa jest przedsięwzięciem kompleksowym w tym sensie, że obejmuje:

- testowanie poprawności działania zaimplementowanych ochronnych środków sprzętowych zintegrowanych z systemem teleinformatycznym,
- testowanie poprawności działania zaimplementowanych ochronnych środków programowych zintegrowanych z systemem teleinformatycznym,
- testowanie poprawności integracji ww. środków za pomocą testów: scalania i regresyjnych,
- testowanie poprawności działania zaimplementowanych środków ochrony technicznej i fizycznej,
- sprawdzenie poprawności wdrożenia ochronnych rozwiązań organizacyjnych,
- sprawdzenie odporności personelu na ataki socjotechniczne,

- sprawdzenie współdziałania ww. środków i personelu, w celu ochrony informacji przetwarzanej, przechowywanej i przesyłanej w chronionym systemie.
  Dwa ostatnie sprawdzenia są wykonywane za pomocą tzw. *testów penetracyjnych*,
- przeprowadzenie testów zgodności (audytów bezpieczeństwa) w przypadku wymagania wystawienia certyfikatu bezpieczeństwa lub,
- przeprowadzenie testów odbiorczych (zwykle jako *audyt bezpieczeństwa*, por. [7]).

Zgodnie z ogólnie uznanymi zasadami, przygotowanie do testowania, (sporządzenie np. planu testów), należy zacząć już podczas specyfikowania wymagań na system ochrony. Podstawowe informacje niezbędne do zaprojektowania planu testów to ustalenie, według jakiego standardu/normy ma być oceniany docelowy system oraz określenie docelowego poziomu ochrony[11].

Badaniem charakterystycznym dla systemu bezpieczeństwa jest audyt tego systemu. **Audytem** [9] jest nazywane postępowanie dla oceny zgodności audytowanego obiektu z wzorcem (normą, wzorcem proceduralnym lub arbitralnie ustanowionym wektorem wartości pewnych cech), prowadzone przez stronę niezależną (osobę lub zespół).

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

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

Jeżeli nie jest dotrzymany któryś z ww. punktów, to można mówić co najwyżej o *przeglądzie zabezpieczeń według listy audytowej* a nie o audycie[12].

[11] Zwykle zaprojektowanie takich badań/testów nie jest proste, np. jak wykazać, że system zapewnia dostępność informacji na poziomie 99,999% ?

[12] Więcej informacji na temat audytu bezpieczeństwa teleinformatycznego oraz jego związków z *audytem informatycznym* można znaleźć w [9].

W praktyce audyt dla celów bezpieczeństwa teleinformatycznego przeprowadza się, aby:

1) wykazać, że informacja i system teleinformatyczny zostały zabezpieczone zgodnie z ustaleniami pomiędzy zleceniodawcą a zespołem budującym system bezpieczeństwa *lub*
2) wykazać, że system bezpieczeństwa spełnia wymagania norm i standardów w tym zakresie, np. PN-I-7799-2 (to będzie ten wzorzec, o którym mowa w ww. definicji audytu) *lub*
3) wystawić ocenianemu systemowi tzw. *certyfikat bezpieczeństwa lub*
4) ocenić jakość systemu bezpieczeństwa i przedstawić ocenę zleceniodawcy, aby podjął decyzję (modernizujemy/zostawiamy tak jak jest).

8. Podsumowanie

W artykule przedstawiony został zarys czynności związanych z projektowaniem systemu bezpieczeństwa teleinformatycznego. Czynności te zostały przedstawione na tle cyklu życia ww. systemu; nacisk położono na etapy analizy, projektowania i testowania. Informacje dotyczące etapu wytwarzania, w szczególności dokumentowania systemu bezpieczeństwa teleinformatycznego, można znaleźć w pierwszej części publikacji [10] oraz w [1].

Ze względu na specyficzny sposób realizacji etapów analizy i projektowania, można zaryzykować stwierdzenie, że są one sterowane analizą ryzyka. Implikuje to m.in. posiadanie odpowiednich kwalifikacji przez zespół projektujący system bezpieczeństwa teleinformatycznego – doświadczenia projektanta oprogramowania mogą być w takim przedsięwzięciu niewystarczające.

Należy podkreślić, że niniejszy artykuł przedstawia jedynie zarys problematyki projektowania systemu bezpieczeństwa teleinformatycznego – pokazuje, jak w tradycyjny schemat projektowania wpisuje się projektowanie takiego szczególnego systemu. Celem podstawowym było pokazanie, że o ile np. projekt sieci teleinformatycznej o wysokim poziomie dostępności do przetwarzanej w niej informacji jest na pewno projektem samym w sobie skomplikowanym, o tyle celów bezpieczeństwa na pewno się nie osiągnie, jeżeli nie będzie on realizowany w ramach szerszego projektu **systemu bezpieczeństwa teleinformatycznego** (por. rozważania o kompleksowości w rozdz. 4 i rys. 4.3).

Literatura

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

[2] Liderman K., Arciuch A.: *Projektowanie systemów komputerowych*, BEL Studio, Warszawa, 2001.

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

[4] Liderman K.: *System bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 17, WAT, Warszawa, 2002.

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

[6] Liderman K.: *Oszacowania jakościowe ryzyka dla potrzeb bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 19, WAT, Warszawa, 2003.

[7] Liderman K., Patkowski A. E.: *Metodyka przeprowadzania audytu z zakresu bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 19, WAT, Warszawa, 2003.

[8] Liderman K.: *Zarys zastosowania metod sieciowych do wyznaczania czasu realizacji audytu bezpieczeństwa teleinformatycznego*, Biuletyn IAiR, nr 20, WAT, Warszawa, 2004.

[9] Liderman K.: *Czy „audyt bezpieczeństwa teleinformatycznego" jest tym samym co „audyt informatyczny"?*, Biuletyn IAiR, nr 21, WAT, Warszawa, 2004.

[10] Liderman K. (red.): *Bezpieczeństwo teleinformatyczne. Problemy formalne i techniczne*, WAT, Warszawa, 2005.

[11] Pressman R.S.: *Praktyczne podejście do inżynierii oprogramowania*, WNT, Warszawa, 2004.

[12] Trocki M. i in.: *Zarządzanie projektami*, PWE, Warszawa, 2003.

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

[14] PN-I-07799-2: *Systemy zarządzania bezpieczeństwem informacji – specyfikacja i wytyczne do stosowania*.

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

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

Recenzent: dr hab. inż. Antoni Donigiewicz

Praca wpłynęła do redakcji: 17.04.2005