**Jakub Piwowarczyk**

**System bezpieczeństwa instytucji**

**Referat z przedmiotu: Ochrona informacji niejawnych**

Prowadzący: dr inż. Jarosław Siuda

Praca przyjęta

.....................................

(data i podpis promotora)

**Uniwersytet Zielonogórski**

**Wydział Ekonomii i Zarządzania**

Zielona Góra 2020

**Spis treści**

[Wstęp 3](#_Toc35460085)

[Rozdział I Podstawowe pojęcia i wprowadzenie 4](#_Toc35460086)

[Rozdział II Fazy realizacji i ogólny schemat funkcjonowania systemu bezpieczeństwa instytucji. 9](#_Toc35460087)

[Rozdział III Zapis sformalizowany modelu trójpoziomowego 13](#_Toc35460088)

[Rozdział IV Zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa 16](#_Toc35460089)

[Zakończenie 19](#_Toc35460090)

[Źródła 20](#_Toc35460091)

[Spis rysunków 21](#_Toc35460092)

# Wstęp

System bezpieczeństwa instytucji to ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia jej niezakłóconego funkcjonowania. Każda instytucja aby w pełni sprawnie realizowała swoje zadania wymaga identyfikacji   
i realizacji działań warunkujących jej efektywne funkcjonowanie, w tym działań podejmowanych w obszarze bezpieczeństwa teleinformatycznego, na które składa się zbiór zagadnień z dziedziny telekomunikacji i informatyki. Zadania te wiążą się   
z szacowaniem i kontrolą ryzyka wynikającego z korzystania z komputerów, sieci komputerowych i przesyłania danych do zdalnych lokalizacji, rozpatrywany   
z perspektywy poufności, integralności i dostępności.

# Rozdział I Podstawowe pojęcia i wprowadzenie

Aby wiedzieć dokładniej czym jest system bezpieczeństwa instytucji niezbędna jest identyfikacja pojęć takich jak:

* System - obiekt fizyczny lub abstrakcyjny, w którym można wyodrębnić zespół lub zespoły elementów wzajemnie powiązanych w układy oraz realizujących jako całość funkcję nadrzędną lub zbiór takich funkcji.
* Bezpieczeństwo - stan dający poczucie pewności i gwarancję jego zachowania oraz szanse na doskonalenie.
* Instytucja - organizacja będąca zespołem współdziałających osób wyposażonych   
  w zasoby.

Warto też przedstawić definicję tego czym jest ryzyko, a także definicji związanych   
z ryzkiem:

* Ryzyko to prawdopodobieństwo wystąpienia zagrożenia, które, wykorzystując podatność(ci) aktywu, może doprowadzić do jego uszkodzenia lub zniszczenia.
* Szacowanie ryzyka to całościowy proces analizy i oceny ryzyka.
* Postępowanie z ryzykiem to proces wyboru i wdrażania środków modyfikujących ryzyko.
* Zarządzanie ryzykiem to proces identyfikowania, kontrolowania   
  i minimalizowania lub eliminowania ryzyka dotyczącego bezpieczeństwa, które może dotyczyć systemów informacyjnych, przy zachowaniu akceptowalnego poziomu kosztów.

System bezpieczeństwa instytucji powinien zawierać w sobie system bezpieczeństwa teleinformatycznego instytucji, a ten z kolei, system bezpieczeństwa autonomicznych systemów teleinformatycznych. Andrzej Białas definiuje system bezpieczeństwa teleinformatycznego instytucji jako ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia właściwego poziomu atrybutów bezpieczeństwa w systemach teleinformatycznych instytucji traktowanych jako całość. Z kolei system bezpieczeństwa autonomicznego systemu teleinformatycznego jako ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia właściwego poziomu atrybutów bezpieczeństwa w danym systemie teleinformatycznym.

W temacie tym kluczowa jest znajomość definicji bezpieczeństwa informacji. Jest to zachowanie poufności, integralności i dostępności informacji, czyli informacja nie jest ujawniana osobom nieupoważnionym, jest ona dokładna i kompletna oraz dostępna   
i użyteczna na żądanie upoważnionego personelu.

Przechowywane w bazach danych informacje, powinny podlegać ochronie. Dotyczy to w szczególności danych o charakterze strategicznym, o kluczowym znaczeniu dla funkcjonowania przedsiębiorstwa. Projekt systemu informacyjnego wspomagającego zarządzanie strategiczne, powinien uwzględniać problematykę bezpieczeństwa informacji, poprzez określenie ogółu zasad, metod i narzędzi ochrony i nadzoru nad informacją.

Do atrybutów bezpieczeństwa zalicza się:

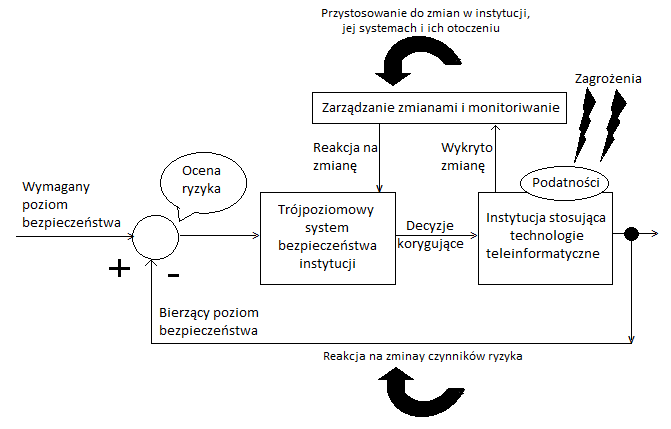
* poufność – oznacza że informacja nie jest dostępna dla nieautoryzowanych osób, podmiotów lub procesów,
* autentyczność – oznacza, że tożsamość podmiotu lub zespołu jest taka jak deklarowano,
* dostępność – daje możliwość wykorzystania w danym czasie przez osobę, która ma do tego prawo,
* integralność danych – ta właściwość oznacza że dane nie zostały zmienione lub zniszczone w sposób nieautoryzowany,
* integralność systemowa – właściwość umożliwiająca systemowi realizację zamierzonej funkcji w nienaruszony przez nieautoryzowane manipulacje (celowe lub przypadkowe) sposób;
* integralność – integralność danych oraz systemu,
* rozliczalność - oznacza, że działania podmiotu np. użytkownika mogą być mu przypisane,
* niezawodność – spójne, zamierzone zachowanie i skutki.

Korzyści z wdrożenia i stosowania systemów zarządzania lub zapewnienia bezpieczeństwa informacji:

* minimalizacja ryzyka wystąpienia zdarzeń związanych z bezpieczeństwem informacji (w tym również kar), czyli pro-aktywna identyfikacja podatności aktywów informacyjnych, zagrożeń i ich skutków w odniesieniu do sterowania operacyjnego oraz definiowanie odpowiednich działań zmniejszających ryzyko,
* gotowość organizacji na incydenty związane z bezpieczeństwem informacji oraz dzięki odpowiednim procedurom ich skuteczne przezwyciężenie (efektywna odpowiedź na incydenty minimalizująca ich wpływ na organizację),
* podniesienie wiarygodność organizacji w oczach klientów, inwestorów   
  i udziałowców (interesariuszy),
* zapewnienie bezpieczeństwa interesom Klientów,
* pozytywny wpływ na ochronę i poprawę reputacji firmy i danej marki,
* zapewnienie zgodności z mającymi zastosowanie przepisami prawa lub wymaganiami ubezpieczycieli,
* zapewnienie ochrony aktywów informacyjnych,
* wzrost świadomości pracowników i osób pracujących w imieniu organizacji odnośnie bezpieczeństwa informacji.

Architektura systemu bezpieczeństwa to układ, kompozycja elementów składających się na ten system, wykorzystywanych przez procesy zarządzania bezpieczeństwem. Reprezentuje w sposób statyczny wszelkie struktury danych, opisujące system bezpieczeństwa według modelu trójpoziomowego, wykorzystywane lub przetwarzane przez zbiór procesów zarządzania bezpieczeństwem.

Na rysunku została przedstawiona instytucja wykorzystująca technologie teleinformatyczne wraz jej systemem bezpieczeństwa. Podstawowym zadaniem tego systemu jest utrzymywanie bezpieczeństwa w instytucji na stałym, adekwatnym do jej potrzeb poziomie. Odbywa się to głównie przez kontrolowanie ryzyka.



Rysunek 1 Instytucja i jej system bezpieczeństwa

Źródło: A. Białas, Ochrona informacji we współczesnej firmie lub instytucji, WNT, Warszawa 2006

Instytucja i jej systemy teleinformatyczne cechują się różnorodnymi podatnościami, wykorzystywanymi przez zagrożenia. Z tego wynika ryzyko, którego do końca nie można wyeliminować, a które powinno być utrzymywane na zaakceptowanym dla instytucji poziomie. System bezpieczeństwa instytucji powinien prawidłowo reagować na zmianę czynników ryzyka, utrzymując ryzyko na wymaganym poziomie. Za to odpowiedzialna jest pętla korygująca wpływ zmiany czynników ryzyka. Bieżący poziom ryzyka jest porównywany z zadanym (akceptowanym) i na tej podstawie system bezpieczeństwa wypracowuje decyzje korygujące, co stanowi istotę procesów zarządzania ryzykiem. Oznacza to, że czynniki ryzyka, czyli przede wszystkim zagrożenia i podatności, są pod kontrolą, a odpowiadające im ryzyko jest na poziomie akceptowalnym w danej instytucji.

System bezpieczeństwa jest wypracowywany dla danej instytucji, stąd musi on dokładnie odzwierciedlać realia jej funkcjonowania i eksploatowanych w niej systemów, a także otoczenia. Tylko w takim wypadku pętla korygująca jest w stanie prawidłowo funkcjonować, co nie zawsze musi zachodzić.

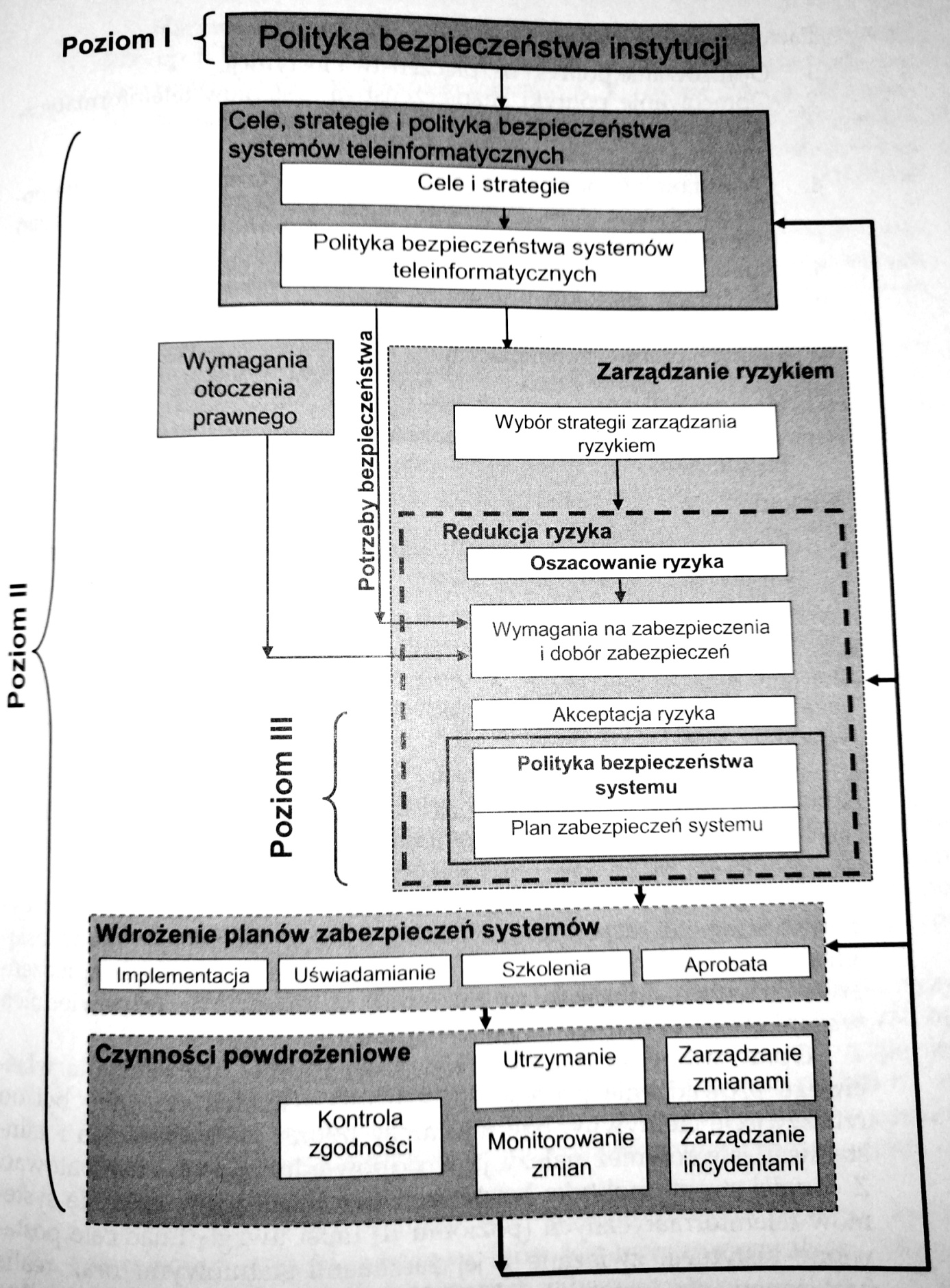
Założenia systemu bezpieczeństwa instytucji:

1. System powinien być kompleksowy, to znaczy obejmować wszystkie poziomy modelu odniesienia - od poziomu funkcjonowania instytucji, po szczegóły techniczne, prawne i organizacyjne.
2. Należy uwzględnić różnorodność charakteru procesów występujących w tej dziedzinie - występują tu procesy ściśle techniczne, jak i pozatechniczne.
3. W maksymalnym stopniu należy zapewnić komputerowe wsparcie procesów zarządzania systemem bezpieczeństwa, a niektóre z procesów starać się zautomatyzować.
4. System bezpieczeństwa powinien mieć zdolność przystosowania się do zmian zachodzących w systemach teleinformatycznych i ich otoczeniu oraz do zmian   
   w środowisku zagrożeń, utrzymując w czasie zadany poziom bezpieczeństwa wyznaczony na podstawie analizy ryzyka.
5. Należy zapewnić skalowość i modularność, w tym możliwość wymiany modułów reprezentujących procesy.
6. Należy zapewnić zgodność z normami międzynarodowymi dotyczącymi bezpieczeństwa teleinformatycznego.

# Rozdział II Fazy realizacji i ogólny schemat funkcjonowania systemu bezpieczeństwa instytucji.

System bezpieczeństwa w instytucji powinien być zgodny z modelem odniesienia. Można wyróżnić trzy fazy jego realizacji, mające odzwierciedlenie w modelu cyklu życia:

* Projekt i planowanie - od określenia potrzeb po selekcję zabezpieczeń.
* Weryfikacja, walidacja i wdrożenie projektu - od instalacji zabezpieczeń po testy ich skuteczności, potwierdzające osiągnięcie zakładanego poziomu bezpieczeństwa.
* Bezpieczna eksploatacja - utrzymanie zakładanego poziomu bezpieczeństwa przy zmianach zachodzących w instytucji i jej systemach oraz w środowisku zagrożeń, w tym zakończenie jego eksploatacji lub tak zwane zbywanie jego elementów.



Rysunek 2 Schemat zarządzania bezpieczeństwem teleinformatycznym

Źródło: A. Białas, Ochrona informacji we współczesnej firmie lub instytucji, WNT, Warszawa 2006

Na rysunku jest przedstawiony ogólny schemat zarządzania bezpieczeństwem na podstawie polityki na wszystkich poziomach modelu, ze szczególnym uwzględnieniem poziomu II, gdyż na nim koncentruje się zarządzanie bezpieczeństwem teleinformatycznym. W celu uproszczenia zasygnalizowano jedynie istnienie najważniejszych sprzężeń zwrotnych. W rzeczywistości zależności między procesami są o wiele bardziej skomplikowane, gdyż system bezpieczeństwa instytucji musi podlegać nieustannym korektom, adaptacjom i doskonaleniom.

Proces budowy systemu bezpieczeństwa:

Faza I:

1. Opracowanie polityki bezpieczeństwa instytucji.
2. Opracowanie polityki bezpieczeństwa systemów teleinformatycznych instytucji (bezpieczeństwa teleinformatycznego).
3. Wybór strategii zarządzania ryzykiem.
4. Określenie wymagań dotyczących zabezpieczeń na podstawie potrzeb otoczenia prawnego.
5. Dobór zabezpieczeń.
6. Akceptacja zredukowanego ryzyka.
7. Opracowanie polityki bezpieczeństwa poszczególnych systemów oraz ich planów zabezpieczeń.

Faza II:

1. Wdrożenie planów zabezpieczeń i sprawdzenie skuteczności zabezpieczeń.

Faza III:

1. Prowadzenie działań powdrożeniowych zmierzających do utrzymywania osiągniętego poziomu bezpieczeństwa w toku eksploatacji systemów.

Fazy te stanowią elementy cyklu życia systemu, podobnie do zawartych w modelu PDCA (Plan, Do, Check, Act). Można zauważyć, że "Planuj" to faza I, "Wykonaj   
i Sprawdzaj" łącznie to faza II, "Działaj" zaś odpowiada trzeciej.   
 Wszelkie działania zmierzające do budowy systemu bezpieczeństwa instytucji powinny rozpocząć się od analizy procesów biznesowych pod kątem ich zapotrzebowania na bezpieczeństwo, wyrażanego za pomocą celów.  
 Po wytyczeniu celów bezpieczeństwa dla instytucji należy sprecyzować strategie określające, w jaki sposób te cele mają zostać osiągnięte. W efekcie prowadzi to do wypracowania polityki bezpieczeństwa instytucji (pierwszego poziomu) i stworzenia odpowiednich warunków do opracowania polityki poziomu drugiego. Opracowanie tej polityki ma z kolei istotne znaczenie dla właściwego prowadzenia procesu zarządzania ryzykiem, tak aby był on rzeczywiście efektywny. Zróżnicowane rezultaty z analizy ryzyka lub zróżnicowane wytyczne dotyczące zabezpieczeń, wynikające z analiz towarzyszących ochronie podstawowej teleinformatyki , mogą wymuszać opracowania różnych form polityki (poziom III) dla poszczególnych systemów.

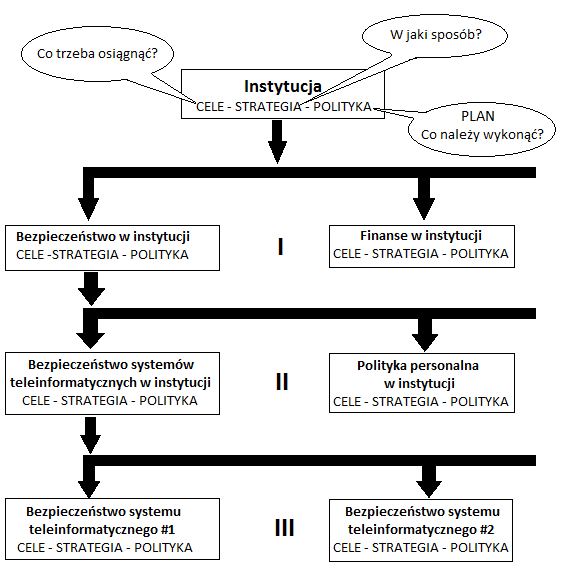
Ogólnie rzecz biorąc, polityka stanowi zawsze zbiór specyficznych zasad, celów   
i wymagań dotyczących przetwarzania informacji, wypracowanych w instytucji w celu wspomagania jej działalności. Najważniejszym elementem polityki jest wskazanie zasobów, które mają podlegać ochronie i sposobu, w jaki się to ma odbywać.

Te same zadania statutowe mogą być realizowane przez systemy działające   
w różnych środowiskach zagrożeń, stąd należy więc zidentyfikować te zagrożenia, ocenić realność związanych z nimi podatności, określić możliwość wystąpienia oraz potencjalne skutki. Tego typu działania obejmuje analiza ryzyka.   
 W instytucji powinna zostać przyjęta strategia zarządzania ryzykiem, przedstawiająca generalnie czy i w jaki sposób ryzyko ma być ograniczone   
i wskazywać metodę jego oceny. Oszacowane ryzyko jest więc czynnikiem decydującym o wyborze wymagań na zabezpieczenia i w konsekwencji o selekcji zabezpieczeń. Obowiązuje tu prosta zasada: im zagrożenia są poważniejsze, tym zabezpieczenia powinny być silniejsze.

Instytucja i jej systemy teleinformatyczne funkcjonują zawsze w pewnym otoczeniu prawnym, które jest trzecim czynnikiem, decydującym o wymaganiach do tyczących zabezpieczeń.

Otoczenie prawne to ogół przepisów prawnych, statutowych, regulacji kontraktowych, które instytucja, jej partnerzy handlowi, kontrahenci i usługodawcy muszą spełniać. Przepisy te nakazują prowadzenie działań zgodnych z prawem oraz ochronę wyspecyfikowanych w przepisach rodzajów informacji wrażliwych. Prawo nakazuje ochronę danych osobowych, informacji niejawnych, finansowych, dotyczących zdrowia i wielu innych rodzajów informacji, zwanych tajemnicami prawnie chronionymi. To również prawo decyduje o tym w jaki sposób można świadczyć różnego typu usługi elektroniczne, na przykład przez operatorów sieci, czy   
w jaki sposób można prowadzić handel na odległość.

# Rozdział III Zapis sformalizowany modelu trójpoziomowego



Rysunek 3 Trójpoziomowy model odniesienia

Źródło: A. Białas, Ochrona informacji we współczesnej firmie lub instytucji, WNT, Warszawa 2006

Na każdym z poziomów modelu odniesienia występują trójki pojęć: cele, strategie osiągania tych celów i polityka, które są podstawowymi elementami modelu, poddawanymi procesowymi elementami modelu, poddawanymi procesowi uszczegóławiania i transformacji w systemie bezpieczeństwa instytucji.

Zapis sformalizowany modelu trójpoziomowego.

* BL (Business Level) - zadania statutowe instytucji (misja), do których realizacji ją powołano: komercyjne, administracyjne, militarne lub inne, gdzie BL jest określony za pomocą czwórki pojęć:

BL = <BO, BS, BP, DD>

przy czym: BO (Business Objectives) -cele działania, czyli zadanie statutowe; BS (Business Strategies) - strategie osiągania celów działania; BP (Business Policy) - polityka działania instytucji; DD (Dependency Degree) - umowny stopień zaangażowania środków teleinformatycznych w realizację danego celu działania instytucji; wyraża uzależnienie realizacji celów od niezakłóconej pracy systemów teleinformatycznych i towarzyszące temu ryzyko biznesowe.

* BLS (Business Level Security) - bezpieczeństwo funkcjonowania instytucji (poziom I), gdzie BLS jest określony za pomocą trójki pojęć:

BLS = <SO, SS, SP>

przy czym: SO (Security Objectives) - cele bezpieczeństwa instytucji; SS (Security Strategies) - strategie bezpieczeństwa instytucji; SP (Security Policy) - polityka bezpieczeństwa instytucji.

* CITSL (Corporate IT Security Level) - bezpieczeństwo ogółu systemów teleinformatycznych instytucji (poziom II), gdzie CITSL jest określony   
  za pomocą trójki pojęć:

CITSL = <CITO, CITS, CITP>

przy czym: CITO (Corporate IT Security Objectives) - cele bezpieczeństwa teleinformatycznego instytucji; CITS (Corporate IT Security Strategies) -strategie bezpieczeństwa teleinformatycznego instytucji; CITP (Corporate IT Security Policy) - polityka bezpieczeństwa teleinformacyjnego instytucji.

* DITSL (Department IT Security Level) - bezpieczeństwo ogółu systemów teleinformatycznych działających w oddziale instytucji (opcjonalny poziom IIa), gdzie DITSL jest określany za pomocą trójki pojęć:

DITSL = <DITO, DITS, DITP>

przy czym: DITO (Department IT Security Objectives) - cele bezpieczeństwa teleinformatycznego oddziału instytucji; DITS (department IT Security Strategies) - strategie bezpieczeństwa teleinformatycznego oddziału instytucji; DITP (Department IT Security Policy) - polityka bezpieczeńśtwa teleinformatycznego oddziału instytucji.

* ITSSL (IT System Security Level) - Bezpieczeństwo konkretnego systemu

teleinformatycznego działającego w instytucji lub jej oddziale (poziom III), gdzie ITSSL jest określany za pomocą trójki pojęć:

ITSSL = <ITSO, ITSS, ITSP>

przy czym: ITSO (IT System Security Objectives) - cele bezpieczeństwa danego systemu; ITSS (IT System Security Strategies) -strategie bezpieczeństwa systemu; ITSP (IT System Security Policy) - polityka bezpieczeństwa systemu.

Przyjmijmy ponadto następujące określenia pojęć związanych z budową systemu bezpieczeństwa instytucji:

* LE (Legal Enviroment - Legal, Statutory and Contractual Requirements) - otoczenie prawne gdzie LE jest określane za pomocą

LE = <LB,OCAL,SDMP>

przy czym: LB (Legal Basis)- podstawa prawna (akt); OCAL (Operation Compliance with Applicable Legislation, Statutes and Contracts) - postanowienia ustaw i rozporządzeń, zarządzeń i umów zewnętrznych, dotyczących funkcjonowania systemów teleinformatycznych instytucji w zgodzie z prawem; SDMP (Sensitive Data Mandatory Protection) - tajemnice prawnicze chronione, chronione we własnym interesie i na podstawie umów o zachowaniu poufności.

* RA (Risk Assessed) - rezultat przeprowadzonej w instytucji analizy ryzyka, gdzie RA jest określony za pomocą

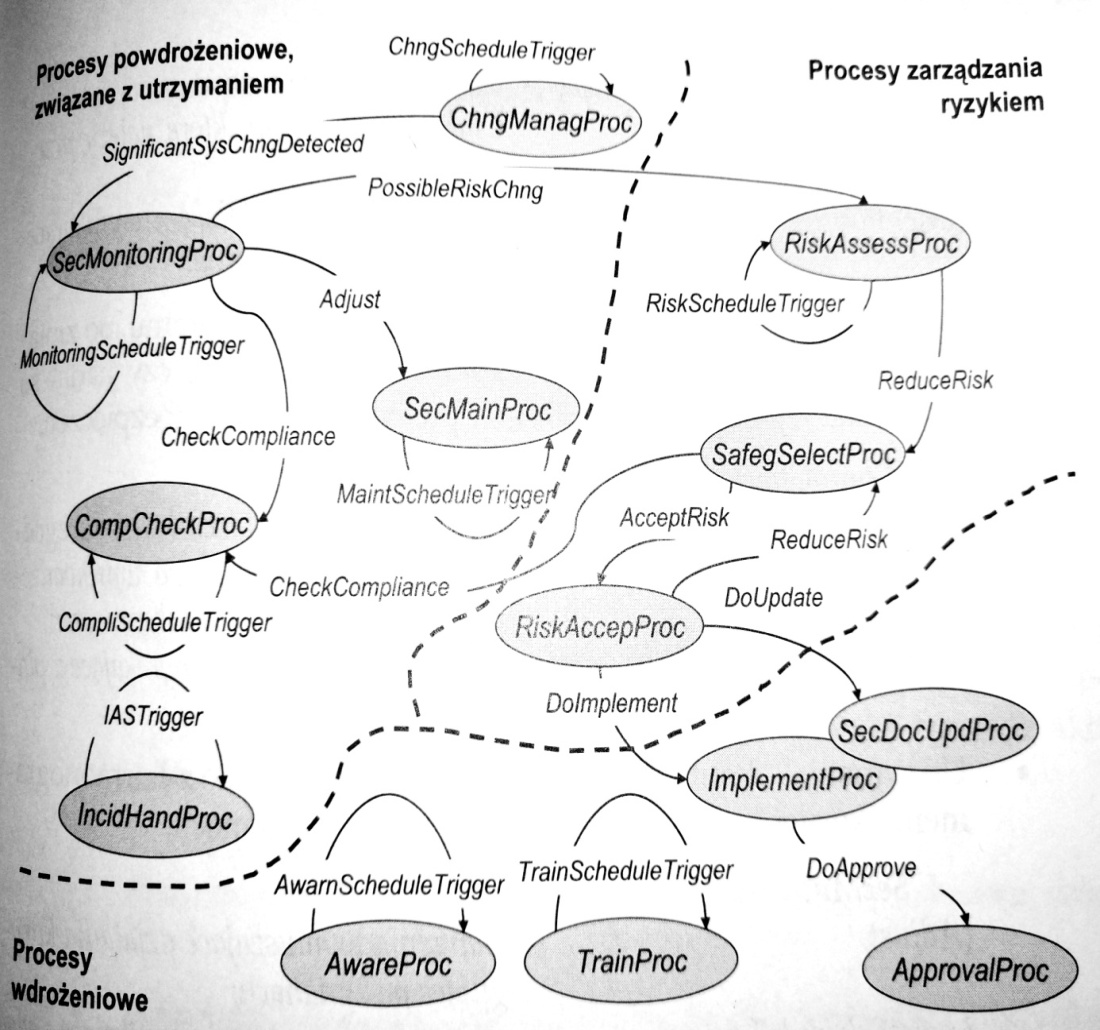
RA = <RSL>

przy czym RSL (Risk Scenarios List) - uporządkowana lista scenariuszy ryzyka wraz z ich wielkościami ryzyka.

# Rozdział IV Zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa

Umownie wyodrębniono trzy grupy procesów:

* Procesy zarządzania ryzykiem, ukierunkowane na dobór właściwych zabezpieczeń.
* Procesy wdrożeniowe, ukierunkowane na ich implementację.
* Procesy powdrożeniowe, których głównym zadaniem jest utrzymywanie stanu bezpieczeństwa i reagowanie na zmiany w systemach i ich otoczeniu.



Rysunek 4 Zbiór procesów zarządzania bezpieczeństwem teleinformatycznym

A. Białas, Ochrona informacji we współczesnej firmie lub instytucji, WNT, Warszawa 2006

Przyjęto następujący zbiór tych współbieżnych procesów:

* Zarządzanie zmianami - wykrywanie i wstępna ocena wpływu wszelkich zmian zachodzących w systemach teleinformatycznych na aktualny stan ich bezpieczeństwa. Zmiany znaczące są przekazywane do procesu monitorowania, gdzie są poddawane szczegółowej analizie, zmiany zaś o mniejszej skali, na przykład dotyczące konfiguracji, są analizowane na bieżąco. Proces wyzwalany jest zdarzeniami wynikającymi z harmonogramu.

**ChngManagProc** (ChngScheduleTrigger) - zdarzenia wyzwalające, wynikające   
z planu zarządzania zmianami

* Monitorowanie bezpieczeństwa - permanentne śledzenie wpływu wykrytych zmian w systemach i ich otoczeniu.

**SecMonitiringProc** (SignificantSysChngDetected - wykryto poważne zmiany   
w systemie i lub jego otoczeniu, które należy przeanalizować;

MonitoringScheduleTrigger) - zdarzenia wyzwalające, wynikające z planu monitorowania.

* Kontrola zgodności - sprawdzenie (według harmonogramu, po zmianach albo po wprowadzeniu nowych zabezpieczeń), czy nadal są spełnione wymagania, określone w polityce i planach zabezpieczeń.

**CompCheckProc** (CheckCompliance, -zdarzenia wymuszające kontrolę zgodności po zmianach lub po wprowadzeniu nowych elementów zabezpieczeń;  
CompliScheduleTrigger) - zdarzenia wyzwalające, wynikające z planu kontroli zgodności.

* Utrzymanie - kontrolowanie zabezpieczeń zgodnie z harmonogramem   
  i korygowanie ich funkcjonowania po zmianach.

**SecMainProc** (Adjust, - zdarzenia wymuszające działania korygujące po zmianach;  
MaintScheduleTrigger) - zdarzenia wyzwalające, wynikające z planu utrzymania.

* Zarządzanie incydentami - bieżące zarządzanie incydentami według planu reagowania i schematu analizy incydentów (IAS - Incident Analysis Scheme), wypracowanych w instytucji.

**IncidHandProc** (IASTrigger) - zdarzenia wyzwalające, wynikające ze schematu analizy incydentów - reakcja.

* Analiza ryzyka - wymuszana uwarunkowaniami opisanymi w polityce bezpieczeństwa, na przykład prowadzona według planu: co rok, po poważnych incydentach, po objawieniu się nowych form zagrożeń o znacznej powadze,   
  a także wymuszana znaczącymi zmianami, jakie zaszły w systemach.  
  **RiskAssessProc** (PossibleRiskChng, - zdarzenia wymuszające analizę ryzyka po znaczących zmianach w systemach;

RiskScheduleTrigger) - zdarzenia wymuszające analizę ryzyka zgodnie z polityką bezpieczeństwa.

* Wybór zabezpieczeń - mających obniżyć wykryte zbyt wysokie ryzyko.  
  **SafeSelectProc** (ReduceRisk) - zdarzenia wymuszające konieczność obniżenia ryzyka przez modyfikację systemu zabezpieczeń.
* Akceptacja ryzyka - akceptacja bieżącego ryzyka przez kierownictwo.  
  **RiskAcceptProc** (AcceptRisk) - zdarzenia wymuszające ocenę bieżącego ryzyka - jego akceptację bądź wskazanie potrzeby dalszej redukcji.
* Aktualizacja doumentacji - wprowadzenie zatwierdzonych zmian do dokumentacji systemu bezpieczeństwa.

**SecSysDocUpdProc** (DoUpdate) - zdarzenia wymuszające aktualizację dokumentacji systemu bezpieczeństwa.

* Wdrożenie zabezpieczeń - wdrożenie nowego zabezpieczenia i sprawdzenie jego skuteczności; proces ściśle współpracuje z poprzednim, gdyż każde wdrożenie lub jego zmiana wymaga aktualizacji dokumentacji zabezpieczeń.

**ImplementProc** (DoImplement) -zdarzenia wymuszające wdrożenie dobranych zabezpieczeń.

* Aprobata - dopuszczenie systemów do eksploatacji po modyfikacji systemu zabezpieczeń.   
  **ApprovalProc** (DoApprove) - zdarzenia wymuszające proces aprobaty.
* Uświadamianie - permanentne działania, utrzymujące właściwy stan świadomości bezpieczeństwa wśród personelu.

**AwareProc** (AwarnScheduleTrigger) - zdarzenia wyzwalające, wynikające   
z programu dziłań uświadamiających.

* Szkolenie i warsztaty według programu wypracowanego w instytucji.  
  **TrainProc** (TrainScheduleTrigger) - zdarzenia wyzwalające, wynikające   
  z programu szkolenia.

Podstawowym procesem, odpowiedzialnym w cyklu życia za ciągłe przystosowanie się systemu bezpieczeństwa do zmian zachodzących w systemach teleinformatycznych   
i ich otoczeniu jest SecMainProc. Same zmiany są wykrywane przez ChngManagProc, analizowane zaś przez SecMonitoringProc.

# Zakończenie

W pracy zostały przedstawione najważniejsze pojęcia w zakresie systemu bezpieczeństwa instytucji. Została omówiona metoda budowy systemu bezpieczeństwa, wyróżniając fazy jego cyklu życia. Zdefiniowane zostały struktury informacji opisujące system oraz zbiór składających się nań procesów. Przedstawiony został także zapis sformalizowany modelu trójpoziomowego oraz zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa. Są to podstawowe elementy, bez których system bezpieczeństwa instytucji nie mógłby być tak efektywnie prowadzony. Bardzo ważne dla organizacji systemu bezpieczeństwa instytucji jest to, aby każdy z elementów systemu bezpieczeństwa był dobrze opracowany.

# Źródła

A. Białas, Ochrona informacji we współczesnej firmie lub instytucji, WNT, Warszawa 2006

<https://www.iso.org.pl/uslugi-zarzadzania/wdrazanie-systemow/systemy-bezpieczenstwa-informacji/>

<https://mpwik.lubin.pl/pdf/Polityka-bezpieczenstwa-informacji.pdf>

<https://mfiles.pl/pl/index.php/Bezpiecze%C5%84stwo_informacji>

# Spis rysunków

[Rysunek 1 Instytucja i jej system bezpieczeństwa 7](#_Toc35460093)

[Rysunek 2 Schemat zarządzania bezpieczeństwem teleinformatycznym 10](#_Toc35460094)

[Rysunek 3 Trójpoziomowy model odniesienia 13](#_Toc35460095)

[Rysunek 4 Zbiór procesów zarządzania bezpieczeństwem teleinformatycznym 16](#_Toc35460096)