**Żaklina Dworska**

**System bezpieczeństwa instytucji**

**Uniwersytet Zielonogórski**

**Wydział Ekonomii i Zarządzania**

Zielona Góra 2020

**SPIS TREŚCI**

[**Wstęp 3**](#_Toc34504158)

[**Rozdział 1. Podstawowe pojęcia i wprowadzenie 4**](#_Toc34504159)

[**Rozdział 2. Fazy realizacji i ogólny schemat funkcjonowania systemu bezpieczeństwa instytucji 6**](#_Toc34504160)

[**Rozdział 3. Zapis sformalizowany modelu trójpoziomowego 9**](#_Toc34504161)

[**Rozdział 4. Zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa 12**](#_Toc34504162)

[**Zakończenie 16**](#_Toc34504163)

[**Spis literatury 17**](#_Toc34504164)

# Wstęp

Bezpieczeństwo informacji można osiągnąć, wdrażając odpowiedni zestaw zabezpieczeń, którymi mogą być polityki, procesy, procedury, struktury organizacyjne oraz funkcje oprogramowania i sprzętu. Zabezpieczenia powinny być ustanawiane, wdrażane, monitorowane, przeglądane i w razie potrzeby ulepszane tak, aby zapewnić spełnienie poszczególnych celów związanych z systemem bezpieczeństwa prowadzonej instytucji.

Niezwykle ważne jest „probiznesowe” podejście do zagadnień systemu bezpieczeństwa instytucji, uwzględniające rachunek kosztów i zysków, ryzyko biznesowe dla instytucji – wszelkie podejmowane działania powinny być prowadzone w kontekście tego, czym instytucja się zajmuje i ponadto powinny prowadzić do poprawy jej pozycji na rynku lub ogólnego postrzegania w społeczeństwie.

#

# Rozdział 1. Podstawowe pojęcia i wprowadzenie

Identyfikacja i realizacja działań determinuje efektywne funkcjonowanie każdej instytucji, jednym z obszarów kontroli postępowania jest bezpieczeństwo teleinformatyczne. Wszelkie czynności podjęte powinny mieć zasadniczy wpływ na funkcjonowanie i innowacyjność procesów oraz dążyć do poprawy pozycji na rynku.

Pojęcie, które definiuje wszystkie działania zaangażowane w system bezpieczeństwa brzmi następująco:

**System bezpieczeństwa instytucji** to ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia jej niezakłóconego funkcjonowania [Białas 2006, s.182].

Opierając się na I modelu odniesienia, można wywnioskować, że system bezpieczeństwa instytucji powinien zawierać w sobie kolejne dwa systemy:

1. **System bezpieczeństwa teleinformatycznego instytucji** to ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia właściwego poziomu atrybutów bezpieczeństwa w systemach teleinformatycznych instytucji traktowanych jako całość. [Białas 2006, s.183].

2. **System bezpieczeństwa autonomicznego systemu teleinformatycznego** to ogół spójnych środków i skoordynowanych przedsięwzięć, zastosowanych w celu zapewnienia właściwego poziomu atrybutów bezpieczeństwa w danym systemie teleinformatycznym. [Białas 2006, s.183].

Kolejnym ważnym pojęciem jest „architektura systemu bezpieczeństwa”, reprezentuje w sposób statyczny wszelkie struktury danych, opisuje system bezpieczeństwa od ogólnych stwierdzeń po szczegóły dotyczące działania zabezpieczeń w systemach teleinformatycznych, instrukcje i procedury.

**Architektura systemu bezpieczeństwa** to układ, kompozycja elementów składających się na ten system, wykorzystywanych przez procesy zarządzania bezpieczeństwem [Białas 2006, s.183].

Architektura bezpieczeństwa na poziomie instytucji odnosi się do procesów biznesowych instytucji, na poziomie systemów teleinformatycznych jest związana ze sposobem ich wykorzystywania.

To co nazywamy systemem bezpieczeństwa, obejmuje elementy materialne tj. zabezpieczenia techniczne i fizyczne oraz przedsięwzięcia organizacyjne czy procedury, które stanowią jak najbardziej właściwe działania przyczyniające się do ulepszania różnego rodzaju zabezpieczeń i urządzeń wspomagających.

Systemy bezpieczeństwa cechują się dużą różnorodnością, dlatego opracowany dla danej instytucji musi on dokładnie odzwierciedlać realia jej funkcjonowania i eksploatowanych w niej systemów oraz otoczenia.

Omawiany system bezpieczeństwa instytucji został opracowany przy następujących założeniach:

1. System powinien być kompleksowy, to znaczy obejmować wszystkie poziomy modelu odniesienia.

2. Należy uwzględnić różnorodność charakteru procesów występujących w tej dziedzinie.

3. W maksymalnym stopniu należy zapewnić komputerowe wsparcie procesów zarządzania systemem bezpieczeństwa.

4. System bezpieczeństwa powinien mieć zdolność przystosowania się do zmian zachodzących w systemach teleinformatycznych i ich otoczeniu oraz do zmian w środowisku zagrożeń.

5. Należy zapewnić skalowalność i modularność, w tym możliwość wymiany modułów reprezentujących procesy.

6. Należy zapewnić zgodność z normami międzynarodowymi dotyczącymi bezpieczeństwa teleinformatycznego.

# Rozdział 2. Fazy realizacji i ogólny schemat funkcjonowania systemu bezpieczeństwa instytucji

Wyróżniamy trzy fazy realizacji systemu bezpieczeństwa instytucji:

* Projekt i planowanie – od określenia potrzeb po selekcje 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.

Ogólny schemat zarządzania bezpieczeństwem na podstawie polityki na wszystkich poziomach modelu, z szczególnym uwzględnieniem poziomu II, gdyż na nim koncentruje się zarządzanie bezpieczeństwem teleinformatycznym.



Rys. 1. Schemat zarządzania bezpieczeństwem teleinformatycznym

Źródło: [Białas 2006, s.187]

W rzeczywistości zależność między procesami jest bardziej skomplikowana, gdyż system bezpieczeństwa instytucji musi podlegać nieustannym korektom, adaptacjom i doskonaleniom.

Rysunek 1 przedstawia proces budowy systemu bezpieczeństwa, umownie w trzech fazach:

Faza I:

1. Opracowanie polityki i bezpieczeństwa instytucji.

2. Wybór strategii zarządzania ryzykiem.

3. Określenie wymagań dotyczących zabezpieczeń na podstawie potrzeb instytucji (misji), wielkość oszacowanego ryzyka i wymagań otoczenia prawnego.

4. Dobór zabezpieczeń.

5. Akceptacja zredukowanego ryzyka.

6. Opracowanie polityki bezpieczeństwa poszczególnych systemów oraz ich planów zabezpieczeń.

Faza II:

7. Wdrożenie planów zabezpieczeń i sprawdzenie skuteczności zabezpieczeń.

Faza III:

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

Opracowanie te sprzyja właściwej gospodarce zasobami i spójności koncepcji bezpieczeństwa wdrażania w bardzo zróżnicowanych środowiskach systemów teleinformatycznych. Ważnym jest, że wszelkie działania dla bezpieczeństwa powinny wynikać z potrzeb biznesowych instytucji i powinny obejmować tylko takie, które są dla niej konieczne i wystarczające. W rezultacie oznacza to osiągnięcie właściwego poziomu bezpieczeństwa bez nadmiernych nakładów.

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

Otoczenie prawne to ogół przepisów prawnych, statutowych, regulacji kontraktowych, które instytucje, jej partnerzy handlowi, kontrahenci i usługodawcy muszą spełnić. [Białas 2006, s.189]

Prawo nakazuje ochronę danych osobowych, informacji niejawnych, finansowych, dotyczących zdrowia i wielu innych rodzajów informacji, zwanych tajemnicami prawnie chronionymi.

Szczegółową identyfikacje otoczenia prawnego jest wygodnie prowadzić na drugim poziomie modelu. Wówczas wszelkie tajemnice prawnie chronione, jako informacje wrażliwe, są identyfikowane jako usługi krytycznie realizowane przez systemy, których to usług najczęściej dotyka problem zgodności prawnej.

Dobór wymagań dla instytucji może odbywać się na podstawie wzorcowych list wymagań. Przykładem takiej listy może być lista zawarta w dokumentach PN-ISO/IEC 17799 i PN-I-07799-2. Z dokumentów tych należy wybrać podzbiór wymagań najbardziej odpowiadających dla danej instytucji. Z list tych można również opracować listy audytowe do późniejszej kontroli tychże wymagać. Celem tych działań jest zredukowanie do akceptowalnego poziomu.

# Rozdział 3. Zapis sformalizowany modelu trójpoziomowego

W toku dość zawiłego procesu, trójpoziomowy model odniesienia jest wypełniony szczegółowymi treściami.

Przebieg transformacji modelu, można wyrazić następująco:

1. Na podstawie zadań statutowych (procesów biznesowych) realizowanych przez instytucję są identyfikowane trójki <BO,BS,BP>.

2. Dla każdej trójki przedstawia się DD, czyli stopień zaangażowania środków teleinformatycznych teleinformatycznych w realizację celu biznesowego i towarzyszące temu ryzyko- wyznacza się w ten sposób BL=<BO,BS,BP,DD>.

3. Zaangażowanie środków teleinformatycznych rodzi określone potrzeby dotyczące bezpieczeństwa, które można wyrazić, formułując cele bezpieczeństwa instytucji SO, z których wynikają strategie SS i polityki SP, co pozwala zdefiniować bezpieczeństwo w instytucji jako: BLS=<SO,SS,SP>.

4. Strategie SS, ale w kontekście SO i SP, są przekładane na cele bezpieczeństwa CITO, dla których należy wskazać strategie realizacji CITS z uwzględnieniem otoczenia prawnego LE i wyników przeprowadzonej analizy ryzyka RA, a także wypracować politykę CITP, to znaczy w pełni zdefiniować poziom II: CITSL=<CITO,CITS,CITP>.

5. W instytucjach mających oddziały różniące się pod względem celów CITO należy podzielić je na grupy DITO, wyróżniające specyficzne potrzeby oddziałów.

6. Na podstawie strategii CITS, ale w kontekście odpowiadającym im celów CITO i polityki CITP, są formułowane cele bezpieczeństwa poszczególnych systemów ITSO, które należy przełożyć na strategie ITSS oraz politykę dla każdego systemu ITSP, to znaczy w pełni zdefiniować poziom III: ITSSL=<ITSO, ITSS, ITSP>.



Rys. 2. Ogólny schemat transformacji modelu trójpoziomowego

Źródło: [Białas 2006, s. 192]

Przyjęto następujące skróty:

* BL (*Business Level*) – zadania statutowe instytucji, gdzie BL jest określony za pomocą czwórki pojęć: BL=<BO,BS,BP,DD>

- BO (*Business Objectives*) – cele działania

- BS (*Business Strategies*) – strategie osiągnięcia celów działania

- BP (*Business Policy*) – polityka działania instytucji

- DD (*Dependency Degree*) – umowny stopień zaangażowania środków teleinformatycznych w realizacje danego celu działania instytucji

* BLS ( *Business Level Security*) – bezpieczeństwo funkcjonowania instytucji, gdzie BLS jest określony za pomocą trójki pojęć: BLS=<SO,SS,SP>

- 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, gdzie CITSL jest określony za pomocą trójki pojęć: CITSL=<CITO,CITS,CITP>

- 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 teleinformatycznego instytucji

* DITSL (*Department IT Security Level*) – bezpieczeństwo ogółu systemów teleinformatycznych działających w oddziale instytucji, gdzie DITSL jest określony za pomocą trójki pojęć: DITSL=<DITO, DITS, DITP>

- 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 bezpieczeństwa teleinformatycznego oddziału instytucji

* ITSSL (IT System Security Level) – bezpieczeństwo konkretnego systemu teleinformatycznego działającego w instytucji lub jej oddziale, gdzie ITSSL jest określony za pomocą trójki pojęć: ITSSL=<ITSO,ITSS,ITSP>

- 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

* LE (Legal Environment) – otoczenie prawne

# Rozdział 4. Zapis sformalizowany procesów związanych z utrzymaniem bezpieczeństwa

Aby dopełnić system bezpieczeństwa, brakuje jeszcze jednego elementu, czyli „skoordynowanych przedsięwzięć”, którym jest zbiór procesów zarządzania przetwarzających te dane. Kierując się zasadami „co” i „dlaczego” dokonuję się rozpadu składników na podprocesy. Podejmowane są określone, zróżnicowane działania w postaci zbioru zawartego wewnątrz procesu. Założono, że źródłami zdarzeń wyzwalających procesy mogą być:

* Zdarzenia zachodzące w systemach i ich otoczeniu
* Zdarzenia wywołane w celu synchronizacji procesów przez inne procesy

Czasy działań, zawarte w planach lub harmonogramach, wynikające z postanowień polityki bezpieczeństwa – pełnią rolę czasowych wyzwalaczy procesów i będą oznaczane słowem „*Trigger*”.



Rys.3. Zbiór procesów zarządzania bezpieczeństwem teleinformatycznym

Źródło: [Białas 2006, s.195]

Na rysunku 3. podany jest wykaz podstawowych procesów systemu bezpieczeństwa instytucji, odpowiedzialnych za osiągnięcie i utrzymanie właściwego dla niej poziomu bezpieczeństwa .

Umownie wyodrębniono trzy grupy procesów:

1. Procesy zarządzania ryzykiem – ukierunkowane na dobór właściwych zabezpieczeń
2. Procesy wdrożeniowe – ukierunkowane na ich implementację
3. Procesy powdrożeniowe – głównym zadaniem jest utrzymanie stanu bezpieczeństwa i reagowanie na zmiany w systemach i ich otoczeniu

Przyjęto następujący zbiór tych współbieżnych procesów wraz z oznaczeniami:

* Zarządzanie zmianami – wykrywanie i wstępna ocena wpływu wszelkich zmian zachodzących w systemach teleinformatycznych na aktualny stan bezpieczeństwa. Kolejno znaczące zmiany są przekazywane do procesu monitorowania, gdzie są poddawane szczegółowej analizie, a zmiany o mniejszej skali są analizowane na bieżąco.

**ChngManagProc**

**-** ChngScheduleTrigger – zdarzenia wyzwalające, wynikające z planu zmian.

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

**SecMonitoringProc**

- SignificantSysChngDetected – wykryto poważne zmiany w systemie i lub ich otoczeniu, które należy przeanalizować.

- MonitoringScheduleTrigger – zdarzenia wyzwalające, wynikające z planu monitorowania.

* Kontrola zgodności – sprawdzanie czy nadal są spełnione wymagania, określone w polityce i planach zabezpieczeń.

**CompCheckProc**

- ChceckCompliane – 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.

**IncidHandProc**

- IASTrigger – zdarzenia wyzwalające, wynikające ze schematu analizy incydentów – reakcja.

* Analiza ryzyka – wymuszona uwarunkowaniami opisanymi w polityce bezpieczeństwa.

**RiskAssessProc**

- PossibleRiskChng – zdarzenia wymuszające analizę ryzyka po znaczących zmianach w systemach.

- RiskScheduleTrigger – zdarzenie wymuszające analizę ryzyka zgodnie z polityką bezpieczeństwa.

* Wybór zabezpieczeń – mających obniżyć wykryte zbyt wysokie ryzyko.

**SafegSelectProc**

- ReduceRisk – zdarzena wymuszające konieczność obniżenia ryzyka przez modyfikacje.

* Akceptacja ryzyka – akceptacja bieżącego ryzyka przez kierownictwo.

**RiskAcceptProc**

- AcceptRisk – zdarzenia wymuszające ocenę bieżącego ryzyka, jego akceptację bądź wskazanie potrzeby dalszej redukcji.

* Aktualizacja dokumentacji - wprowadzenie zatwierdzonych zmian do dokumentacji systemu bezpieczeństwa.

**SecSysDocUpdProc**

- DoUpdate – zdarzenia wymuszające aktualizację dokumentacji systemu bezpieczeństwa.

* Wdrożenie zabezpieczeń – wdrożenie nowego zabezpieczenia i sprawdzenie jego skuteczności.

**ImplementProc**

- DoImplement – zdarzenia wymuszające wdrożenie dobranych zabezpieczeń.

* Aprobata – dopuszczenie systemów do eksploatacji po modyfikacji systemu zabezpieczeń.

**ApprovalProc**

- DoApprove – zdarzenia wymuszające proces aprobaty.

* Uświadomienie – permanentne działania, utrzymujące właściwy stan świadomości bezpieczeństwa wśród personelu.

**AwareProc**

- AwarnScheduleTrigger – zdarzenia wyzwalające, wynikające z programu działań uświadamiających.

* Szkolenie i warsztaty według programu wypracowanego w instytucji.

**TrainProc**

- TrainScheduleTrigger – zdarzenia wyzwalające, wynikające z programu szkoleń.

Podstawowym procesem, odpowiedzialnym w cyklu życia za ciągłe przystosowanie się systemu bezpieczeństwa do zmian zachodzących w systemach teleinformatycznych i ich otoczeniu jest SecMainProc. Monitorowanie zmian pełni szczególną rolę, iż wykrywa, selekcjonuje i pobudza odpowiednie ścieżki, w zależności od głębokości zmian i ich potencjalnego wpływu na bezpieczeństwo. Na każdą zmianę musi nastąpić reakcja, czasem jest to prosta analiza wpływu zmiany konfiguracji, czasem pełna analiza ryzyka.

# Zakończenie

Metodyka budowy systemu bezpieczeństwa, wyróżnia fazy jego cyklu, w której stosowane metody to zstępujące z pętlami korygującymi sprzężenia zwrotne. Struktury informacji opisujące system oraz zbiory składających się nań procesów to kluczowe elementy budowy i eksploatacji systemu bezpieczeństwa instytucji. Jego budowę powinno rozpocząć się od analizy potrzeb biznesowych instytucji, bo to właśnie one w maksymalnym stopniu odzwierciedlają system bezpieczeństwa. Najkorzystniej wyrazić potrzeby jest poprzez formułowanie coraz bardziej szczegółowym celów, strategii i zasad polityki, a wszystko to zgodnie z modelem odniesienia.

# Spis literatury

Białas M., 2006, *Bezpieczeństwo informacji i usług w nowoczesnej instytucji i firmie*, Wydawnictwo WNT, Warszawa.

Polska Norma PN-ISO/IEC 17799:2007, *Technika informatyczna. Praktyczne zasady zarządzania bezpieczeństwem informacji,* Polski komitet Normalizacyjny, Warszawa.

Ustawa z dnia 22.01.1999r. O ochronie informacji niejawnych, Dz.U. nr 11 z późniejszymi zmianami.

# Spis rysunków i schematów

Rys. 1. Schemat zarządzania bezpieczeństwem teleinformatycznym 6

Rys. 2. Ogólny schemat transformacji modelu trójpoziomowego 10

Rys.3. Zbiór procesów zarządzania bezpieczeństwem teleinformatycznym 12