**Paulina Ćmiel**

**Bezpieczeństwo w instytucji**

**Uniwersytet Zielonogórski**

**Wydział Ekonomii i Zarządzania**

Zielona Góra 2020

**Spis treści**

[Wstęp 3](#_Toc35358840)

[1. Architektura systemu bezpieczeństwa instytucji 3](#_Toc35358841)

[2. Analiza procesów biznesowych ze względu na stopień zaangażowania systemów teleinformatycznych w ich realizację 4](#_Toc35358842)

[3. Ogólne potrzeby bezpieczeństwa systemów teleinformatycznych instytucji 6](#_Toc35358843)

[3.1 Podstawowe wymagania bezpieczeństwa teleinformatycznego 7](#_Toc35358844)

[4. Formułowanie dokumentu polityki bezpieczeństwa instytucji 9](#_Toc35358845)

[4.1 Dokument polityki bezpieczeństwa informacji 10](#_Toc35358846)

[5. Zarządzanie bezpieczeństwem na poziomie instytucji 12](#_Toc35358847)

[Bibliografia 13](#_Toc35358848)

# Wstęp

Podejmowane na tym etapie przedsięwzięcia dotyczą funkcji instytucji- jej zadań statutowych, biznesowych – często określanych mianem misji instytucji. W tym miejscu powinna rozpocząć się budowa systemu bezpieczeństwa informacji i usług dla nowoczesnej instytucji.

Bezpieczeństwo w instytucji – podstawowe przedsięwzięcia.

1. Podjęcie przez rząd inicjatywy budowy systemu bezpieczeństwa instytucji i zadeklarowanie nadzoru oraz wsparcia dla całości przedsięwzięcia.
2. Powołanie zespołu specjalistów, który będzie przekształcany ewolucyjnie w docelowe struktury zarządzania bezpieczeństwem informacji i usług; można założyć, że na początek w skład tego zespołu wejdą: członek zarządu, konsultant z zewnątrz, kierownik, działu informatyki i powoływany (najczęściej dopiero teraz) inspektor bezpieczeństwa.
3. Przeprowadzenie analizy zapotrzebowania instytucji na bezpieczeństwo i wyrażenie tego w postaci celów, strategii i polityki bezpieczeństwa instytucji.

# Architektura systemu bezpieczeństwa instytucji

Załóżmy, że zarząd instytucji podjął już inicjatywę budowy systemu bezpieczeństwa instytucji i powołał stosowny zespół do realizacji tego przedsięwzięcia. Aby postępowanie przy budowie pierwszego poziomu bezpieczeństwa było prawidłowe w instytucji powinien zobowiązywać dany schemat procesu transformacji. Proces ten zawiera w sobie takie elementy jak: identyfikacja, analiza, w tym analiza dla procesów biznesowych, synteza sformułowań, porządkowań, porządkowanie czy kompozycja i dekompozycja. W dużej mierze ma on charakter heurystyczny czyli, ma za zadanie znajdowanie rozwiązań, dla której nie ma gwarancji znalezienia rozwiązania optymalnego, a często nawet prawidłowego, aczkolwiek jest dość uporządkowany.

# Analiza procesów biznesowych ze względu na stopień zaangażowania systemów teleinformatycznych w ich realizację

Do zwięzłego przedstawienia misji instytucji, jej celów biznesowych i stopnia zaangażowania środków teleinformatycznych w ich realizację, może być pomocny szablon BL\_tpl, pokazany w tab. 2.1. Celem tych działań jest zebranie podstawowych informacji od zarządu instytucji, które po przeanalizowaniu będą pełnić rolę ogólnych wytycznych do dalszych etapów bodowy systemu bezpieczeństwa.

Tabela 2.1 Szablon BL\_tpl – zadania statutowe instytucji i stopień zaangażowania środków teleinformatycznych w ich realizację

|  |  |  |  |
| --- | --- | --- | --- |
| BOCele działania | BSStrategie działania | BPPolityka działania | DDStopień zaangażowania środków teleinformatycznych |
| BO(i) | BS(i,j) | BP(i,j,k) | DD(i,j,l) |
|  |  |  | Według szablonu DD\_tpl |
|  |  |  |  |
|  |  |  |  |

Źródło: [Białas 2017, s.201]

Korzystając z szablonu, w jego lewej kolumnie należy wymienić podstawowe zadania statutowe instytucji BO(i) – zwykle jest ich kilka, na przykład „osiągnięcie założonego przychodu z działalności gospodarczej”, „zarządzanie organem administracji w zakresie …” , „świadczenie usług medycznych dla … na podstawie …” i tym podobne.

Dla każdego celu BO(i) należy wskazać strategie BS(i,j), czyli odpowiedzieć na pytanie, za pomocą jakich działań dany cel ma być osiągnięty. Dla danego celu może występować po kilka strategii stanowiących pewien podzbiór wszystkich możliwych strategii. Strategie są realizowane przez szczegółowe formy polityki BP(i,j,k), które w instytucjach zwykle już egzystują. Można by wspomnieć o formach polityki, a czasem już planach: finansowym, prac badawczo – rozwojowych, wdrożenia określonej technologii, marketingowym, sprzedaży na dany rok, itp. Należy je tylko wskazać, by móc potem wykorzystań jego źródło szczegółowych informacji w wypadku konieczności rozstrzygania bądź interpretowania problemów na styku misja – bezpieczeństwo. W dalszych rozważaniach formy tej polityki będą stanowić tło biznesowe dla bezpieczeństwa informacji i usług.

Należy jeszcze wspomnieć, że dla danej pary <cel, strategia> może występować kilka wspomnianych wcześniej form polityki.

Przykład 1

Prosty wypadek przełożenia celów biznesowych na strategie, a te na politykę – firma produkcyjna

Cel: BO(1) =osiągnięcie założonego przychodu

Strategie: BS(1,1) = przez wyprodukowanie określonej ilości towarów BS(1,2) = przez dystrybucję określonej ilości towarów

Polityka: BP(1,1,1) = plan badawczo-rozwojowy dotyczący wyboru BP(1,1,2) = plany wdrożenia technologii nowego wyboru BP(1,1,3) = plany produkcji wyboru BP(1,1,4) = plany finansowe firmy BP(1,2,1) = plany promocji nowego wyboru BP(1,2,2) = roczny plan marketingu i sprzedaży

Funkcjonowanie instytucji można wyrazić za pomocą zbioru pewnych elementarnych funkcji składających się na tak zwaną jej misję lub też zadania statutowe, które dla instytucji komercyjnych zwykło się określać mianem zadań biznesowych. W przyjętym modelu każdej takiej funkcji odpowiada strategia BS, ale rozpatrywana w kontekście BO i BP, czyli można przyjąć, że funkcji odpowiada trójka: <BO, BS, BP>.

Cały obszar funkcjonowania instytucji został zdekomponowany na pewne moduły realizujące poszczególne funkcje instytucji (zadania biznesowe).

Należy scharakteryzować również stopień zaangażowania środków teleinformatycznych w realizację każdej z tych funkcji związane z tym ryzyko dla instytucji, czyli DD (i,j,l). Można to wyrazić na dwa sposoby:

* W zdefiniowanej dla instytucji skali umownej z uzasadnieniem słownym, na przykład od 0 do 9 (ilościowo) albo maksymalny – wysoki – umiarkowany – niski (jakościowo).
* W formie opisowej.

# Ogólne potrzeby bezpieczeństwa systemów teleinformatycznych instytucji

Nowoczesne technologie teleinformatyczne zaangażowane w realizację procesów biznesowych rodzą określone zapotrzebowanie na bezpieczeństwo teleinformatyczne w instytucji, dlatego w następnym etapie należy je zidentyfikować. Pomocnym do tego będzie szablon BLS\_tpl.

Tabela 3.1 Szablon BLS\_tpl – cele, strategie i polityka bezpieczeństwa instytucji

|  |  |  |
| --- | --- | --- |
| SOCele bezpieczeństwa instytucji | SSStrategie bezpieczeństwa instytucji „przez” | SPPolityka bezpieczeństwa instytucji (zasady) |
| SO(i) | SS(i,j) | SP(i,j) |
|  |  |  |
|  |  |  |
|  |  |  |

Źródło: [Białas 2017, s. 211]

Ocena wymagań w tym zakresie jest bardzo pomocna przy formułowaniu celów SO i strategii SS. W dużej mierze zależy ona od doświadczenia specjalistów oraz zgłębienia przez nich istoty procesów biznesowych instytucji i towarzyszącego im ryzyka.

Formułowanie celów – wskazówki.

Ogólna zasadą jest takie formułowanie celów bezpieczeństwa instytucji SO, alby przeciwstawiały się one bezpośrednio (cele sporadyczne) lub pośrednio (cele ogólne) czynnikom ryzyka dla procesów biznesowych (DD), dotyczących zasobów chronionych na poziomie pierwszym modelu odniesienia, to jest: ciągłość funkcjonowania, działania zgodnego z prawem, ochrony wizerunku i reputacji.

Powstaje problem do rozstrzygnięcia, czym jeszcze należy kierować się, formułując cele bezpieczeństwa? Spośród wielu czynników, warto wymienić:

* Znaczenie poszczególnych celów biznesowych.
* Stopień zaangażowania środków teleinformatycznych w ich realizację.
* Ryzyko według oceny zarządu.
* Różnorodność zadań realizowanych w instytucji.
* Możliwość wyizolowania poszczególnych zadań statutowych albo ich łączenia ze względu na podobieństwo.
* Zróżnicowania działów instytucji pod względem stosowania teleinformatyki.

Z rozważań praktycznych wynika, że dobrze jest wyróżnić:

* Cele związane z ogólnymi aspektami bezpieczeństwa, służące tak zwanemu bezpieczeństwu wewnętrznemu systemów.
* Cele specyficzne, związane z najbardziej żywotnymi zadaniami dla instytucji, a przy tym silnie zinformatyzowanymi, które wyrażają jej szczególne zapotrzebowanie na bezpieczeństwo.

Zbiór celów powinien obejmować te, które można uznać za:

* Konieczne, aby przeciwstawić się wszystkim czynnikom ryzyka dla procesów biznesowych i pozbyć się luk w systemie bezpieczeństwa zbudowanym na ich podstawie;
* Wystarczające, aby uniknąć celów nadmiarowych, co w efekcie podwyższyłoby nakłady na zabezpieczenia i koszty na ich utrzymanie.

Każda pomyłka na tym etapie oznacza lukę w bezpieczeństwie, albo zbędne nakłady. Można tu popełnić grube błędy, dlatego należy uzasadnić, że zbiór celów jest konieczny i wystarczający dla potrzeb instytucji.

## 3.1 Podstawowe wymagania bezpieczeństwa teleinformatycznego

§ 5. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w systemie teleinformatycznym zapewnia się przez wdrożenie spójnego zbioru zabezpieczeń w celu zapewnienia poufności, integralności i dostępności tych informacji.

2. Cel, o którym mowa w ust. 1, osiąga się przez:

1. objęcie systemu teleinformatycznego procesem zarządzania ryzykiem dla bezpieczeństwa informacji niejawnych przetwarzanych w  systemie teleinformatycznym, zwanego dalej „zarządzaniem ryzykiem w systemie teleinformatycznym”;
2. ograniczenie zaufania, polegające na traktowaniu innych systemów teleinformatycznych jako potencjalnych źródeł zagrożeń oraz wdrożeniu w systemie teleinformatycznym zabezpieczeń kontrolujących wymianę informacji z tymi systemami teleinformatycznymi;
3. wprowadzenie wielopoziomowej ochrony systemu teleinformatycznego, polegającej na stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu teleinformatycznego, w  celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia skutkuje naruszeniem celu, o którym mowa w ust. 1;
4. wykonywanie okresowych testów bezpieczeństwa;
5. ograniczanie uprawnień, polegające na nadawaniu użytkownikom systemu teleinformatycznego wyłącznie uprawnień niezbędnych do wykonywania pracy;
6. minimalizację funkcjonalności, polegającą na instalowaniu, uaktywnianiu i  wykorzystywaniu w  systemie teleinformatycznym wyłącznie funkcji, protokołów komunikacyjnych i usług niezbędnych do prawidłowej realizacji zadań, do których system teleinformatyczny został przeznaczony.

§ 18. 1. Bezpieczeństwo informacji niejawnych przetwarzanych w  systemie teleinformatycznym uwzględnia się w całym cyklu funkcjonowania systemu teleinformatycznego, składającym się z etapów:

1. planowania;
2. projektowania;
3. wdrażania;
4. eksploatacji;
5. wycofywania.

2. Na etapie planowania ustala się potrzeby w zakresie przetwarzania informacji niejawnych w systemie teleinformatycznym, w szczególności określa się:

1. przeznaczenie systemu teleinformatycznego;
2. maksymalną klauzulę tajności informacji niejawnych, które będą przetwarzane w systemie teleinformatycznym;
3. tryb bezpieczeństwa pracy systemu teleinformatycznego;
4. szacunkową liczbę użytkowników;
5. planowaną lokalizację.

3. Na etapie projektowania:

1. przeprowadza się wstępne szacowanie ryzyka dla bezpieczeństwa informacji niejawnych w celu określenia wymagań dla zabezpieczeń;
2. dokonuje się wyboru zabezpieczeń dla systemu teleinformatycznego w oparciu o wyniki wstępnego szacowania ryzyka dla bezpieczeństwa informacji niejawnych;
3. uzgadnia się z podmiotem akredytującym plan akredytacji obejmujący zakres i harmonogram przedsięwzięć wymaganych do uzyskania akredytacji bezpieczeństwa teleinformatycznego;
4. uzgadnia się z podmiotem zaopatrującym w klucze kryptograficzne rodzaj oraz ilość niezbędnych urządzeń lub narzędzi kryptograficznych, a także sposób ich wykorzystania;
5. opracowuje się dokument szczególnych wymagań bezpieczeństwa.

# Formułowanie dokumentu polityki bezpieczeństwa instytucji

Ogólną strukturę i zawartość dokumentu zaproponowano w postaci szablonu SP\_tpl, przedstawiono w tabeli 4.1. Szablon przedstawia nazwy poszczególnych rozdziałów (założono, że będzie ich 10) wraz z komentarzem, co w nich powinno się znaleźć.

Przyjęta budowa szablonu będzie spójna z szablonami polityki niższych poziomów, które zostaną przedstawione dalej, przy czym treść rozdziałów będzie w nich podobna, ale uwzględniająca coraz więcej szczegółów.

Tabela 4.1 Szablon SP\_tpl – dokument polityki bezpieczeństwa instytucji (poziomu I)

|  |  |
| --- | --- |
| Nr rozdz. | Polityka bezpieczeństwa instytucji - zawartość dokumentu  |
| 1 | **Deklaracja zarządu instytucji o ustanowieniu**W deklaracji zarządu o ustanowieniu niniejszej polityki powinny się znaleźć takie elementy jak:* Wnioski z przeglądu celów i strategii związanych z realizacją zadań statutowych przy wykorzystaniu środków teleinformatycznych..
* Wnioski przedstawiające w zwięzłej formie świadomość zarządu o znaczeniu bezpieczeństwa teleinformatyki instytucji.
* Ustanowienie polityki wyrażenie gotowości do wsparcia organizacyjnego i finansowego przedsięwzięcia.
* Powołanie trzonu zespołu odpowiedzialnego za budowę i utrzymanie systemu bezpieczeństwa.
 |
| 2 | **Cel opracowania i zawartość dokumentu**Celem powstania tego typu dokumentu jest zainicjowanie przedsięwzięcia budowy systemu bezpieczeństwa w instytucji i wytyczanie dla niej ogólnych i wymagań w tym zakresie. |
| 3 | **Postawy normatywne i terminologia**Należy wymienić tylko podstawowe standardy i zalecenia, na podstawie których będzie budowany system bezpieczeństwa instytucji. |
| 4 | **Podstawy prawne**Należy zwrócić uwagę, że dokumenty polityki bezpieczeństwa muszą być zgodne z obowiązującym prawem.  |
| 5 | **Zakres oddziaływania** Należy przedstawić obszary funkcjonowania instytucji, najczęściej jest to całość aktywów, które mają podlegać polityce, w kontekście struktury organizacyjnej, personelu, kooperantów, partnerów i zleceniobiorców. |
| 6 | **Bezpieczeństwo w instytucji**Jest to główny rozdział dokumentu polityki, który wyraża potrzeby instytucji dotyczące bezpieczeństwa informacji i usług, a jak wiadomo, można wyrazić je poprzez cele i strategie, wykorzystując szablon BLS\_tpl. |
| 7 | **Role i odpowiedzialność**Zarząd powinien powołać (albo zreorganizować) strukturę organizacyjną, która:* Będzie stanowiła trzon struktury docelowej;
* Realizuje zasadę rozdziału pionu eksploatacji od pionu bezpieczeństwa;
* Ułatwia zarządowi zaangażowanie się i sprawowanie nadzoru nad budowę systemu bezpieczeństwa;
* Zapewnia dostęp do wiedzy eksperckiej;
* Będzie zdolna do rozwinięcia i uszczegółowienia poziomu I do poziomu II i III architektury bezpieczeństwa.
 |

|  |  |
| --- | --- |
| 8 | **Rozpowszechnianie i zarządzanie dokumentem polityki**1. Zasady rozpowszechniania

Ze względu na to, że dokument polityki poziomu I ma duże znaczenie propagandowe, kształtujące pozytywny wizerunek instytucji w jej środowisku i przy tym zawiera tylko bardzo szczególne informacje dotyczące bezpieczeństwa, należy go możliwie szybko rozpowszechnić.1. Zasady zarządzania (przeglądy, aktualizacja)
 |
| 9 | **Załączniki**Ze względu na konieczność zachowania zwięzłości dokumentu, wszelkie uregulowania szczegółowe, na przykład akty powołania na stanowiska, wykazy przepisów prawa, norm, terminologia powinny być umieszczane w załączniku. |
| 10 | **Odwołanie do polityki bezpieczeństwa systemów teleinformatycznych instytucji**W tym miejscu powinno znaleźć się odwołanie do dokumentu polityki bezpieczeństwa teleinformatycznego instytucji (poziom II), który ma dopiero powstać jako wynik pracy powołanego zespołu. Nie jest to jakiś inny, dodatkowy dokument polityki, a tylko uszczegółowienie niniejszego dokumentu. |

Z doświadczeń wynika, że tego typu dokument może liczyć od kilku do kilkunastu stron wraz z załącznikami.

Należy pamiętać, że nie istnieją na rynku gotowe do zastosowania dokumenty polityki bezpieczeństwa, bowiem politykę wypracowuje się indywidualnie dla instytucji. Jednak w tym zakresie bardzo użyteczne mogą być różnego typu oferowane wzorce otwarte lub dokumenty ramowe. Pokazany szablon jest jednym z możliwych przykładów takiego wzorca.

## 4.1 Dokument polityki bezpieczeństwa informacji

Zabezpieczenie

Zaleca się, aby dokument polityki bezpieczeństwa informacji został zatwierdzony przez kierownictwo, opublikowany i podany do wiadomości wszystkim pracownikom i właściwym stronom zewnętrznym.

Wskazówki do wdrożenia

Zaleca się, aby w dokumencie polityki bezpieczeństwa informacji zawarto deklarację zaangażowania kierownictwa i określenie podejścia organizacji do zarządzania bezpieczeństwem informacji. Zaleca się, aby dokument polityki zawierał następujące stwierdzenia:

* 1. definicję bezpieczeństwa informacji, jego ogólne cele, zakres oraz znaczenie bezpieczeństwa, jako mechanizmu umożliwiającego współużytkowanie informacji;
	2. oświadczenie o intencjach kierownictwa, potwierdzające cele i zasady bezpieczeństwa informacji w odniesieniu do strategii i wymagań biznesowych;
	3. strukturę wyznaczania celów stosowania zabezpieczeń i zabezpieczeń, w tym strukturę szacowania i zarządzania ryzykiem;
	4. krótkie wyjaśnienie polityki bezpieczeństwa, zasad, norm i wymagań zgodności mających szczególne znaczenie dla organizacji, zawierające:

1) zgodność z prawem, regulacjami wewnętrznymi i wymaganiami wynikającymi z umów;

2) wymagania dotyczące kształcenia, szkoleń i uświadamiania w dziedzinie bezpieczeństwa;

3) zarządzanie ciągłością działania biznesowego;

4) konsekwencje naruszenia polityki bezpieczeństwa;

* 1. definicje ogólnych i szczególnych obowiązków w odniesieniu do zarządzania bezpieczeństwem informacji, w tym zgłaszania incydentów związanych z bezpieczeństwem informacji;
	2. odsyłacze do dokumentacji mogącej uzupełniać politykę, np. bardziej szczegółowych polityk bezpieczeństwa i procedur dotyczących poszczególnych systemów informatycznych lub zalecanych do przestrzegania przez użytkowników zasad bezpieczeństwa.

Zaleca się udostępnienie polityki bezpieczeństwa informacji użytkownikom w całej organizacji w formie właściwej, dostępnej i zrozumiałej dla czytelników, do których jest adresowana.

# Zarządzanie bezpieczeństwem na poziomie instytucji

Dokument polityki bezpieczeństwa na poziomie I, aczkolwiek niezwykle doniosły dla instytucji, gdyż wytycza kierunki zarządzania bezpieczeństwem informacji i usług, jest jednocześnie zbyt ogólny, by stanowić o szczegółach działań składających się na to zarządzanie. Tego typu działania muszą być podejmowane na poziomach niższych modelu odniesienia.

Czynności podejmowane na poziomie I są dość ogólne i dotyczą na przykład zmiany charakteru procesów biznesowych, otoczenia prawnego czy zmian organizacyjnych w instytucji. Wszystkie te zmiany mogą jednak wpływać na konieczność poważnej rewizji polityki bezpieczeństwa instytucji, która z kolei pociąga konieczność głębokich modyfikacji całego systemu bezpieczeństwa.

Zarządzanie bezpieczeństwem informacji wymaga, jako minimum, udziału wszystkich pracowników organizacji. Może także wymagać współpracy akcjonariuszy, dostawców, stron trzecich, klientów lub innych podmiotów zewnętrznych. Potrzebne może być także specjalistyczne, zewnętrzne doradztwo.

# Bibliografia

A. Białas, Bezpieczeństwo informacji i usług we współczesnej firmie lub instytucji, WNT, Warszawa 2017r.

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

Rozporządzenie Prezesa Rady Ministrów z dnia 20 lipca 2011 r. w sprawie podstawowych wymagań bezpieczeństwa teleinformatycznego.