

# Polityka bezpieczeństwa organizacji „na miarę”

Andrzej Adamczyk

*ITTI Sp. z o. o.*

*e-mail: andrzej.adamczyk@itti.com.pl*

Jakub Radziulis

*Uniwersytet im. Adama Mickiewicza w Poznaniu*

*e-mail: jradziulis@wp.pl*

Rafał Renk

*Uniwersytet im. Adama Mickiewicza w Poznaniu*

*e-mail: rrenk@wp.pl*

prof. Witold Hołubowicz

*Uniwersytet im. Adama Mickiewicza w Poznaniu*

*e-mail: holub@amu.edu.pl*

## **Abstrakt**

Polityka bezpieczeństwa jest zbiorem założeń konstytuującym wszelkie działania na rzecz bezpieczeństwa prowadzone w ramach organizacji. Zbiór ten powinien zostać rzetelnie spisany, zaakceptowany przez naczelne kierownictwo, a następnie skutecznie wdrożony w życie. Opracowanie „Polityki Bezpieczeństwa” tak, aby mogła być faktycznie wdrożona i realizowała cele strategiczne instytucji nie jest trywialne. W niniejszym artykule przedstawiono autorską metodykę – wypracowaną przez firmę ITTI w trakcie wielu projektów – służącą do tworzenia „Polityki Bezpieczeństwa” na miarę konkretnej organizacji.

Zgodnie z metodą, ostateczne sformułowanie zapisów „Polityki” jest zawsze poprzedzone skrupulatną analizą profilu instytucji, w której ma ona obowiązywać. O profilu decydują m.in. liczba pracowników, stopień komputeryzacji, współpraca z otoczeniem, rodzaje wykorzystywanych informacji i innych zasobów. Czynniki te mają wymierny wpływ na treść „Polityki Bezpieczeństwa”. Konstrukcja dokumentu obejmuje m.in.: definicję i strukturę przedmiotu ochrony oraz klasyfikację jego elementów wraz z przypisanym poziomem ich istotności, jak również podstawowe zasady ochrony wraz z ich streszczeniem.

Na zakończenie artykułu zostały omówione zalecenia odnośnie sposobu realizacji zadań związanych z opracowaniem „Polityki Bezpieczeństwa”, etapów pracy, metodyki pozyskiwania i przetwarzania informacji źródłowych.



## Filozofia i polityka

„Przede wszystkim silnie osadzić bezpieczeństwo w celach biznesowych” – Piotr Chodziecki

Bezpieczeństwo jest pewnego rodzaju idealnym stanem osoby, grupy osób lub organizacji. Ludzkość od swojego zarania dąży do osiągnięcia tego stanu. Stan bezpieczeństwa polega na zapewnieniu możliwości realizowania realnych i istotnych planów<sup>1</sup> aby osiągnąć zamierzone cele.

Cele te muszą być realne, bo ktoś kto stawia przed sobą nierealne cele będzie ustawicznie zaniepokojony tym, że nie uda mu się ich osiągnąć, co sprawi, że nie będzie się czuł bezpiecznie.

Podobnie niemożność zrealizowania małoistotnych celów nie jest w stanie wywołać w nas uczucia niebezpieczeństwa.

Zwykle podstawowymi środkami służącymi osiągnięciu celów życiowych każdego człowieka są: zachowanie życia, odpowiedniego zdrowia (fizycznego i psychicznego) oraz utrzymanie posiadania istotnych dla niego rzeczy. Nie muszą wyczerpywać one wszystkich zamierzeń jednostki bądź zbiorowości, lecz jeśli te warunki nie będą spełnione, wszystkie cele człowieka nie zostaną osiągnięte.

Podobnie jest z organizacjami. Organizacje to nic innego jak reprezentacje pewnych zbiorowości ludzkich. Posiadają cele, które odzwierciedlają cele osób powołujących je do istnienia, a w idealnym przypadku są zbieżne z celami całej zbiorowości. Podobnie jak człowiek, tak i organizacja dla osiągnięcia swoich celów musi istnieć i być w odpowiedniej kondycji oraz dysponować niezbędnymi zasobami. Innymi słowy musi być zapewniona celowość i ciągłość jej działania.

Oczywiście nie zawsze cele te muszą być znane *explicite*. Mogą one nie być wyartykułowane i istnieć jedynie w naszej podświadomości. Jeżeli tak jest nie możemy ich kontrolować i cieszyć się z ich zaspokajania. Dlatego organizacje starają się uświadomić sobie cele własnego istnienia i działania, a następnie spisać je, co jest również warunkiem uświadomienia wszystkich jednostek zbiorowości do czego zmierza cała organizacja, do której należą. Takim usystematyzowanym (najlepiej spisanim) zbiorem istotnych i realnych celów organizacji są tzw. cele biznesowe lub statutowe (dalej zwane celami biznesowymi). W zależności od charakteru działalności prowadzonej przez organizację mogą być one wyznaczone m.in. względami prawnymi, ekonomicznymi lub humanitarnymi.

Czym zatem jest tytułowa polityka bezpieczeństwa organizacji? Wokół tego terminu narosło wiele często sprzecznych ze sobą pojęć. W rozumieniu niektórych osób polityka bezpieczeństwa to cały system zarządzania bezpieczeństwem, a zatem zbiór planów, procedur, zasobów i działań zmierzających do podwyższenia i utrzymania poziomu bezpieczeństwa organizacji. Inna grupa osób pojmuje politykę bezpieczeństwa jako zbiór konkretnych zabezpieczeń i wzorów konfiguracji urządzeń sieci informatycznych. Polityka bezpieczeństwa w rozumieniu ITTI nie jest, ani pierwszym, ani drugim.

Otóż, polityka bezpieczeństwa organizacji zawsze jest pochodną celów biznesowych, co oznacza, że bez ich określenia, nie ma racji bytu. Politykę bezpieczeństwa tworzy się w celu ochrony głównych czynników sprzyjających osiągnięciu założonych celów biznesowych. De facto polityka to według słownika języka polskiego „przemysłany przez kogoś sposób postępowania mający doprowadzić do osiągnięcia zamierzonego celu; taktyka, strategia”. Posługując się skrótem myślowym można użyć pojęcia polityki bezpieczeństwa również w odniesieniu do dokumentu zawierającego założenia dotyczące wyżej wspomnianego sposobu postępowania. Politykę konstruuje się przez określenie przedmiotu ochrony oraz wytycznych sposobu jego zabezpieczenia.

---

<sup>1</sup> Plany te powinny być istotne i realne przynajmniej w trakcie ich tworzenia



Rys. 1. Poziom funkcjonowania „Polityki Bezpieczeństwa”

Nie ulega wątpliwości, że polityka, jako dokument, powinna stanowić opis kierunków działań na poziomie strategicznym koncentrując się na celach. Nie jest to zatem plan działania na poziomie operacyjnym określający konkretne procedury i instrukcje postępowania. „Polityka” ma być nadrzędna dla działań operacyjnych i jako taka wytyczać podstawowe założenia, które działania muszą spełnić. Dzięki temu polityka pozostaje aktualna wiele lat bez konieczności wprowadzania do niej zmian. Głównym bodźcem do modyfikacji polityki bezpieczeństwa jest zmiana samych celów biznesowych.

Cele biznesowe organizacja powinna określić sama dla siebie, gdyż stanowią one o tożsamości organizacji. Można by rzec, iż zmiana celów biznesowych zmienia jedną organizację w inną, która stawia przed sobą inne zadania. Dobrze jeśli cele biznesowe są opracowywane w ramach organizacji, której dotyczy. Często jednak bieżące priorytety bądź niska świadomość dotycząca zagadnień zarządzania bezpieczeństwem wymaga, aby tworzeniem tych najważniejszych dla bezpieczeństwa organizacji założeń zajął się profesjonalny i fachowy partner. ITTI zajmował się kilkakrotnie opracowywaniem polityk bezpieczeństwa dla organizacji i pomocą w ich wdrożeniu. Dzięki temu konsultanci ITTI posiadają wystarczającą wiedzę i doświadczenie by podjąć się realizacji tego rodzaju projektów. Do planowania działań w ramach takich projektów ITTI stosuje własną, autorską metodykę, której założeniem jest dostosowanie polityki do wielkości i charakteru działalności każdej organizacji. W kolejnych rozdziałach przedstawiono tę metodykę.

## Słownik pojęć

Poniżej przedstawiono słownik pojęć wykorzystany w ramach artykułu.

Tab. 1. Słownik pojęć

Pojęcie	Objaśnienie
audyt stanu bezpieczeństwa	Systematyczny, niezależny i udokumentowany proces uzyskiwania dowodów na brak stosowania określonych we wzorcu środków bezpieczeństwa oraz ich obiektywnej oceny w celu określenia poziomu bezpieczeństwa organizacji.
działanie operacyjne	Działanie podejmowane przez pracowników w celu realizacji celów biznesowych lub statutowych danej organizacji.

Pojęcie	Objaśnienie
cele biznesowe (statutowe)	Usystematyzowany (najlepiej spisany) zbiór istotnych i realnych celów do jakich dąży organizacja, wyrażonych na poziomie strategicznym.
częstość	Estymator prawdopodobieństwa w analizie ryzyka; miara występowania incydentu wyrażająca się liczbą incydentów w jednostce czasu (najczęściej w ciągu roku).
grupa incydentów	Zbiór incydentów charakteryzujących się podobnymi cechami.
incydent lub zdarzenie	Zdarzenie polegające na naruszeniu bezpieczeństwa organizacji i powodujące określone skutki w postaci: strat finansowych, utraconych korzyści oraz konsekwencji prawnych lub dyscyplinarnych.
obszar działań	Zbiór działań operacyjnych zmierzających do uzyskania określonego wyniku służącego celom biznesowym (statutowym).
organizacja	Grupa ludzi mająca wspólny cel, plan, program; instytucja np. społeczna, polityczna. (według słownika wyrazów obcych).
polityka bezpieczeństwa	<i>(sposób postępowania)</i> Przemysłany sposób postępowania mający zapobiec uniemożliwieniu osiągnięcia zamierzonych celów związanych z bezpieczeństwem. <i>(dokument – w treści artykułu pisany dla odróżnienia wielkimi literami i w cudzysłowie)</i> Dokument definiujący przedmiot ochrony wraz z określeniem istotności jego składników, służący ujednoczeniu i utrwaleniu kierunków i kryteriów oceny działań w zakresie zapewnienia bezpieczeństwa organizacji.
pracownik	Osoba, wobec której został nawiązany przez organizację stosunek pracy w rozumieniu ustawy z dnia 26 czerwca 1974 r. Kodeks pracy (Dz. U. 1974 Nr 24 poz. 141), zarówno na podstawie umowy o pracę, jak i na skutek powołania, wyboru, mianowania lub spółdzielczej umowy o pracę lub inna osoba biorąca udział w działalności organizacji na zasadach umowy zlecenia lub umowy o dzieło oraz stażysta lub osoba odbywająca przygotowanie zawodowe w organizacji.
ryzyko	Szansa zaistnienia zagrożenia (incydent) mającego negatywny wpływ na cele strategiczne organizacji; mierzone według prawdopodobnych skutków i częstości występowania.
skutek	Strata lub utracona korzyść związana z jednostkowym wystąpieniem incydentu .
zagrożenie	Potencjalna przyczyna wystąpienia niepożądanego incydentu.
zasób	Pracownicy organizacji (stanowiących podmiot działań), jak i infrastruktura (przedmioty działania), która jest im potrzebna do realizacji tych działań.

## Struktura „Polityki Bezpieczeństwa”

Przy tworzeniu „Polityki Bezpieczeństwa” w przeciwieństwie do np. analizy ryzyka, nie czyni się żadnych założeń wynikających z aktualnego stanu zabezpieczeń i stosowanych w organizacji środków bezpieczeństwa. Stan ten jest nieistotny, gdyż polityka to wytyczne, które mają charakter uniwersalny i obowiązują zawsze; niezależnie; czy są przestrzegane, czy też nie.

Dokument polityki bezpieczeństwa (pisany w dalszej części artykułu wielkimi literami i w cudzysłowie – „Polityka Bezpieczeństwa” – dla odróżnienia od polityki bezpieczeństwa jako sposobu postępowania) nie powinien być zbyt długi. W metodyce ITTI dokument taki ma zazwyczaj dwadzieścia kilka stron. Z założenia skierowany jest do wszystkich pracowników organizacji, a jego fragmenty mogą być zakomunikowane osobom i partnerom zewnętrznym, których postępowanie też może mieć wpływ na realizację polityki. Dlatego też powinien mieć zwięzłą i jasną formę, w przeciwnym razie maleje prawdopodobieństwo, że adresaci dokumentu zapoznają się w sposób wyczerpujący z jego treścią, nie mówiąc o jej zapamiętaniu i stosowaniu.

Ponadto, dokumentowi polityki bezpieczeństwa powinno towarzyszyć jednostronicowe streszczenie podstawowych zasad ochrony. Taka forma jest łatwiejsza do rozpowszechniania w formie plakatów-zawieszek ściennych, podobnie jak to często czyni się z polityką jakości.

Dokument powinien rozpoczynać się listem przewodnim skierowanym przez naczelne kierownictwo organizacji (zarząd, prezesa, dyrektora zarządzającego itp.). Taki list uwierzytelnia informacje zawarte w dokumencie co ma zasadnicze znaczenie dla zapewnienia odpowiedniego poziomu zaufania czytelników do treści „Polityki Bezpieczeństwa” w sensie rzetelności oraz nieuchronności. Następnie list przedstawia cel stworzenia „Polityki” i adresuje ją do konkretnych odbiorców. Ważnym elementem listu jest zaakcentowanie czynników motywujących członków organizacji do przestrzegania zapisów „Polityki”. Może być to zarówno motywacja pozytywna, jak i negatywna w zależności od skuteczności obu metod w kontekście kultury organizacji. W dalszej kolejności list ustanawia właściciela dokumentu, który będzie dbał o aktualizowanie i kontrolował modyfikowanie jego treści w ciągu całego cyklu życia.

Według metodyki ITTI dalsza część dokumentu polityki bezpieczeństwa zawiera:

- cel dokumentu (formalna wersja w odróżnieniu od części listu przewodniego),
- zakres stosowania,
- odpowiedzialność za przestrzeganie,
- zasady aktualizacji dokumentu,
- słownik użytych w dokumencie pojęć,
- cele biznesowe organizacji,
- definicję przedmiotu ochrony (wynikająca z celów biznesowych organizacji),
- podstawowe zasady postępowania (wytyczne i kierunki na poziomie strategicznym zmierzające do zapewnienia bezpieczeństwa organizacji).

„Polityka Bezpieczeństwa” może też zawierać (czasem jest to powtórzenie części listu przewodniego) konsekwencje grożące pracownikom w przypadku jej nieprzestrzegania oraz ewentualnie wskazania na inne dokumenty związane.

Pomijając rozdziały „Polityki” związane z metryką i zasadami utrzymania dokumentu, najważniejszymi merytorycznie elementami są: lista celów biznesowych, opis przedmiotu ochrony oraz podstawowe zasady postępowania. W poniższych podrozdziałach omówiono dwa ostatnie z nich stanowiące wartość dodaną „Polityki Bezpieczeństwa”, gdyż przed jej sformułowaniem informacje te najczęściej nie istnieją.

## **Przedmiot ochrony**

Tak jak to stwierdzono na wstępie niniejszego artykułu organizacja dla osiągnięcia swoich celów musi istnieć i być w odpowiedniej kondycji oraz dysponować niezbędnymi zasobami. Jeśli dwa pierwsze warunki nazwiemy elementami instytucjonalnymi i potraktujemy jako pewnego rodzaju zasób, sprowadzimy cały problem do zapewnienia bezpieczeństwa zbiorowi rodzajów

zasobów. Z doświadczenia wynika, iż wystarczy podzielić zasoby na następujące rodzaje, aby zapewnić odpowiedni poziom ogólności treści „Polityki Bezpieczeństwa”:

- pracownicy (P),
- elementy instytucjonalne (I),
- budynki i pomieszczenia (B),
- meble i wyposażenie (M),
- systemy IT i telekomunikacyjne (S),
- dokumenty papierowe i elektroniczne (D),
- środki finansowe (F),
- usługi świadczone przez podmioty zewnętrzne (U).

Na liście podano też jednoliterowe symbole, którymi posługuje się „Polityka Bezpieczeństwa” tworzona przez konsultantów ITTI.

Przedmiotem ochrony jest właściwy stan tych zasobów, polegający na zgodności ich faktycznych właściwości z właściwościami pożądanymi im przypisanymi. Przypisanie to zazwyczaj jest wynikiem uwzględnienia celów biznesowych organizacji. Zatem celem ochrony w zakresie działań na rzecz bezpieczeństwa organizacji, jest zachowanie wymienionej wcześniej zgodności. Przedmiot ochrony można określić według rodzajów zasobów oraz ich cech, którymi są:

- dostępność (w przypadku pracowników ich obecność),
- użyteczność (w przypadku pracowników ich zdolność do działania),
- oraz legalność (w przypadku pracowników legalność ich działania) zasobów.

Należy poczynić założenie, iż własności zasobów z punktu widzenia wymienionych cech są dwuwartościowe (np. zasób jest dostępny albo nie jest dostępny). Konkretna cecha danego rodzaju zasobów w Polityce nazywana jest elementem przedmiotu ochrony.

Poziom istotności zachowania pożądanego stanu zasobów, z punktu widzenia działalności organizacji (w kontekście ich rodzaju i cech) jest różnorodna. W Polityce zamieszczana jest tabela istotności określona na podstawie zebranych informacji na temat specyfiki działania konkretnej organizacji. W tym sensie jest to jeden z elementów decydujący o tym, że „Polityka” jest tworzona „na miarę” czyli jest dedykowana. Przykładowe poziomy istotności poszczególnych elementów przedmiotu ochrony zostały przedstawione w Tab. 2.

Tab. 2. Istotność przykładowych elementów przedmiotu ochrony

Istotność pożądanых cech zasobów	Pracownicy	Budynki i pomieszczenia	Systemy IT i telekom.	...
Dostępność (obecność pracowników)	<b>K</b>	***	<b>K</b>	...
Użyteczność (zdolność pracowników do działania)	<b>K</b>	**	***	...
Legalność stanu (legalność działania pracowników)	<b>K</b>	**	***	...

Legenda: K – konieczne; \*\*\* – bardzo istotne; \*\* – istotne; \* – przydatne

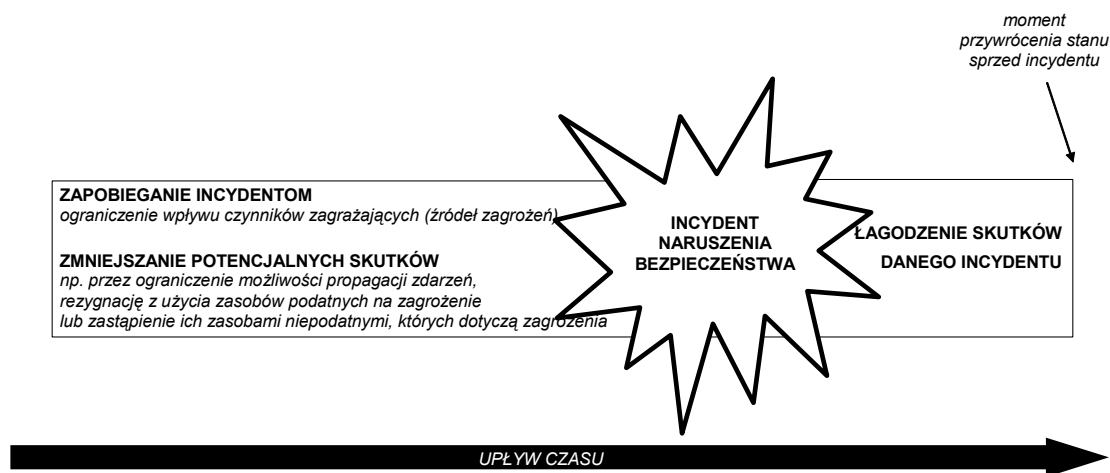
Powyższa tabela dekomponuje przedmiot ochrony w zbiór elementów, którymi następnie „Polityka” będzie zajmowała się odrębnie. Każdemu z elementów zostaną przypisane podstawowe zasady postępowania.

## Podstawowe zasady postępowania

W niniejszym rozdziale opisano podstawowe zasady postępowania w celu zapewnienia bezpieczeństwa. Podstawowe zasady postępowania stanowią wytyczne dla działań na rzecz bezpieczeństwa organizacji i realizują następujące zadania:

- zapobiegają incydom naruszenia bezpieczeństwa,
- zmniejszają potencjalne skutki danej grupy incydentów,
- łagodzą skutki konkretnych incydentów.

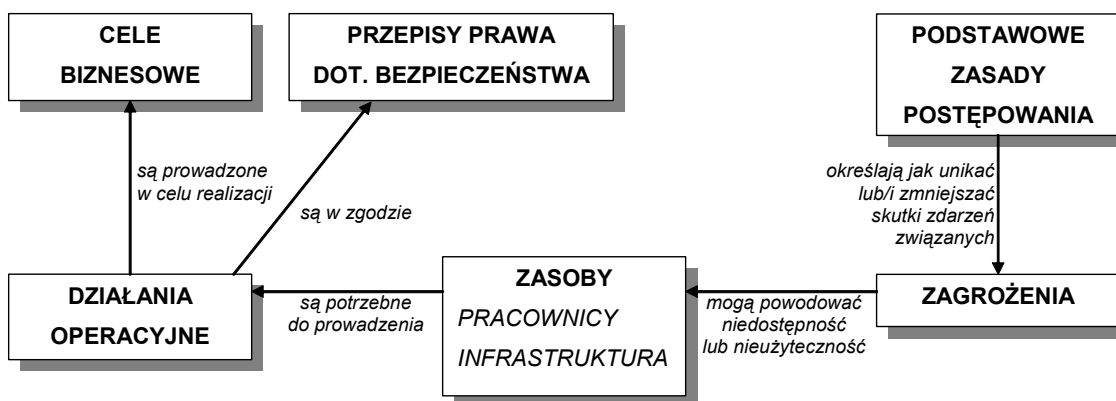
Działania na rzecz bezpieczeństwa powinny być prowadzone w kolejności przedstawionej w postaci schematu na Rys. 2.



Rys. 2. Rodzaje i kolejność działań na rzecz bezpieczeństwa

Wytyczne postaci podstawowych zasad postępowania są skierowane do pracowników firmy na wszystkich szczeblach, gdyż od ich postępowania zależy bezpieczeństwo organizacji. Mogą oni oczywiście wywierać wpływ na otoczenie polityczne, prawne oraz ekonomiczne organizacji dla osiągnięcia pewnych celów, jednak to też powinni robić uwzględniając podstawowe zasady postępowania zawarte w Polityce Bezpieczeństwa.

Aby zrozumieć związki zachodzące pomiędzy podstawowymi zasadami ochrony a pozostałymi pojęciami można posłużyć się schematem z Rys. 3.

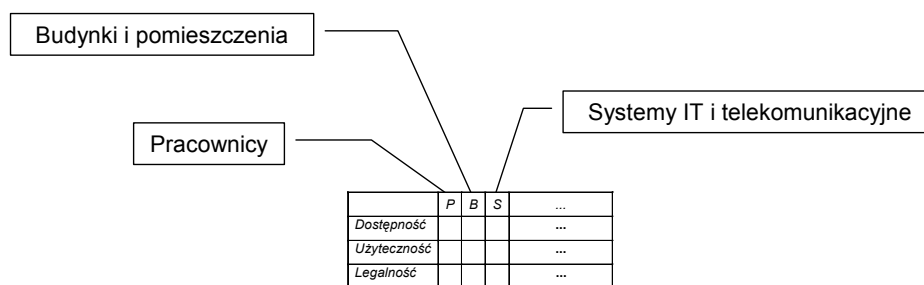


Rys. 3. Powiązanie kluczowych pojęć użytych w polityce bezpieczeństwa

Schemat na powyższym rysunku przedstawia relację pomiędzy podstawowymi zasadami postępowania, które stanowią wynikowy element „Polityki”, a celami biznesowymi organizacji i ogólnie obowiązującymi przepisami prawa dotyczącymi bezpieczeństwa. Schemat należy czytać następująco:

- *Podstawowe zasady postępowania* określają jak unikać lub/i zmniejszać skutki zdarzeń związanych z występowaniem zagrożeń.
- *Zagrożenia* mogą powodować niedostępność lub nieużyteczność zasobów.
- *Zasoby* są potrzebne do prowadzenia *działań operacyjnych*.
- *Działania operacyjne* są prowadzone w celu realizacji *celów biznesowych* i są w zgodzie z ogólnymi *przepisami prawa m.in. dotyczącymi bezpieczeństwa*.

Struktura opisu podstawowych zasad ochrony jest zgodna z przedmiotem ochrony i opiera się na klasyfikacji zasobów istotnych z punktu widzenia prowadzonych działań operacyjnych. Dla łatwiejszej i szybszej orientacji w treści podstawowych zasad ochrony każdy podrozdział opisu oznaczany jest zgodnie z metodą pokazaną na rys. 4.



Rys. 4. Metoda oznaczenia kategorii podstawowych zasad postępowania w odniesieniu do poszczególnych elementów przedmiotu ochrony

Poniżej przytoczono kilka przykładów podstawowych zasad postępowania, które mogą dotyczyć dotyczą losowo wybranych rodzajów zasobów, czyli elementów przedmiotu ochrony.

„Należy zapobiegać wystąpieniom i minimalizować skutki:

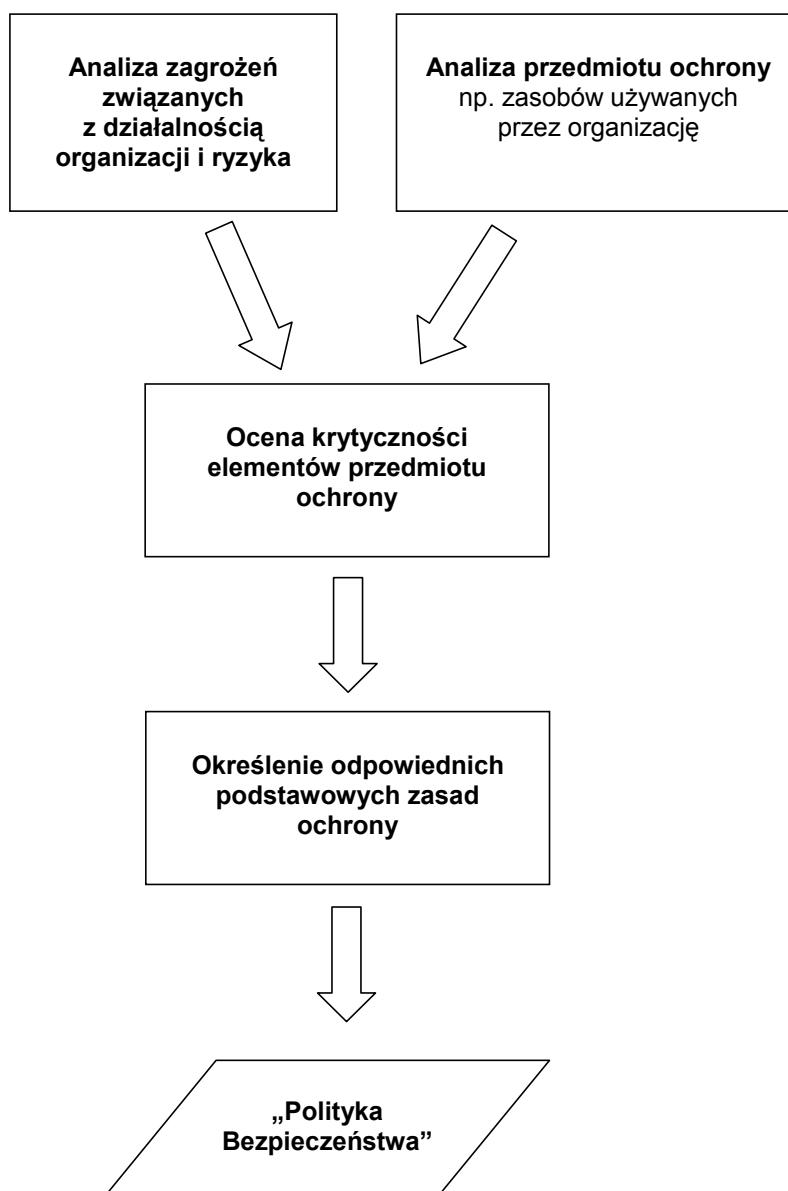
- nieobecności pracowników w miejscu pracy na skutek przyczyn obiektywnych (np. choroba, śmierć, aresztowanie, porwanie) – P,
- braku potrzebnych kompetencji (np. niewiedza jak należy wykonywać dane działanie, nieumiejętność użycia narzędzi potrzebnych do wykonania działania) – P,

- braku dyspozycyjności pracowników ze względu na realizowanie przez nich innych działań (np. odgórne polecenie będące w sprzeczności z obowiązkiem wykonywania danego działania, absorbowanie pracownika na podstawie przepisów określających obowiązki działania pracodawców na rzecz obronności kraju) – P,
- braku określonej struktury organizacyjnej z przydziałem odpowiedzialności za działania lub braku nadania odpowiedniego pełnomocnictwa – I,
- ograniczenia skuteczności działań na skutek pogorszenia wizerunku lub zmniejszenia się zaufania społecznego (np. niewystarczający poziom zaufania klientów na skutek pogorszenia wizerunku) – I,
- braku niezbędnych warunków do pracy (zbyt niska temperatura na skutek awarii ogrzewania, zbyt mała zawartość tlenu w powietrzu na skutek awarii wentylacji, za słabe oświetlenie miejsca pracy na skutek braku prądu, brak funkcji sanitarnych na skutek awarii wodociągowej lub kanalizacyjnej, szkodliwy wpływ otoczenia na skutek skażenia lub zapylenia) – B,
- przemieszczenia mebli lub wyposażenia powodującego ich niedostępność (np. kradzież, nieautoryzowane pożyczenie, zagubienie) – M.”

Podstawowe zasady ochrony w skrótej formie zawarte są ponadto na jednej stronie formatu A3 i nadają się do powieszenia w widocznym miejscu w pomieszczeniach zajmowanych przez pracowników organizacji, jako streszczenie „Polityki Bezpieczeństwa”.

## Metodyka

Droga do opracowania dokumentu pt. „Polityka Bezpieczeństwa” jest wieloetapowa. Dobre rozeznanie specyfiki działania danej organizacji stanowi warunek konieczny stworzenia „Polityki” „na miarę”. Rys. 5 prezentuje zadania, które według metodyki ITTI należy wykonać w drodze do opracowania ostatecznego dokumentu.



Rys. 5. Zadania zmierzające do stworzenia dokumentu polityki bezpieczeństwa

Jednym z elementów przygotowania do sformułowania „Polityki Bezpieczeństwa” jest określenie zagrożeń i ryzyka z nimi związanego. Pozwala to uświadomić sobie jakie czynniki i w jakim stopniu mogą uniemożliwić organizacji osiągnięcie założonych przez nią celów biznesowych. Jednocześnie zagrożenia stanowią niejako schemat formułowania podstawowych zasad ochrony. Do wyznaczenia zagrożeń i ryzyka służy analiza ryzyka.

### **Analiza ryzyka**

ITTI analizę ryzyka wykonuje według normy australijsko-nowozelandzkiej AS/NZ 4360 pt.: „Risk Management” [ASNZ99]. Analizę ryzyka wykonuje się według następującego schematu działania:

- W badaniu ankietowym dotyczącym zagrożeń, ITTI przedstawia przykładową listę zagrożeń, jakie mogą dotyczyć konkretnej organizacji.

- Spośród tych propozycji ankietowani pracownicy wybierają, ich zdaniem zagrożenia odpowiadające ich organizacji (bądź dodają nowe zagrożenia) i wskazują grupy incydentów związanych z tymi zagrożeniami podając jednocześnie częstość ich występowania, jak i średnie skutki, jakie mogą potencjalnie spowodować.
- W przeprowadzonym badaniu ankietowym dotyczącym zdarzeń, jakie wystąpiły w historii organizacji pracownicy wskazują incydenty, które faktycznie wystąpiły w historii organizacji podając moment ich wystąpienia i skutek, jaki wywołały.
- Po zebraniu danych dotyczących grup incydentów i incydentów historycznych następuje szacowanie częstości i średnich skutków, co pozwala na wyznaczenie poziomu ryzyka związanego z zagrożeniami, którym odpowiadają poszczególne grupy incydentów.

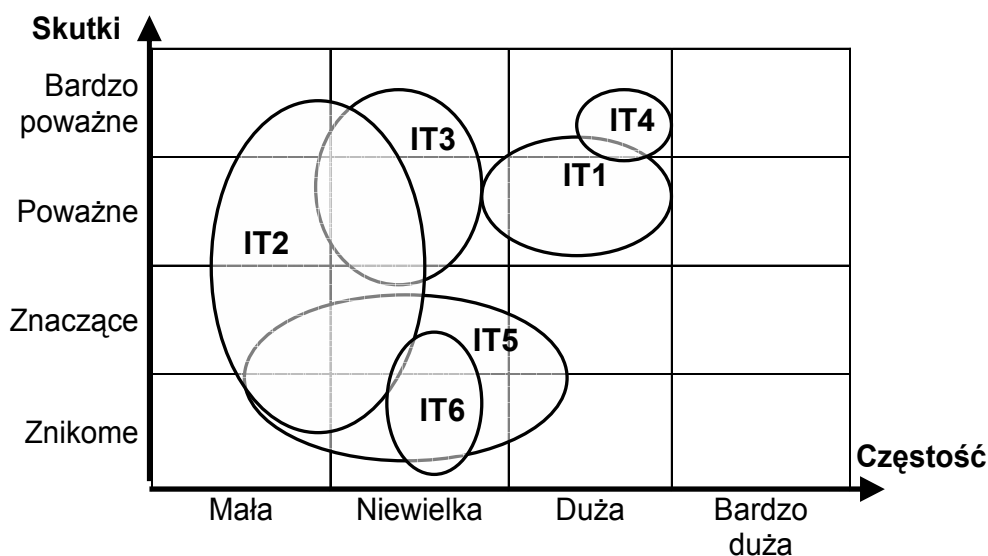
Trzeba zaznaczyć, że etap pozyskiwania informacji w formie wywiadów bezpośrednich, dyskusji oraz badania kwestionariuszowego lub ankietowego jest bardzo ważny. Należy dołożyć wszelkich starań, by zebrane dane były rzetelne i wiarygodne, a ponadto na odpowiednim poziomie ogólności, aby móc służyć do konstruowania treści „Polityki Bezpieczeństwa”.

Analiza ryzyka przeprowadzana jest jakościowo, a więc kategoryzuje ryzyka jako niskie, średnie i wysokie. Jest to podejście wystarczające do ustalenia priorytetów podstawowych zasad ochrony. Przykładowy wynik analizy zagrożeń dla losowo wybranych rodzajów zasobów pokazuje Tab. 3.

Tab. 3 Poziomy ryzyka, skutków i częstości dla zagrożeń z grupy Infrastruktura

ID	Grupa incydentów/zagrożenia	Częstość		Skutki		Poziom ryzyka
		Średnia	Odchylenie standardowe	Średnia	Odchylenie standardowe	
IT1	Awaria infrastruktury budynku	2,8	0,5	3,3	0,5	A
IT2	Awaria sieci	1,5	0,6	2,8	1,5	B
IT3	Awaria systemu IT	1,8	0,4	3,4	0,9	B
IT4	Brak odpowiednich zabezpieczeń infrastruktury budynku	3,0	0,0	4,0	0,0	A
IT5	Problemy z bazą lokalową	1,8	0,8	1,8	0,8	C
IT6	Nieodpowiednie warunki pracy	2,0	0,0	1,5	0,7	C

Liczby w tabeli są jedynie wartościami na abstrakcyjnej osi, a nie konkretnymi kwotami strat lub roczną liczbą incydentów. Analogiczne wyniki przedstawiane są w postaci diagramu, którego przykład zaprezentowano na rys. 6.



Rys. 6. Poziomy ryzyko zagrożeń z grupy Infrastruktura na płaszczyźnie częstość-skutki

Analiza ryzyka kończy się podsumowaniem.

Równoległe z analizą ryzyka przeprowadza się identyfikację obszarów działań i zasobów wykorzystywanych przez organizację.

### Identyfikacja obszarów działań i zasobów

Celem identyfikacji obszarów działania i zasobów jest określenie istotnych z punktu widzenia funkcjonowania organizacji obszarów działań oraz wykorzystywanych w tych obszarach zasobów (np. informacje, ludzie, zasoby materialne). Po identyfikacji obszarów działań nadaje się im miarę istotności dla funkcjonowania organizacji, co pozwala na wytypowanie zasobów krytycznych. Określenie tych zasobów pozwala z kolei na ustalenie priorytetów dla poszczególnych elementów przedmiotu ochrony. W ramach pracy identyfikuje się również podmioty zewnętrzne, z którymi współpracuje organizacja i rodzaj tej współpracy. Czynniki te pozwalają sformułować podstawowe zasady ochrony na styku z otoczeniem organizacji.

Dane wykorzystane do identyfikacji obszarów działań i określenia najbardziej istotnych zasobów są zebrane w ramach ankiety dotyczącej obszarów działania i zasobów, a często również w trakcie spotkań i rozmów bezpośrednich.

Uczestnicy badania ankietowego dotyczącego obszarów działań i zasobów określają takie atrybuty zidentyfikowanych obszarów jak:

- nazwa obszaru działania,
- opis czynności wykonywanych w ramach danego obszaru działania,
- informacje, dokumenty i stan, generowane po zakończeniu pracy w ramach danego obszaru,
- zasoby wykorzystywane w obszarze działania:
  - ludzie – pracownicy (stanowiska pracy) potrzebni do wykonania działań w ramach obszaru działań,
  - informacja i dokumentacja,
  - infrastruktura,

- krytyczność – jakie opóźnienie w działaniu obszaru powoduje zagrożenie dla działalności organizacji.

Typowe obszary działań można zgrupować w następujące kategorie:

- administracja (w tym administracja ICT),
- finanse,
- kadry,
- działania operacyjne (charakterystyczne dla organizacji prowadzącej określoną działalność)
- kontakty z otoczeniem,
- zaopatrzenie.

Wynikiem badania ankietowego jest lista obszarów działań potrzebna do określenia cech charakterystycznych dla funkcjonowania danej organizacji przed przygotowaniem treści „Polityki Bezpieczeństwa” oraz lista zasobów z wyróżnieniem tych najbardziej istotnych dla zapewnienia ciągłości działania instytucji.

Lista najistotniejszych zasobów, którymi organizacja dysponuje jest wyznaczona zgodnie z następującymi krokami:

- Zidentyfikowanie zasobów wykorzystywanych w poszczególnych obszarach działań.
- Zidentyfikowanie obszarów działań najbardziej istotnych dla funkcjonowania organizacji – takich, których opóźnienie dłuższe niż 1 godzina lub 1 dzień powodują przerwę w działaniu organizacji.
- Zidentyfikowanie zasobów służących realizacji działań w najbardziej istotnych obszarach określonych w poprzednim kroku.

Po wykonaniu powyższych kroków, zasoby niezbędne do wykonywania prac w ramach najistotniejszych obszarów działania są już zidentyfikowane. Zasoby te zostają następnie podzielone na podgrupy (infrastruktura, ludzie, informacja). Ponieważ zależą one w znacznym stopniu od specyfiki działania analizowanej organizacji przykładowe wyniki tego zadania nie zostały zamieszczone w niniejszym artykule. Identyfikacja obszarów działań i zasobów kończy się podsumowaniem.

## Prace dodatkowe

Oprócz samego dokumentu polityki bezpieczeństwa” klienci ITTI często życzą sobie wykonania audytu stanu bezpieczeństwa oraz sformułowania zaleceń zmian wraz z priorytetami ich wprowadzania, w oparciu o treść „Polityki” oraz wyniki audytu.

Wzorzec audytowy jest konstruowany na bazie ogólnie przyjętych standardów dotyczących bezpieczeństwa działania organizacji i bezpieczeństwa informacji (m.in. standard BS7799 [BS7799], najlepsze praktyki NRIC [NRIC], normę PAS 56 [PAS56], zalecenia Banku Światowego [WB04]). W ramach audytu określa się które ze środków ochrony organizacja już wdrożyła, a które nie są jeszcze stosowane. Następnie w raporcie klient otrzymuje wyselekcjonowane zalecenia dotyczące środków ochrony, które nie zostały w pełni, bądź w ogóle wdrożone w organizacji. Zwykle jest ich kilkadziesiąt lub ponad 100. Konsultanci ITTI wskazują na najbardziej istotne z punktu widzenia realizowania polityki bezpieczeństwa. Często na zamówienie klienta szacowany jest czas i nakład, jaki jest potrzebny do ich wdrożenia.

Przykładowe zalecenia przedstawiają się następująco.

- „Należy wskazać osoby odpowiedzialne za każdy z aktywów lub procesów bezpieczeństwa i udokumentować szczegóły tej odpowiedzialności.” – I

- „Należy opisać stosowaną w urzędzie klasyfikację informacji w zależności od ich ważności dla firmy, ich wrażliwości, dostępności lub też krytyczności, która pomoże określić w jaki sposób informacja ma być przechowywana i chroniona.” – D
- „Procedury operacyjne powinny być jasno zdefiniowane i przestrzegane przez pracowników również w sytuacji zagrożenia, aby uniknąć obniżenia poziomu bezpieczeństwa przez ich niestosowanie.”
- „W przypadku wynoszenia z urzędu sprzętu, informacji i oprogramowania należy opracować zasady udzielania zezwolenia w formie pisemnej.”

Konsultanci ITTI dostosowują metodykę prowadzenia projektu do konkretnych wymagań klienta, który ze względu na swoje przekonania lub np. standardy korporacyjne potrzebują nieco innego podejścia lub wyników pracy.

## Wnioski

*Nie ma bezpieczeństwa za darmo i obrony za małe pieniądze* – G. Robertson

Bezpieczeństwo jest jedną z funkcji jakości. Dlatego dążąc do ustawicznego podwyższania jakości naszego życia warto jest zatroszczyć się również o bezpieczeństwo firmy lub instytucji w której pracujemy. Pierwszym krokiem w kierunku bezpiecznej organizacji musi być sformułowanie i wdrożenie własnej polityki bezpieczeństwa. Wszystkie inne działania na rzecz bezpieczeństwa powinny być jej bezwzględnie podporządkowane.

Gdyby opracowanie „Polityki Bezpieczeństwa” było prostym do zrealizowania zadaniem większość organizacji posiadałaby obecnie tego rodzaju dokumenty. Jak pokazują jednak statystyki nie wiele organizacji w Polsce posiada „Politykę Bezpieczeństwa”. Nie wiele jest też polskich publikacji na ten temat<sup>2</sup>. Zaproponowana metodyka jest prawdopodobnie jedną z wielu dróg prowadzących do „bezpiecznej organizacji”. Warto jednak z którejś z nich skorzystać, aby móc spać spokojnie wiedząc, że dołożyliśmy wszelkich starań, by nasze zawodowe zaangażowanie nie poszło na marne.

„Polityka Bezpieczeństwa” to nie standard lub ogólny zbiór dobrych praktyk w zakresie bezpieczeństwa. „Polityka Bezpieczeństwa” to – jak to zostało powiedziane – pochodna celów biznesowych lub statutowych organizacji. Powinna być zatem „szyta na miarę” konkretnej organizacji. Wszak nikt z nas nie lubi chodzić w za luźnej marynarce, bądź zbyt ciasnych spodniach. Podejście dedykowane wymaga analizy specyfiki działania organizacji, zasobów, którymi się posługuje i realnych zagrożeń.

W artykule nie określono w sposób wyczerpujący sposobu wdrażania „Polityki Bezpieczeństwa” w organizacji. Jest to temat nie mniej ważny i prawdopodobnie dużo bardziej skomplikowany, gdyż przeważają w nim czynniki socjologiczne i miękkie (ang. *soft*) m.in. psychika pracownika, kultura organizacji, podatność na motywację itp. Wdrożenie „Polityki Bezpieczeństwa” jest dużym wyzwaniem dla organizacji, jednak bez wdrożenia opracowany dokument staje się bezużyteczną książką do której nikt nie zagląda. A przecież nie o to nam wszystkim chodzi.

## Bibliografia

- [CP-CSO] Chodzicki P., Poniewierski A.: Najczęstsze błędy polityki bezpieczeństwa i jej wdrożeń, CSO – Magazyn Zarządzających bezpieczeństwem, <http://cso.cxo.pl/>
- [ASNZ99] AS/NZ 4360 – Risk Management, 1999

---

<sup>2</sup> Dostępna jest jedyna książka po polsku [K99].

- [BS7799] BS 7799-2 – Security Standard: Information Security Management Systems - Specification with guidance for use, 2002
- [NRIC] NRIC Best Practice, Network Reliability and Interoperability Council, <http://www.nric.org/>
- [PAS56] PAS 56 – Guide to business continuity management, BSI, 2003
- [WB04] Technology Risk Checklist, World Bank, 2004
- [K99] T. Kifner, Polityka bezpieczeństwa i ochrony informacji, Helion, 1999, ISBN: 83-7197-187-7