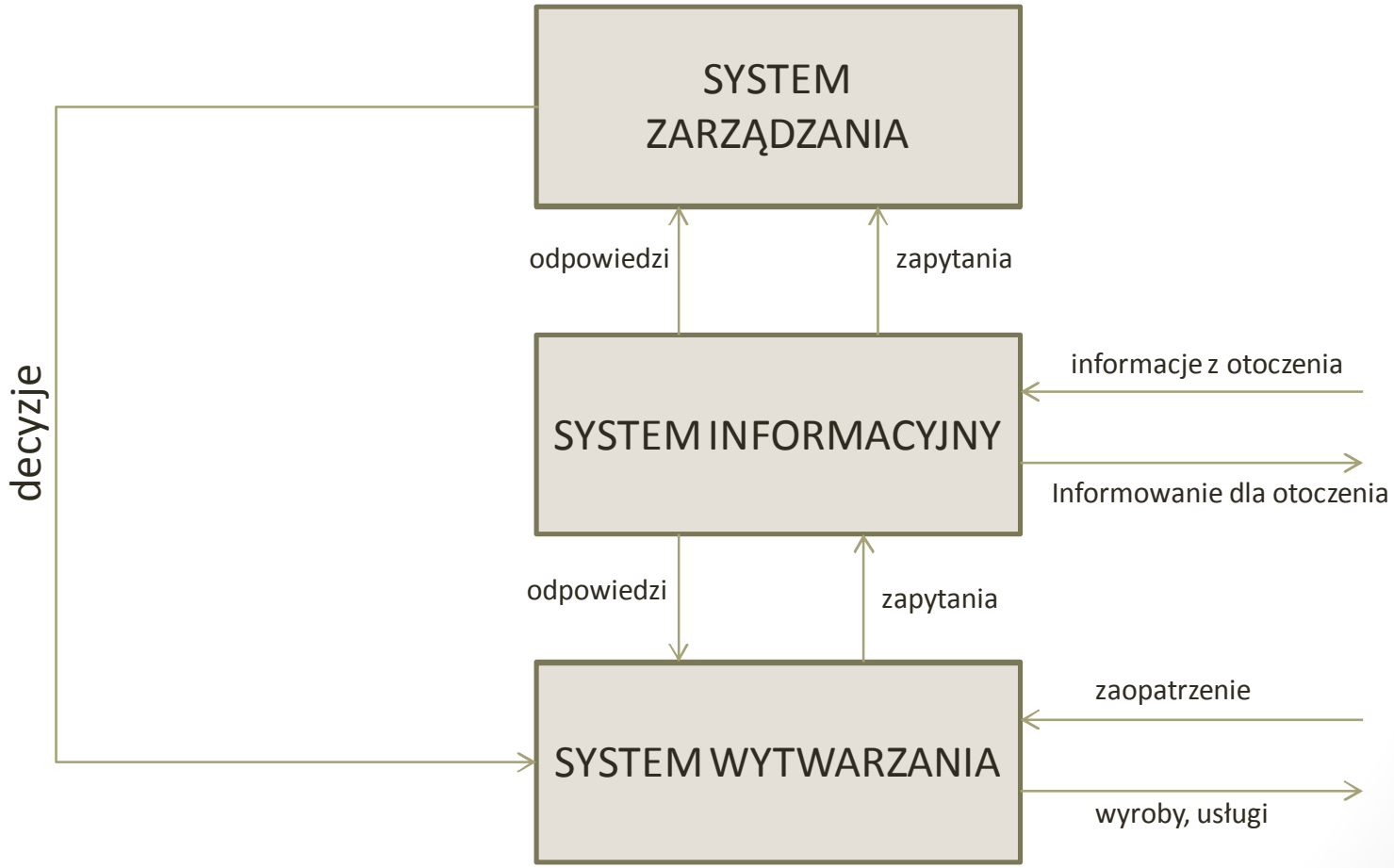
Bezpieczeństwo i koszty wdrażania Informatycznych Systemów Zarządzania

Hubert Szczepaniuk
Wojskowa Akademia Techniczna
im. Jarosława Dąbrowskiego

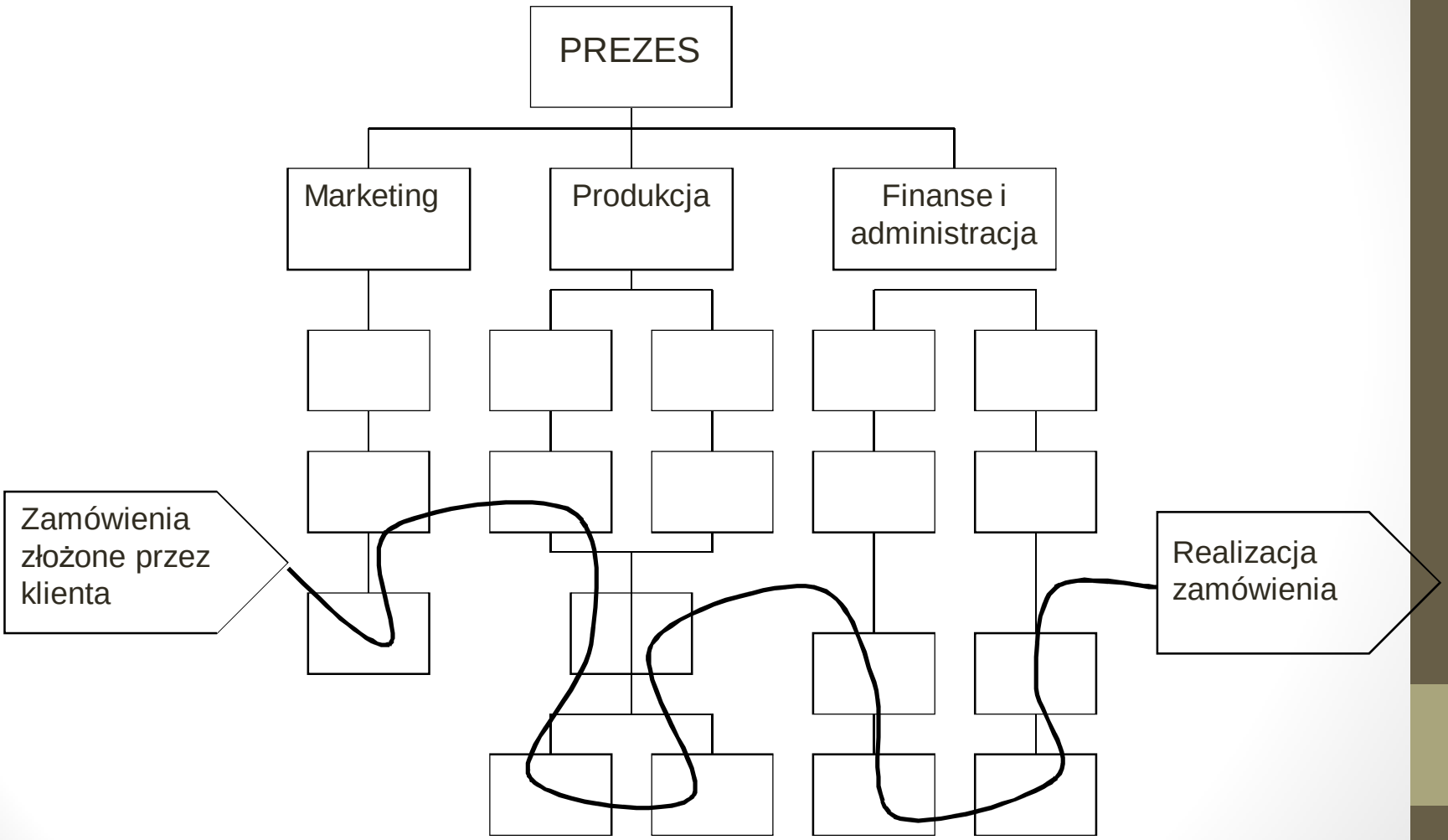
Problem wdrażania IT w organizacji

- Wskaźnik powodzeń dużych przedsięwzięć informatycznych wdrażanych w organizacjach jest bardzo niski.
- Za najpoważniejsze zagrożenia wynikające z niewłaściwego wdrożenia IT uznaje się utratę przychodów, klientów lub reputacji oraz wzrost kosztów prowadzonej działalności.
- Awarie systemów informatycznych są najgroźniejsze działów produkcyjnych, finansowych i zajmujących się obsługą klienta.
- **Brak metodologii, która pozwoliłaby zmierzyć spodziewane korzyści finansowe wdrożenia systemu przed rozpoczęciem wdrożenia.**

Rola i miejsce systemu informacyjnego



Przykład podejścia procesowego

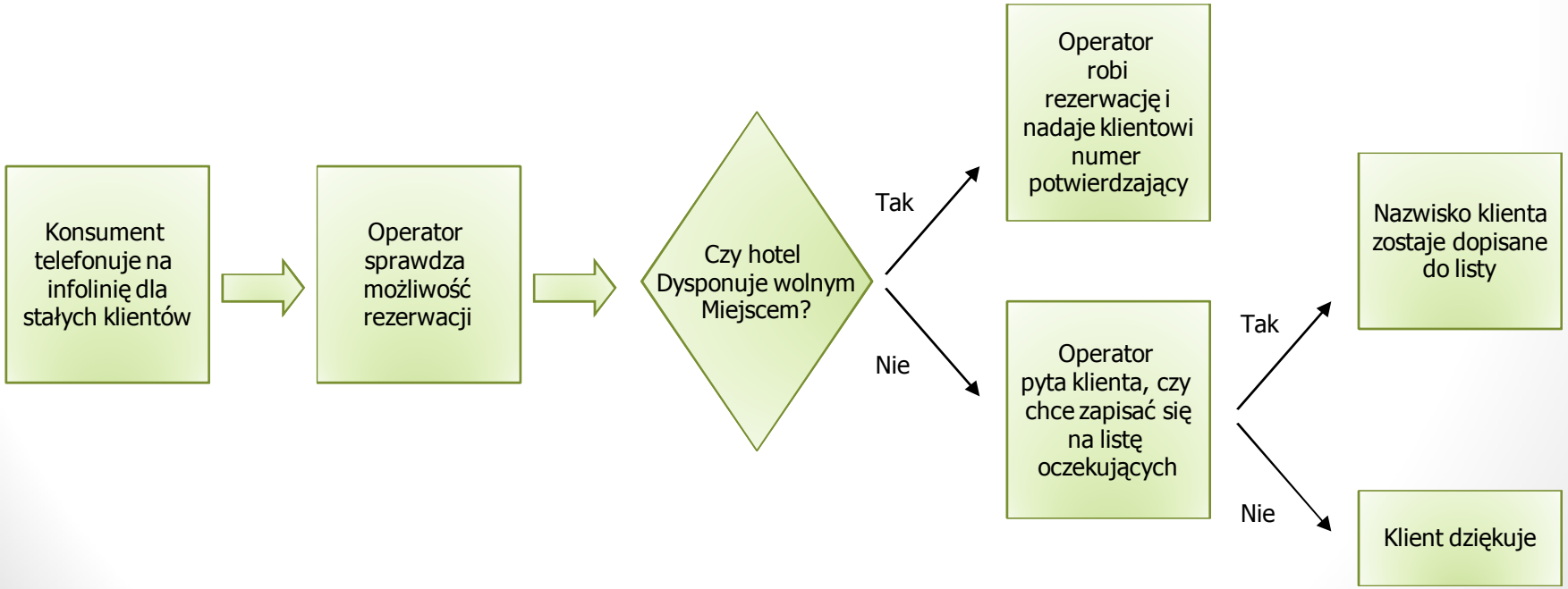


Przykład dotyczący jednej z sieci hoteli

- Proces rezerwacji pokoi dla stałych klientów

  Rola odpowiednio sformułowanych pytań w rozważaniu istniejących procesów, np.: „W jaki sposób powinniśmy traktować wartościowych klientów, gdy pytają o wolny pokój w momencie, gdy wszystkie są zajęte?”

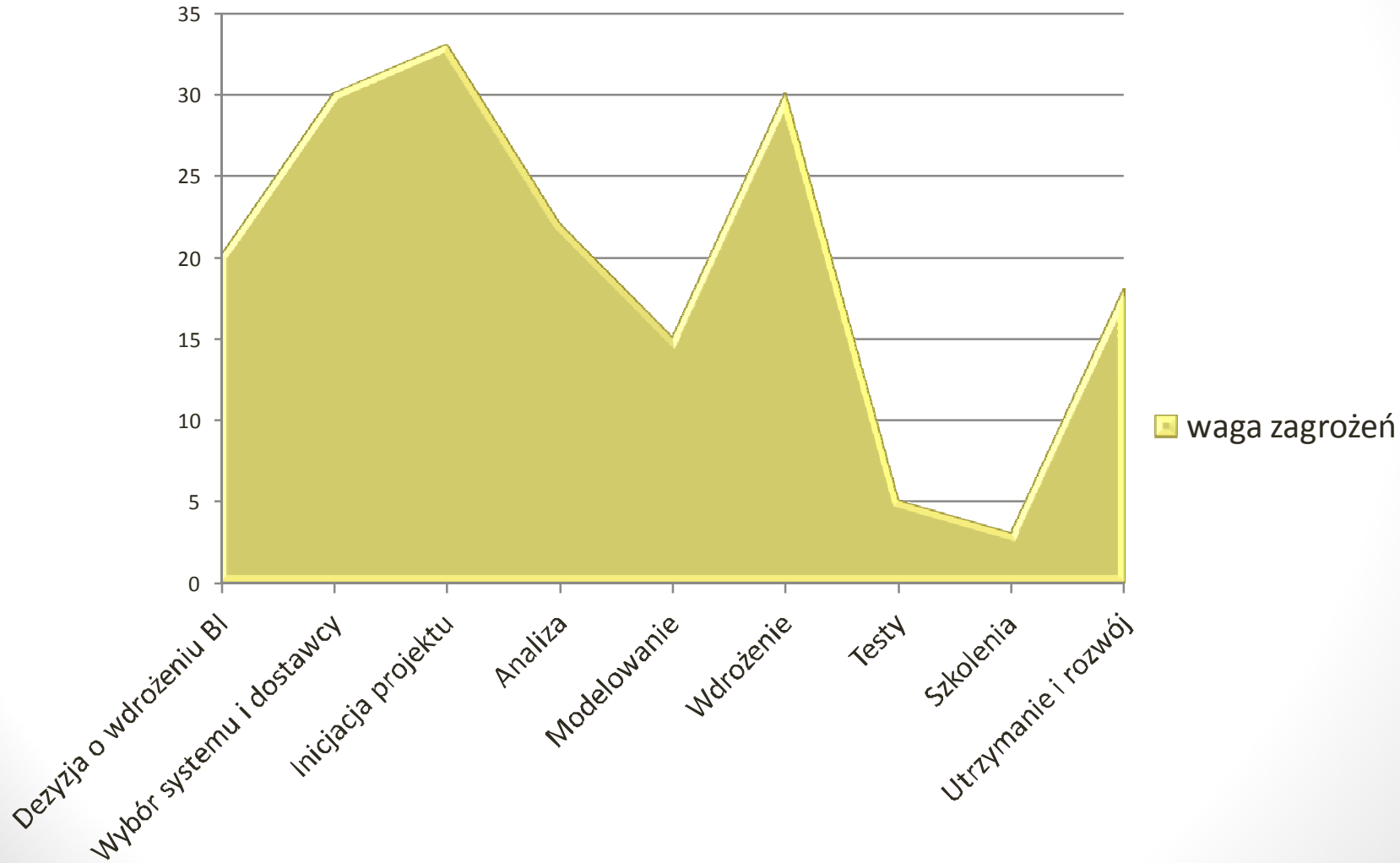
- <u>Dotychczasowy proces:</u>



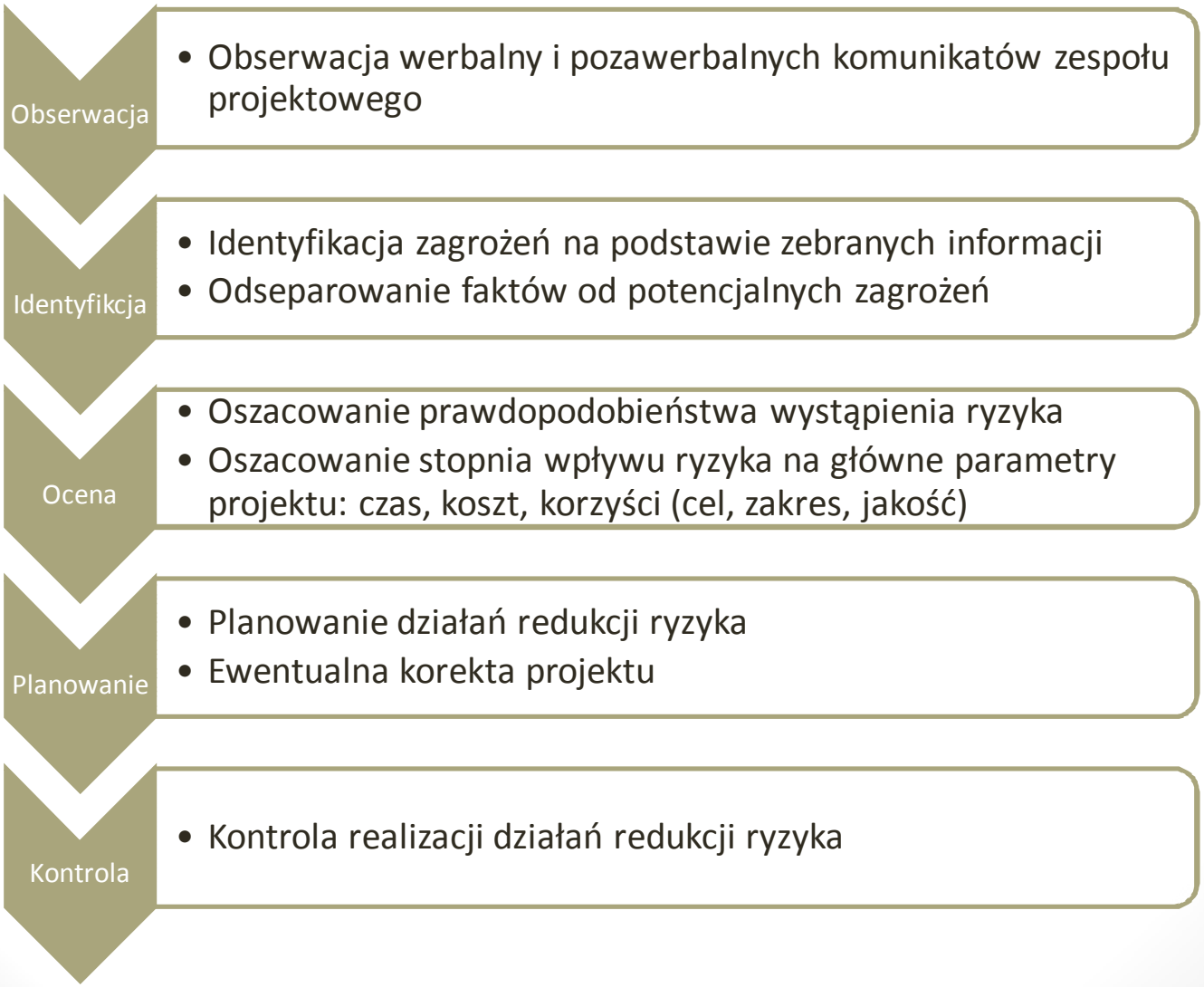
Przykład dotyczący jednej z sieci hoteli

- Nowy proces:
  - Zmieniony proces uwzględnia następujące elementy:
  - wielokanałowe możliwości rezerwacji (telefon, fax, Internet)
  - specjalna witryna dla stałych klientów
  - monitorowanie wolnych miejsc w pobliskich hotelach
  - blokowanie z wyprzedzeniem większej ilości miejsc dla klientów stałych

Intensywność występowania zagrożeń na poszczególnych etapach projektowania



Metamodel zarządzania ryzykiem przy wdrożeniu Informatycznych Systemów Zarządzania



Ilościowe szacowanie ryzyka

- Podstawą do sprawnego zarządzania ryzykiem wdrożenia Systemów Informatycznych Zarządzania jest wyznaczanie odpowiednich charakterystyk ilościowych.
- ***Ryzyko formalnie można zdefiniować jako wymierne skutki wystąpienia negatywnego zdarzenia rozpatrywanego łącznie z prawdopodobieństwem zrealizowanie się takiego zdarzenia.***
- Przekładając podaną definicję na ogólny model matematyczny formuła ryzyka ma postać:

$$R = P \times S \qquad (1)$$

gdzie:

R – wartość ryzyka,

S – wymierne skutki wystąpienia negatywnego zdarzenia,

P – prawdopodobieństwo wystąpienia zdarzenia.

Ocena ryzyka w systemach informatycznych

- Przy ocenie ryzyka w systemach informatycznych, ze względu na specyfikę systemu, wykorzystuje się najczęściej trzy atrybuty ryzyka: wartość zasobu, częstotliwość wystąpienia zagrożenia dla zasobu, podatność elementów systemu informatycznego na zagrożenie. Można to opisać zna pomocą następującego modelu matematycznego:

$$P = C \times Po \quad (2)$$

$$R = C \times Po \times S \quad (3)$$

gdzie:

P – prawdopodobieństwo wystąpienia zdarzenia,

R – wartość ryzyka,

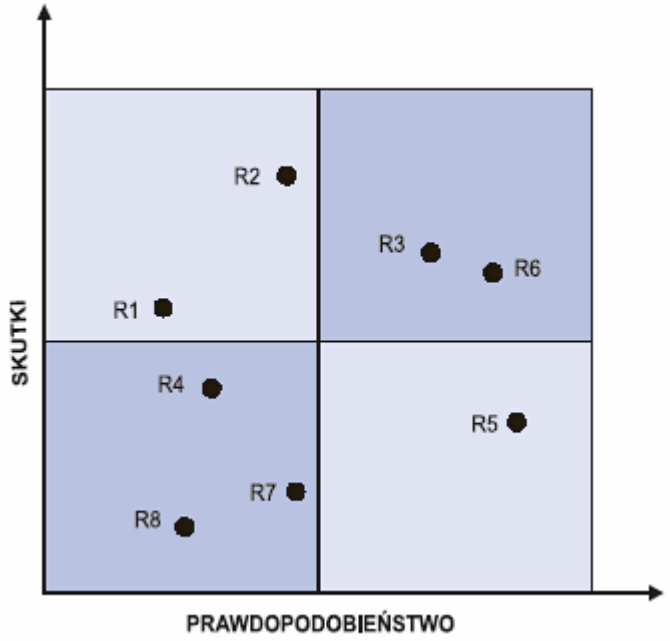
S – wymierne skutki wystąpienia negatywnego zdarzenia np.: przewidywana średnia utrata wartości aktywów, w wyniku wystąpienia zdarzenia,

C – częstotliwość występowania zagrożenia dla zasobu,

Po – podatność elementów systemu na zagrożenie – zgodnie z normą PN-I-13335–1:1999 podatność elementów systemu na zagrożenie jest to miara prawdopodobieństwa wykorzystania określonej podatności przez dane zagrożenie.

Metoda mapy ryzyka

- Na podstawie podstawowych parametrów ryzyka: skutków negatywnych zdarzeń i prawdopodobieństw ich wystąpienia można zbudować łączącą ich relację zwaną mapą ryzyka.
- Tworzenie mapy ryzyka polega na naniesieniu poszczególnych ryzyk na wykres kartezjański, gdzie współrzędnym X odpowiada wartość prawdopodobieństwa, zaś współrzędna Y wyraża skutki.



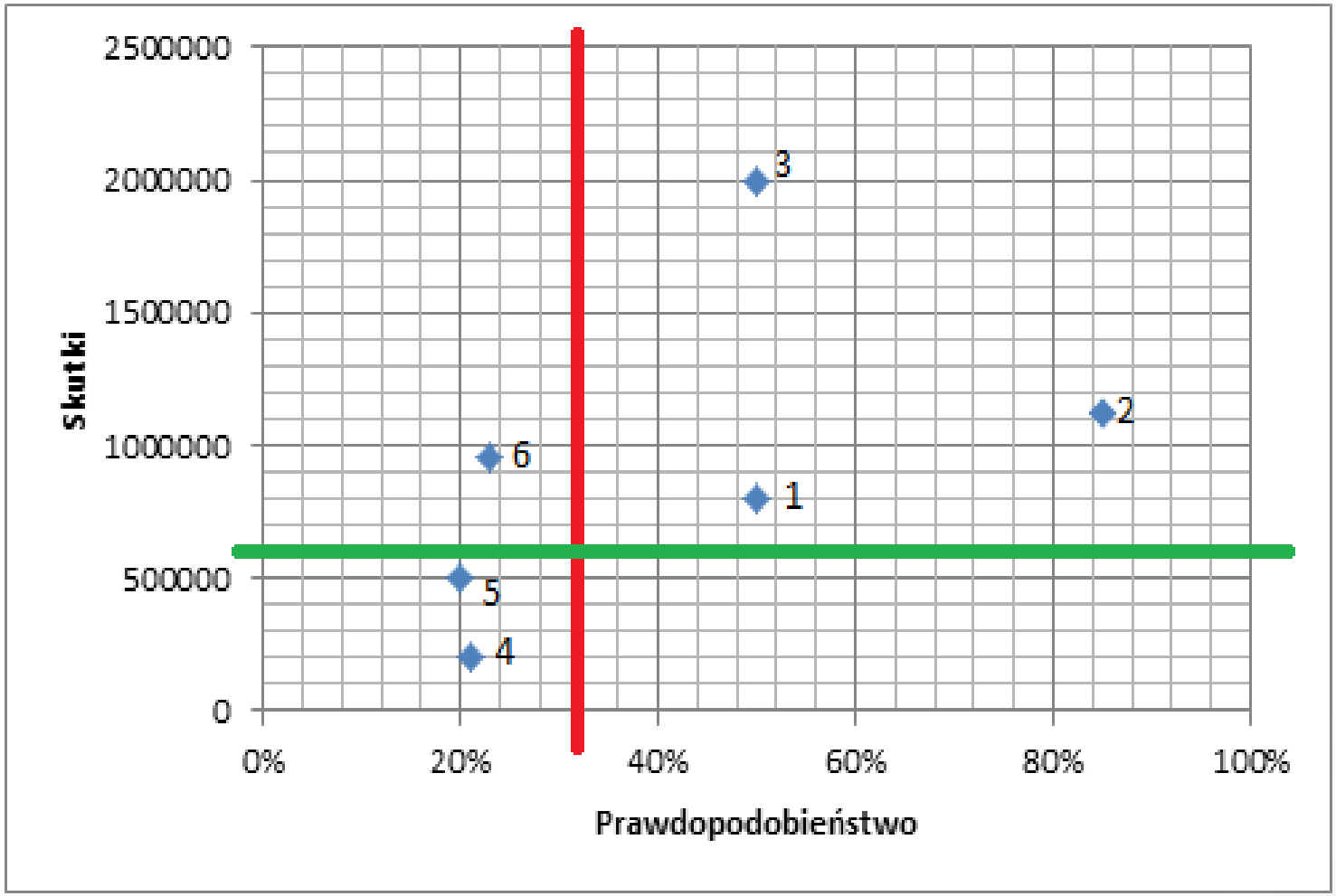
Przykład budowy mapy ryzyka

Lp.	Rodzaj zagrożenia	Prawdopo-dobieństwo wystąpienia %	Straty PLN	Współczynnik ekspozycji	Ilościowa wartość ryzyka
1	Brak świadomości i poparcia projektu na najwyższym poziomie zarządzania w firmie.	50%	800 000	1	400 000
2	Niekompatybilność zakupionego sprzętu z pozostałymi systemami lub jego niedostosowanie do wymagań systemu.	85%	1 122 000	5	4 768 500
3	Wdrażane rozwiązanie nie obsługuje wszystkich wymagań procesowych	50%	2 000 000	3	3 000 000

Przykład budowy mapy ryzyka

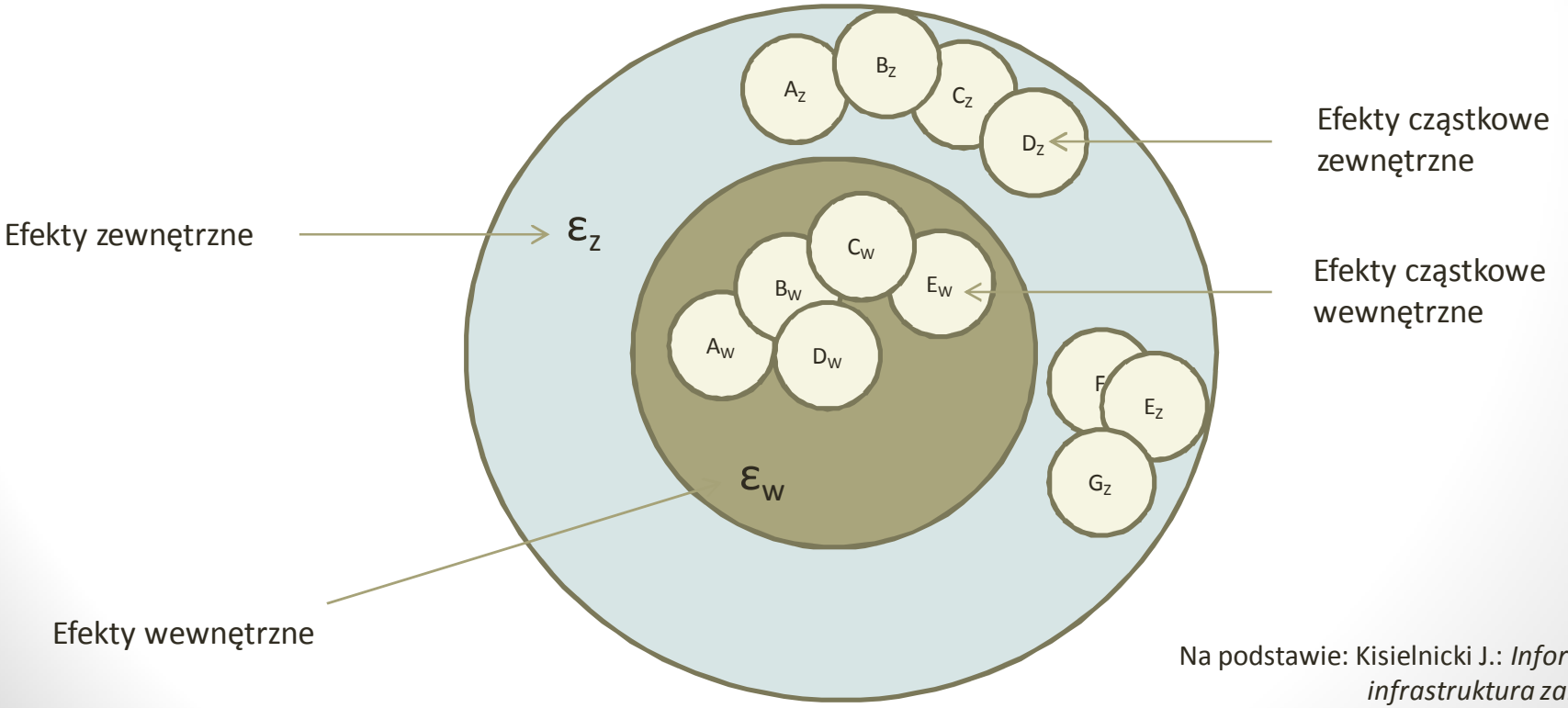
Lp.	Rodzaj zagrożenia	Prawdopo-dobieństwo wystąpienia %	Straty PLN	Współczynnik ekspozycji	Ilościowa wartość ryzyka
4	Problemy komunikacyjne na poziomie języka i pojęć między instytucją wdrażającą system, a zespołem dostawcy.	21%	200 000	5	210 000
5	Złe zabezpieczenie repozytoriów danych.	20%	500 000	3	300 000
6	Błędne zaplanowanie procesów w czasie.	23%	950 000	3	655 500
…	…	…	…	…	…

Przykład budowy mapy ryzyka



Modelowanie analizy i oceny efektywności SIZ

- Na efekty przedsięwzięcia informatycznego ma wpływ nie tylko ocena efektów działania systemu informatycznego w samej organizacji, ale również trudne do oszacowania oddziaływanie otoczenia.



Na podstawie: Kisielnicki J.: *Informatyczna infrastruktura zarządzania*

Wnioski

- Ryzyko powinno być mierzone i monitorowane w trakcie opracowywania i wdrażania Systemu Informatycznego Zarządzania, tak aby przedsiębiorstwo mogło kierować wdrożeniem na podstawie ryzyka, jakie jest gotowe zaakceptować.
- Efektywne działanie SIZ w organizacji może zostać podniesiona przez:
  - reorganizację procesów biznesowych (podejście procesowe do projektowania aktywności biznesowej przedsiębiorstwa),
  - wprowadzenie zarządzania ryzykiem,
  - efektywne wdrożenie SIZ (zapewnienie ciągłości działania organizacji),
  - wprowadzenie zarządzania bezpieczeństwem systemu informatycznego,
  - wprowadzenie badania efektywności SIZ już na etapie zamiaru podjęcia zmian w organizacji oraz przez cały okres eksploatacji inwestycji.

Bibliografia

[1] Barczak A., Sydoruk T., *Bezpieczeństwo systemów informatycznych zarządzania*, Bellona, Warszawa 2003

[2] Bartoszewicz G., Projektowanie wdrażania modułów logistycznych zintegrowanych systemów klasy ERP, WAE, Poznań 2007

[3] Champy J., *X-enginering przedsiębiors*twa, Placet, Warszawa 2003

[4] Chmielarz W., *Zagadnienia analizy i projektowania informatycznych systemów wspomagających zarządzanie*, Uniwersytet Warszawski, WNWZ, Warszawa 2000

[5] Gałach A., *Instrukcja zarządzania bezpieczeństwem systemu informatycznego*, ODDK, Gdańsk 2004

[6] Kisielnicki J., *MIS systemy informatyczne zarządzania*, Placet, Warszawa 2009

[7] Maleszka A., Łagowski E., *Wdrażanie zintegrowanych systemów zarządzania*, WSL, Poznań 2009

Dziękuje za uwagę