Wprowadzenie do systemów informacyjnych

Jakość i niezawodność systemu informacyjnego

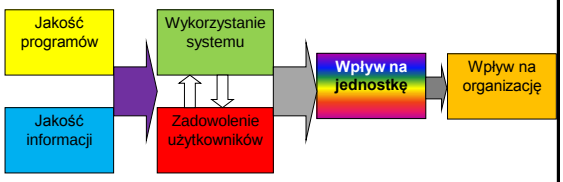
informatyka stosowana

Systemy informatyczne, które nie spełniają odpowiednich kryteriów jakościowych oraz niezawodnościowych należy oddać na złom

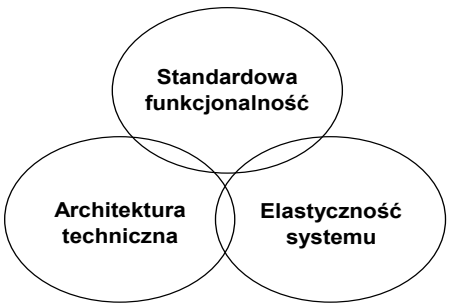
Jakość systemu informacyjnego główne czynniki

- **Poprawność** określa, czy oprogramowanie wypełnia postawione przed nim zadania i czy jest wolne od błędów.
- **Łatwość użycia** jest miarą stopnia łatwości korzystania z oprogramowania.
- **Czytelność** pozwala na określenie wysiłku niezbędnego do zrozumienia oprogramowania.
- **Ponowne użycie** charakteryzuje przydatność oprogramowania, całego lub tylko pewnych fragmentów, do wykorzystania w innych produktach programistycznych.
- **Stopień strukturalizacji (modularność)** określa, jak łatwo oprogramowanie daje się podzielić na części o dobrze wyrażonej semantyce i dobrze wyspecyfikowanej wzajemnej interakcji.
- **Efektywność** opisuje stopień wykorzystania zasobów sprzętowych i programowych stanowiących podstawę działania oprogramowania.
- **Przenaszalność** mówi o łatwości przenoszenia oprogramowania na inne platformy sprzętowe czy programowe.
- **Skalowalność** opisuje zachowanie się oprogramowania przy rozroście liczby użytkowników, objętości przetwarzanych danych, dołączaniu nowych składników, itp.
- **Współdziałanie** charakteryzuje zdolność oprogramowania do niezawodnej współpracy z innym niezależnie skonstruowanym oprogramowaniem.

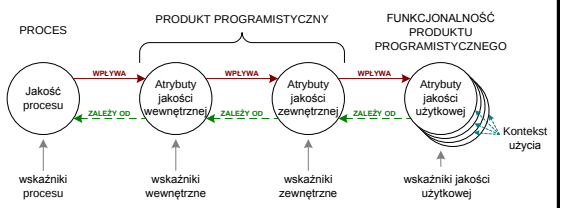
Czynniki determinujące ocenę jakości systemu informacyjnego



Podstawowe elementy oceny systemu informacyjnego



Proces oceny sytemu informacyjnego



Transakcje przeprowadzane w dobrze zaprojektowanym systemie informacyjnym powinny mieć cztery właściwości, określane kryptonimem **ACID**:

Atomicity – atomowość oznacza, że każda transakcja może być tylko w jednym z dwóch stanów: albo jest albo wykonana w całości, ale stan systemu jest taki, jakby nigdy nie była wykonywana

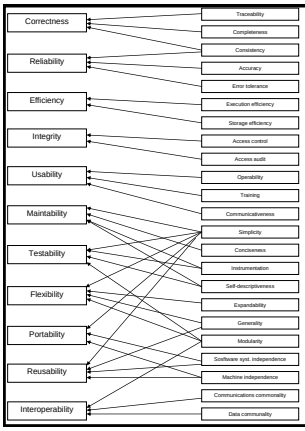
Consistency – konsekwencja oznacza, że system zachowuje integralność danych i pilnuje wszystkich ich ograniczeń

Isolation – izolacja oznacza, że nawet jeśli pewne czynności są w systemie wykonywane współbieżnie, to ich skutki ujawniają się w taki sposób, jakby były wykonywane niezależnie od siebie

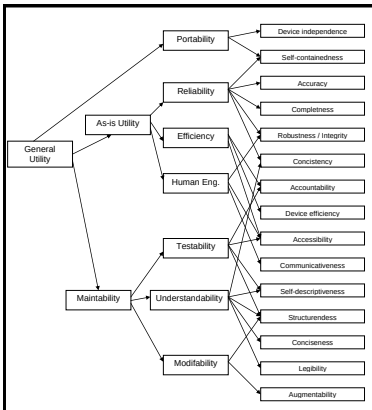
Durability – twardość oznacza, że skutki wykonywanych czynności są trwałe i niezmienne, nawet jeśli sprzęt albo oprogramowanie ulegnie awarii

Jakość systemu informacyjnego główne czynniki

- **Poprawność** określa, czy oprogramowanie wypełnia postawione przed nim zadania i czy jest wolne od błędów.
- **Łatwość użycia** jest miarą stopnia łatwości korzystania z oprogramowania.
- **Czytelność** pozwala na określenie wysiłku niezbędnego do zrozumienia oprogramowania.
- **Ponowne użycie** charakteryzuje przydatność oprogramowania, całego lub tylko pewnych fragmentów, do wykorzystania w innych produktach programistycznych.
- **Stopień strukturalizacji (modularność)** określa, jak łatwo oprogramowanie daje się podzielić na części o dobrze wyrażonej semantyce i dobrze wyspecyfikowanej wzajemnej interakcji.
- **Efektywność** opisuje stopień wykorzystania zasobów sprzętowych i programowych stanowiących podstawę działania oprogramowania.
- **Przenaszalność** mówi o łatwości przenoszenia oprogramowania na inne platformy sprzętowe czy programowe.
- **Skalowalność** opisuje zachowanie się oprogramowania przy rozroście liczby użytkowników, objętości przetwarzanych danych, dołączaniu nowych składników, itp.
- **Współdziałanie** charakteryzuje zdolność oprogramowania do niezawodnej współpracy z innym niezależnie skonstruowanym oprogramowaniem.

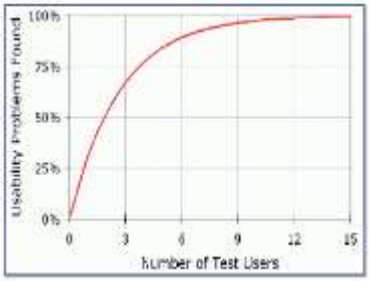


Model jakości systemu informatycznego McCalla wyróżnia 11 atrybutów głównych i 25 szczegółowych.



Model jakości Boehma

Testowanie w celu wykrycia i usunięcia błędów w systemie informacyjnym prowadzi do szybkiego wykrycia dużej liczby prostych błędów, ale potem dalsze błędy wykrywa się coraz trudniej, a 100% pewności, że system jest bezbłędny, nie osiąga się w praktyce nigdy.



Jakość systemu informacyjnego można rozważać w różnych aspektach

Model sukcesu zintegrowanego systemu zarządzania

Najstarszą instytucją, zajmującą się sprawą jakości oprogramowania jest *Software Engineering Institute* (SEI) przy Carnegie Mellon University w Pitsburgu

Model Dojrzałości Organizacyjnej (ang. *Capability Maturity Model*)

CMM

obejmuje:

„*software process assessment*”

„*software capability evaluation*”

Model CMM został stworzony przy założeniu, że:

„ciągły proces poprawy jest oparty na wielu małych, ewolucyjnych krokach, a nie na rewolucyjnych innowacjach.”

Doskonalszym narzędziem jest Zintegrowany Model Dojrzałości Organizacyjnej (ang. *Capability Maturity Model Integration*)

CMMI

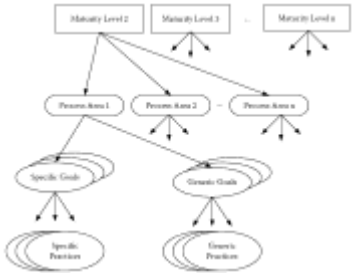
CMMI powstał jako połączenie istniejących modeli dojrzałości organizacyjnej, a przede wszystkim:

- **SW-CMM** for Software;
- **EIA/IS 731** for System Engineering;
- **IPD-CMM** for Integrated Product and Process Development

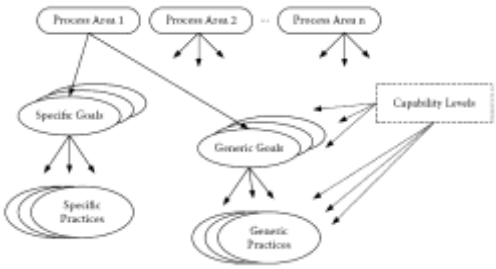
Model CMMI posiada dwie reprezentacje:

- reprezentacja stopniowana (ang. Staged)
- reprezentacja ciągła (ang. Continuous)

Komponenty modelu CMMI dla reprezentacji stopniowanej



Komponenty modelu CMMI w reprezentacji ciągłej



Unia Europejska stworzyła projekt o nazwie „Bootstrap”

Metodologia Bootstrap może być stosowana w małych i średnich przedsiębiorstwach produkujących oprogramowania lub w departamentach dużych organizacji.

Najlepsze doświadczenia w zakresie oceny dojrzałości systemów informatycznych zbiera i porządkuje norma

ISO/IEC 15504

Norma ISO/IEC 15504 składa się z 5 części:

ISO/IEC 15504-1 Information Technology – Process Assessment – Part 1 – Concepts and vocabulary.

ISO/IEC 15504-2 Information Technology – Process Assessment – Part 2 – Performing an assessment.

ISO/IEC 15504-3 Information Technology – Process Assessment – Part 3 – Guidance on performing an assessment.

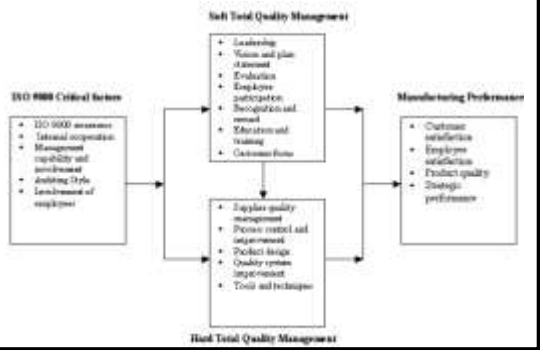
ISO/IEC 15504-4 Information Technology – Process Assessment – Part 4 – Guidance on use for process improvement and process capability determination.

ISO/IEC 15504-5 Information Technology – Process Assessment – Part 5 – An Exemplar Process Assessment Model.

Poziomy dojrzałości i odpowiadające im atrybuty procesów

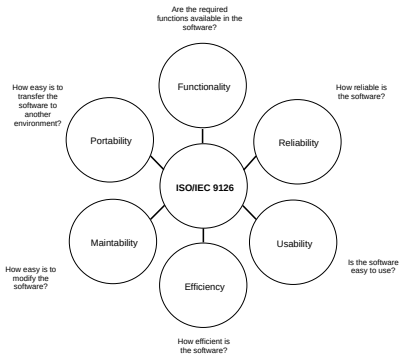
Kompleksowe zarządzanie jakością w zastosowaniu do projektowania systemów informacyjnych

Wymagania określające jakość systemów informatycznych dzielą się na 4 kategorie

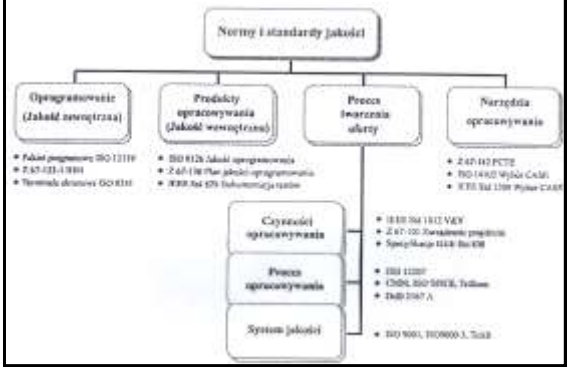


Bardzo istotną rolę przy zapewnianiu jakości systemów mają normy z serii **ISO 9000**

Model jakości systemów informatycznych ISO 9126



Normy ISO tworzą jednolity system



Względny koszt naprawy błędów oprogramowania w zależności od fazy produkcji, w której zostały znalezione

Zbieranie i analiza wymagań / Projekt architektury systemu	Kodowanie / Testowanie modułów	Integracja / Test systemu	Wczesna informacja zwrotna / Test wersji beta	Użytkowanie produktu
1X	5X	10X	15X	30X

Straty w aeronautyce (lotnictwie i lotach kosmicznych) spowodowane błędami w oprogramowaniu

	(1993)	(1996)	(1997)	(1998)	(1999)
	Airbus A320	• Ariane 5 • Galileo • Posejdon • Flight 965	• Lewis • Pathfinder • USAF Step	• Zenit 2 • Delta 3 • NEAR	• DS-1 Orion • 3 Galileo • Titan 4B
Łączny koszt		$640 milionów	$116.8 milionów	$255 milionów	$1.6 miliardów
Utrata życia	3	160			
Utrata danych		Tak	Tak	Tak	Tak

Dawniej mówiono o kontroli jakości, potem przedmiotem wysiłków było sterowanie jakością, następnie dbano o zapewnienie jakości i wreszcie obecnie hasłem przewodnim jest

zarządzanie jakością

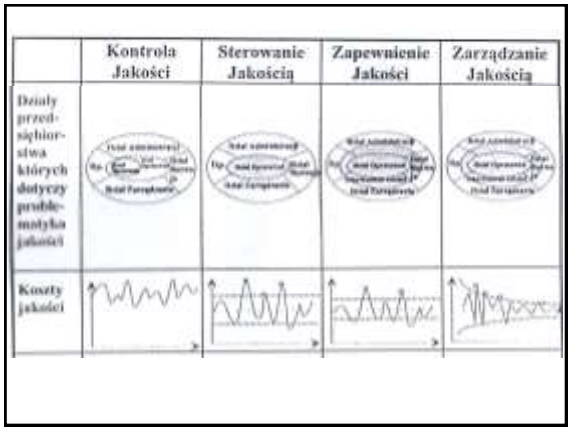
	Kontrola Jakości	Sterowanie Jakością	Zapewnienie Jakości	Zarządzanie Jakością
Okres	60–...	70–...	80–...	90–...
Cel	Ewaluacja i uzyskanie jakości na końcu łańcucha	Regularność uzyskiwania jakości	Zapewnienie sterowania jakością Zapewnienie zaufania	Ustawiczne doskonalenie jakości

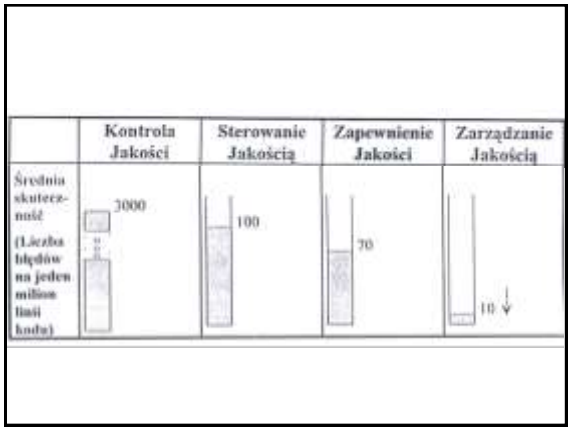
	Kontrola Jakości	Sterowanie Jakością	Zapewnienie Jakości	Zarządzanie Jakością
Stosowane środki	Test • Statyczny • Dynamiczny	Zdefiniowany, udokumentowany i opomiarowany proces • Proces standardowy • Cykle życia • Metody, narzędzia, zasady i procedury • Bazy danych procesu	Zdefiniowany, udokumentowany i zweryfikowany system jakości • Audity • Zapisy jakości	Zdefiniowany, udokumentowany, opomiarowany i doskonalony system jakości • Przyczynowa analiza błędów • Nadzór technologiczny • Uwzględnianie potrzeb klientów, kierownictwa, pracowników

Zarządzanie jakością systemu informatycznego jest jednym z najważniejszych zadań projektanta

	Kontrola Jakości	Sterowanie Jakością	Zapewnienie Jakości	Zarządzanie Jakością
Jakość oferty • Po sprawdzeniu • W trakcie • Przed sprawdzeniem • Ustawiczna	• Tak (oprogramowanie)	• Tak • Tak (terminy i koszty)	• Tak (+ usługi) • Tak • Tak (gwarancja)	• Tak • Tak • Tak (jeżeli stosowane jest zapewnienie jakości) • Tak

	Kontrola Jakości	Sterowanie Jakością	Zapewnienie Jakości	Zarządzanie Jakością
Sposób otrzymania jakości produktów	Detekcja/korekcja na końcu łańcucha (oprogramowanie dostarczone)	Detekcja/korekcja w trakcie projektowania (produkty pośrednie)	Detekcja/korekcja w trakcie projektowania. Detekcja/korekcja w odniesieniu do procesu	Detekcja/korekcja w trakcie projektowania. Detekcja/korekcja w odniesieniu do procesu (jeżeli stosowane jest zapewnienie jakości). Zapobieganie błędom poprzez analizę przyczynową.

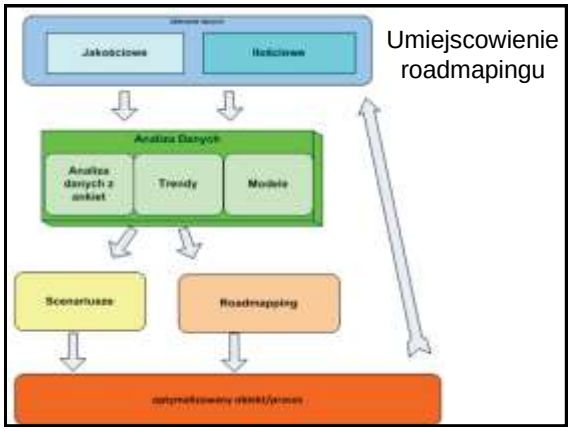




W zarządzaniu jakością dużą rolę odgrywa „roadmaping" projektu

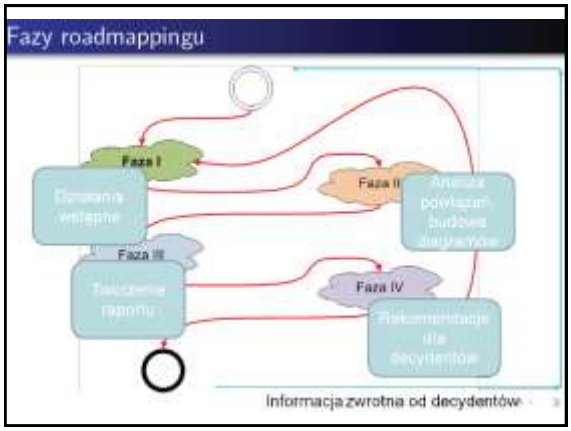
Co to jest roadmapping?

- Proces wspomagania decyzji integrujący działania biznesowe, naukowe lub administracyjne z czynnikami technologicznymi i produktowymi poprzez analizę i wizualizację relacji i związków czasowych między modelowanymi obiektami
- Powiązanie sfery technologicznej z innymi odbywa się poprzez ukazanie interakcji pomiędzy obiektami produktowymi i technologicznymi, a rynkiem i sektorem b-r
- Analizowane są związki kauzalne pomiędzy przeszłością, stanem obecnym i przyszłymi uwarunkowaniami i konsekwencjami podjętych decyzji, z naciskiem na te ostatnie



Umiejscowienie roadmapingu

Fazy roadmappingu

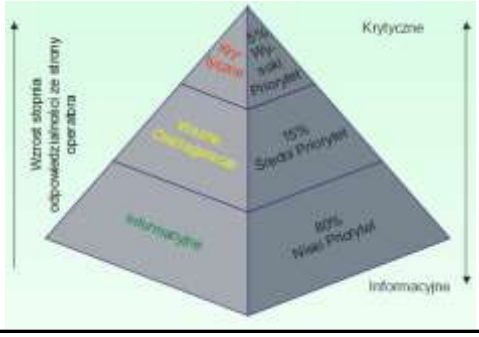


Ze względu na innowacyjność zwykle najbardziej cenione są programy tworzone przez młode zespoły programistów

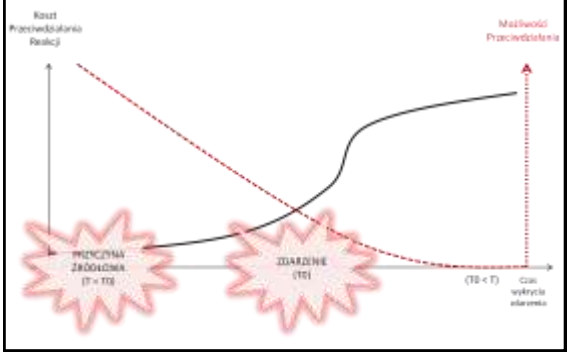
Ale – bez przesady!

Z problemem jakości systemów informacyjnych wiąże się problem zapewnienia odpowiedniej **niezawodności** ich działania

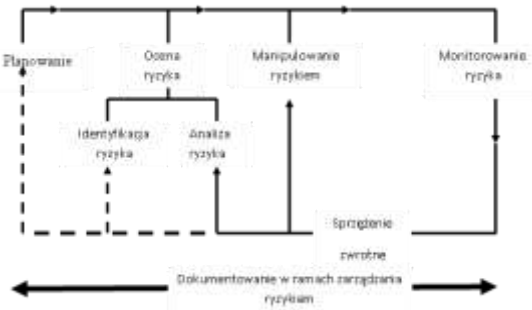
Klasyfikacja sygnałów zagrożeń



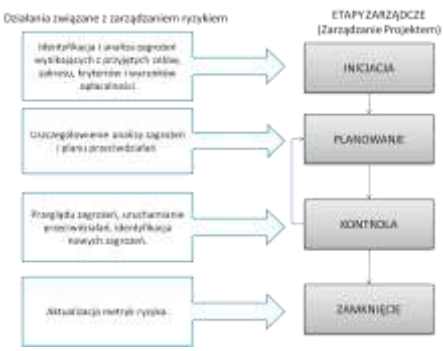
Ważnym pojęciem jest **zarządzanie ryzykiem**



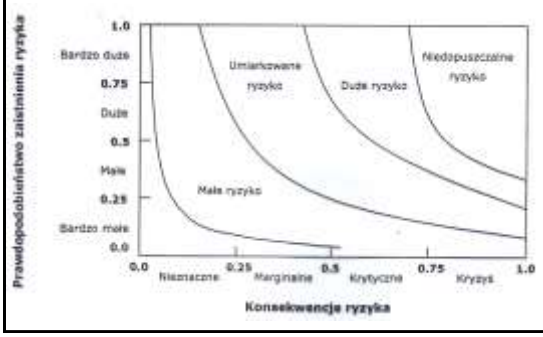
Przykładowy proces zarządzania ryzykiem



Zarządzanie ryzykiem a zarządzanie projektem



Można rozważać różne kategorie ryzyka



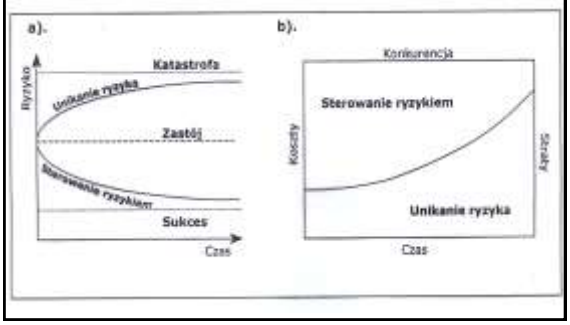
Przeciętny koszt godzinnej awarii systemu informacyjnego

Charakter Firmy	Koszt jednogodzinnej awarii w tys. dolarów
Brokerska	6480
Energetyczna	2800
Karty Kredytowe	2580
Telekomunikacyjna	2000
Wytwórcza	1600
Finansowa	1500
Sprzedaż detaliczna	1100
Farmaceutyczna	1000
Chemiczna	704
Ochrona Zdrowia	636
Rezerwacja Biletów Lotniczych	90

Etapy przygotowania strategii zabezpieczeń

1. Sprecyzowanie, co i przed czym mamy chronić, czyli określenie zasobów chronionych i zagrożeń.
2. Określenie prawdopodobieństwa poszczególnych zagrożeń
3. Określenie zabezpieczeń, czyli, w jaki sposób chronimy zasoby
4. Ciągłe analizowanie SI i zabezpieczeń w celu aktualizacji procedur zabezpieczających poprawiania jego ewentualnych błędów

Ryzyka można unikać albo można nim świadomie sterować

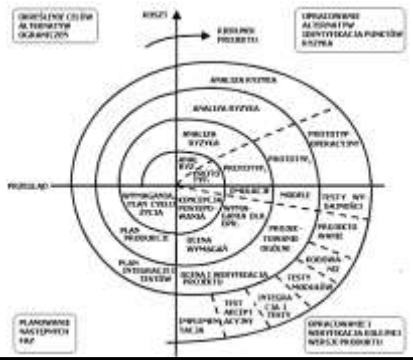


Pod pojęciem **sterowania ryzykiem** kryje się działanie mające na celu ograniczanie ryzyka poprzez planowanie, projektowanie i wdrażanie rozwiązań mających zapewnić utrzymanie ryzyka na poziomie możliwym do zaakceptowania.

W procesie sterowania ryzykiem można wyróżnić następujące etapy:

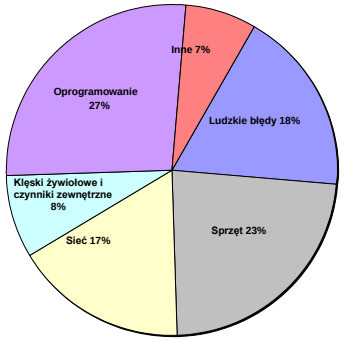
- wskazywanie zagrożeń,
- rozpoznawanie zagrożeń,
- analiza ryzyka,
- planowanie i przeciwdziałanie ryzyku,
- określenie i projektowanie działań,
- wdrażanie standardów i procedur,
- przeciwdziałanie ryzyku.

Analiza ryzyka przy metodzie spiralnej



Wybór strategii zarządzania ryzykiem w procesie planowania zabezpieczeń

Główne przyczyny awarii systemów



Sposoby zapewnienia dostępności pracy systemu informatycznego oraz ich koszty

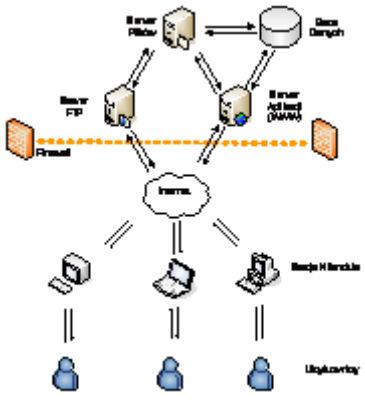
Co oznacza określony poziom niezawodności i dostępności systemu informatycznego

Ilość "dziewiątek"	Procentowa dostępność systemu w roku	Czas trwania awarii w roku	Jednostka	Czas trwania awarii w tygodniu	Jednostka
1	90%	37	Dni	17	Godziny
2	99%	3,65	Dni	1,41	Godziny
3	99,9%	8,45	Godziny	10,5	Minuty
4	99,99%	52,5	Minuty	1	Minuty
5	99,999%	5,25	Minuty	6	Sekundy
6	99,9999%	31,5	Sekundy	0,6	Sekundy

Ze sprawami bezpieczeństwa nie należy przesadzać!

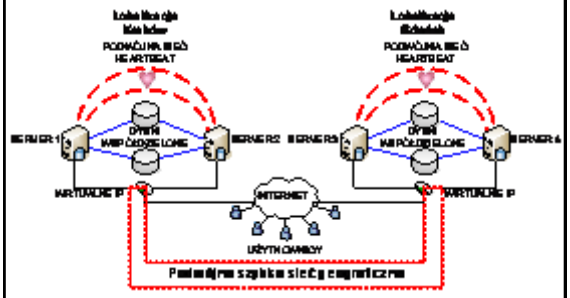
Pożądany poziom zabezpieczeń zależy od profilu instytucji:

Profil instytucji i poziom zabezpieczenia	
Profil instytucji	**Poziom zabezpieczenia systemu informacyjnego**
Uszkodzenie systemu informacyjnego prowadzi do całkowitego załamania instytucji i może mieć poważne konsekwencje polityczne, społeczne lub ekonomiczne.	**maksymalny**
W przypadku uszkodzenia systemu informacyjnego część organizacji nie może funkcjonować. Dłuższe utrzymywanie się tego stanu może mieć poważne konsekwencje dla instytucji lub jej partnerów.	**wysoki**
Konsekwencją poważnego i długotrwałego uszkodzenia systemu informacyjnego może być upadek instytucji.	**średni**
Uszkodzenie systemu informacyjnego może spowodować jedynie niewielkie perturbacje w funkcjonowaniu instytucji.	**niski**

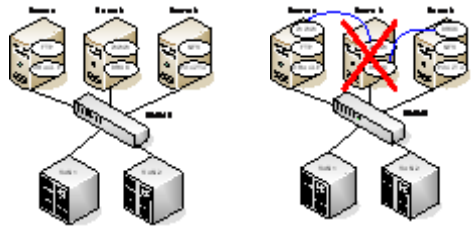


Schemat aplikacji internetowej wraz z elementami jej zabezpieczenia

Przykładowe rozwiązanie systemu o zwiększonej dostępności

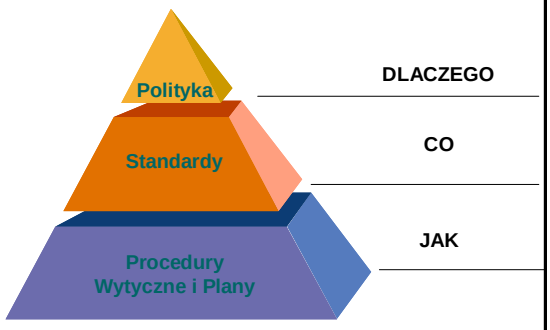


VERITAS Cluster Server przed i po awarii jednego komputera

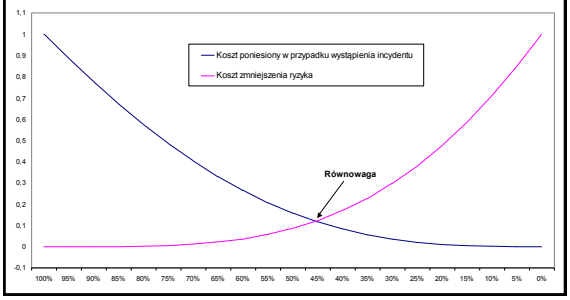


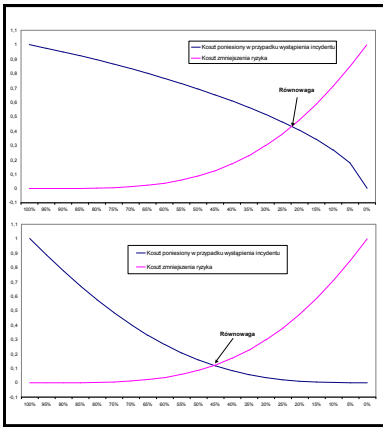
Ważne jest, żeby do właściwych celów używać właściwych narzędzi

Sposoby budowy wysokiego poziomu bezpieczeństwa systemu



Techniki ograniczania ryzyka są kosztowne, więc trzeba ustalić opłacalny poziom zabezpieczeń





Punkt równowagi zależy od stopnia **krytyczności** zabezpieczanego systemu

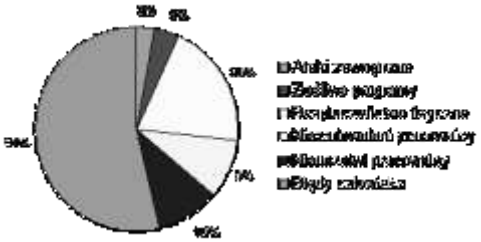
Typy najczęściej spotykanych zagrożeń w sieci komputerowej

- fałszerstwo komputerowe,
- włamanie do systemu, czyli tzw. hacking,
- oszustwo, a w szczególności manipulacja danymi,
- manipulacja programami,
- oszustwa, jakim są manipulacje wynikami,
- sabotaż komputerowy,
- piractwo,
- podsłuch,
- niszczenie danych oraz programów komputerowych

Klasyfikacja ataków na systemy komputerowe:

- atak fizyczny,
- atak przez uniemożliwienie działania,
- atak przez wykorzystanie „tylnego wejścia”,
- atak poprzez błędnie skonfigurowaną usługę,
- atak przez aktywne rozsynchronizowanie tcp

Wpływ poszczególnych czynników na bezpieczeństwo systemów komputerowych:



Na tworzenie warunków bezpieczeństwa *systemów komputerowych* w firmie składają się działania **techniczne** i działania **organizacyjne**

Dla zachowania bezpieczeństwa przetwarzania informacji stosowane są różne techniki:

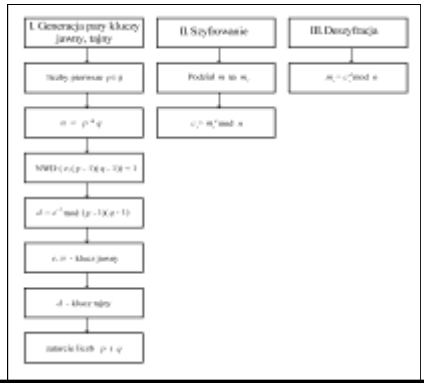
Łatwiejsze do zdefiniowania i do **wyegzekwowania** są z reguły działania techniczne

Najważniejsze z działań technicznych polegają na szyfrowaniu przesyłanych i przechowywanych informacji oraz korzystanie z techniki podpisów elektronicznych

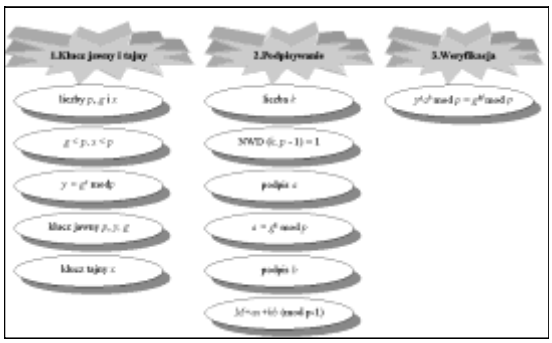
Bezpieczne algorytmy realizacji transakcji w sieciach komputerowych oparte są na kryptografii

Najczęściej stosowanymi ***algorytmami kryptograficznymi z kluczem jawnym,*** *mającymi na celu ochronę danych podczas transmisji internetowych wykorzystywanych w handlu elektronicznym, są algorytmy RSA i ElGamala.*

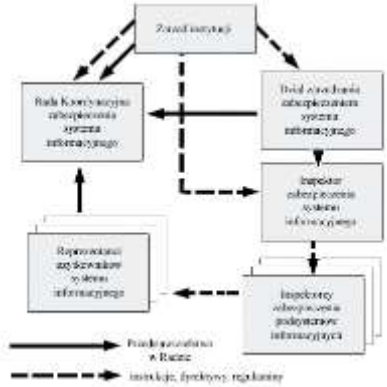
Schemat algorytmu RSA



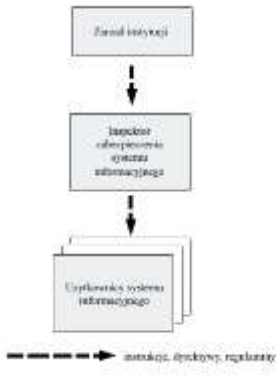
Schemat algorytmu podpisów cyfrowych ElGamala

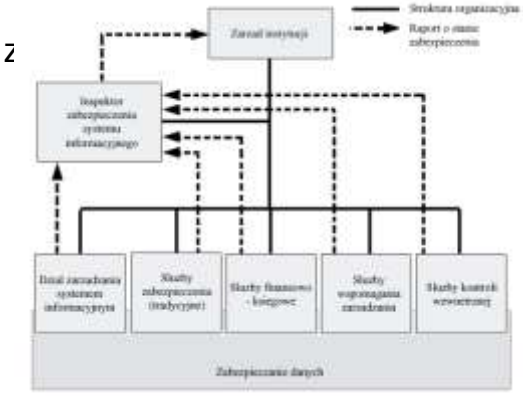


W zakresie działań organizacyjnych trzeba zapewnić bezpieczeństwo informacji poprzez odpowiednią strukturę służb informacyjnych :

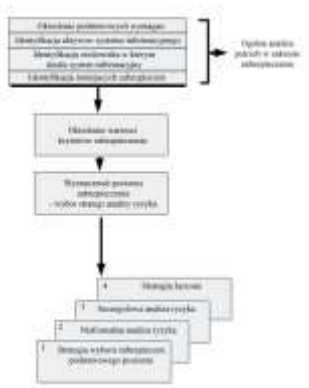


Struktura ta może być uproszczona dla małej firmy, jednak nie może być zredukowana do zera





Bardzo ważna jest w tym kontekście analiza ryzyka



Analiza i projektowanie systemów informacyjnych

Jakość i niezawodność systemu informacyjnego

informatyka stosowana