Wdrożenie systemu informatycznego na uczelni wyższej

Dobre praktyki i doświadczenia

CPI, 28 stycznia 2009

Prowadzący

Janina Mincer-Daszkiewicz

Instytut Informatyki

Uniwersytet Warszawski

jmd@mimuw.edu.pl

Mariusz Czerniak

Uczelniane Centrum Informatyczne

Uniwersytet Mikołaja Kopernika

Mariusz.Czerniak@uni.torun.pl

Uczestnicy

?

Plan dnia

- 10:00 – 12:00

  Zakup systemu i przygotowanie infrastruktury
- Przerwa
- 12:20 – 14:40

  Pierwsze kroki wdrożenia
- Przerwa
- 15:00 – 17:00

  System działa produkcyjnie

Część I
Zakup systemu i przygotowanie infrastruktury

1. Wybór systemu

Projektowanie zakupu systemu informatycznego

(źródło: P.Kowalski, http://www.computerworld.pl/)

1. Powołanie zespołu specjalistów i wyznaczenie głównego koordynatora prac
2. Opracowanie harmonogramu prac z określeniem terminów realizacji poszczególnych etapów
3. Sformułowanie wymagań wobec systemu
4. Penetracja rynku
5. Kontakty z oferentami
6. Wstępna selekcja

Projektowanie zakupu systemu informatycznego (2)

7. Sporządzenie oficjalnego zapytania ofertowego
8. Analiza własnego zaplecza informatycznego (sprzęt, oprogramowanie)
9. Analiza nadesłanych ofert
10. Szczegółowe konsultacje z oferentami
11. Organizacja pokazów
12. Próba wyboru najlepszego systemu

Projektowanie zakupu systemu informatycznego (3)

13. Ocena realiów finansowych
14. Negocjacje finansowe z zaakceptowanymi oferentami
15. Synteza (sporządzenie dokumentu końcowego)
16. Wybór docelowego systemu (decydenci)
17. Opracowanie wstępnego projektu instalacji

O czym należy pamiętać

- Strategia licencjonowania systemu
- Wymagania sprzętowe i systemowe (systemy operacyjne na serwer i stacje klienckie, bazy danych, inne)
- Koszty ukryte (np. administrowanie, rozwój)
- Możliwość konwersji danych ze starego systemu
- Wsparcie na etapie wdrożenia
- Aktualizacje, konserwacja, rozwój systemu
- Własność kodu źródłowego

Sformułowanie wymagań wobec systemu

- Opis za pomocą zbioru funkcjonalności
  - zebranie wymagań w formie tekstu
  - opis wymagań np. w formie przypadków użycia
- Opis funkcjonalności za pomocą procesów, jakie system ma obsłużyć
  - mega procesy (np. badania naukowe, tok studiów, gospodarka własna)
  - procesy (np. obsługa spraw pracowniczych, obsługa finansowa, wnioskowanie o dotacje, ...)
  - podprocesy (np. przyjmowanie do pracy, rozliczanie umów cywilno-prawnych, planowanie urlopów, ...)
  - działania

Sformułowanie wymagań wobec systemu (2)

- Zaletą opisu procesowego jest precyzyjne i kompletne (na wielu poziomach) określenie w jaki sposób wskazany proces ma być wspierany przez system informatyczny
- Wadą zapisu procesowego jest konieczność posiadania wewnątrz organizacji zidentyfikowanych procesów
- Wdrożenie systemu informatycznego to dobra okazja do zinwentaryzowania i uporządkowania procesów
- Warto na samym początku wskazać właścicieli procesów, czyli osoby odpowiedzialne za ich realizację, będące formalnymi zwierzchnikami osób uczestniczących w ich realizacji

2. Przygotowanie infrastruktury

Sprzęt i oprogramowanie

- Wybór platformy sprzętowej
  - co optymalizować (procesory, pamięć, dyski)
- Wybór oprogramowania
  - systemy operacyjne dla serwerów
  - systemy operacyjne dla stanowisk klienckich
  - centralna baza danych
  - aplikacje webowe
  - usługi katalogowe
  - narzędzia integracyjne
  - narzędzia analityczne
  - narzędzia dla administratorów

Inne elementy infrastruktury

- Sieć, przepustowość łączy
- Sprzęt i oprogramowanie do tworzenia kopii zapasowych
- Koszty sprzętu i oprogramowania a koszty administrowania (systemem, aplikacją)
- System informowania o awariach
- Zapory ogniowe, szyfrowanie łącza, VPN, stunnel
- Kioski multimedialne czy stare PC-ty z dostępem do sieci przez przeglądarkę

O czym należy pamiętać

- Cel: zapewnienie ciągłości pracy przy zachowaniu budżetu i spełnieniu założeń biznesowych
- W dużym systemie informatycznym nie należy oszczędzać na oprogramowaniu bazodanowym
- Administratorzy potrzebują narzędzi do administrowania, monitorowania i powiadamiania o awariach
- Łatwiej i taniej zdobyć sprzęt niż sprawnych administratorów (a jeszcze trudniej ich utrzymać)
- Skalowalność, pojedyncze punkty awarii
- Umowy serwisowe
- A może outsourcing?

3. Stan prawny

Wpływ na system informatyczny

- Prawo krajowe
  - ustawy
  - rozporządzenia ministerialne
- Prawo uczelniane
  - uchwały Senatu
  - regulaminy (studiów, pomocy materialnej itp.)
  - zarządzenia Rektora
  - uchwały Rad Wydziałów
  - „prawo zwyczajowe”

Prawo o szkolnictwie wyższym

- Ustawa z dnia 27 lipca 2005 r. Prawo o szkolnictwie wyższym (Dz. U. 2005 Nr 164 poz. 1365 z późn. zm.) – określa ustrój szkolnictwa wyższego w Polsce
- Struktura organizacyjna uczelni
- Mienie i finanse
  - Ustawa z dnia 30 czerwca 2005 r. o finansach publicznych (Dz. U. 2005 Nr 249 poz. 2104 z późn. zm.) – uczelnia jest podmiotem finansów publicznych
  - Ustawa z dnia 29 września 1994 r. o rachunkowości (Dz. U. 2002 r. Nr 76 poz. 694 z późn. zm.).
    - Zasady i sposoby prowadzenia ksiąg rachunkowych
    - Metody ustalenia wyniku finansowego
    - Zasady rozliczania kosztów i przychodów

Prawo o szkolnictwie wyższym (2)

- Formy i stanowiska zatrudnienia, wynagrodzenia, pensum pracownika, urlopy, odpowiedzialność dyscyplinarna
- Organizacja studiów
  - tryb, poziom i czas trwania studiów
  - dokumenty uprawniające do podjęcia studiów
  - przebieg postępowania rekrutacyjnego
- Udzielanie pomocy materialnej studentom i doktorantom
  - rodzaj pomocy (typy stypendiów)
  - kryteria przyznawania
- Pobieranie opłat za usługi edukacyjne

Dokumentacja przebiegu studiów

- Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 2 listopada 2006 r. w sprawie dokumentacji przebiegu studiów (Dz. U. Nr 224, poz. 1634)
- Zawartość teczki akt osobowych studenta, m.in.
  - decyzje władz uczelni dotyczące przebiegu studiów (np. udzielone urlopy, zgody na powtarzanie roku, skreślenia z listy studentów, nagrody, wyróżnienia i kary dyscyplinarne)
  - dokumenty dotyczące przyznania pomocy materialnej
  - egzemplarz pracy dyplomowej i recenzja (recenzje), jeżeli regulamin studiów przewiduje ich napisanie
  - protokół egzaminu dyplomowego

Dokumentacja przebiegu studiów (2)

- Elektroniczna legitymacja studencka
  - wzór i specyfikacja techniczna
  - przeznaczenie i przedłużanie ważności
  - wydawanie duplikatów
- Rejestry dokumentów (mogą być prowadzone elektronicznie)
  - Wydane indeksy i legitymacje
  - Album studentów
  - Księga dyplomów
- Szczegóły dokumentów opisujących przebieg studiów
  - protokoły zaliczenia przedmiotu
  - karty okresowych osiągnięć studenta

Rodzaje i wzory dyplomów

- Rozporządzenie Ministra Nauki i Szkolnictwa Wyższego z dnia 19 grudnia 2008 w sprawie rodzajów tytułów zawodowych i wzorów dyplomów oraz świadectw wydawanych przez uczelnie (Dz. U. 2009 Nr 11 poz. 61)
- Tytuły zawodowe nadawane absolwentom
- Warunki wydawania i wzory
  - dyplomów i suplementów do dyplomów (np. wielostronicowy oryginał dyplomu – miejsca na legalizację i apostille)
  - świadectw ukończenia studiów doktoranckich, podyplomowych i kursów dokształcających

Ochrona danych osobowych

28 stycznia – dniem ochrony danych osobowych (GIODO)

- Ustawa z dnia 29 sierpnia 1997 r. o ochronie danych osobowych (tekst jednolity: Dz. U. Nr 101 z 2002 r., poz. 926, z późn. zm.) – UODO
- Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych (Dz. U. Nr 100, poz. 1024)
  - dane osobowe – wszelkie informacje dotyczące zidentyfikowanej lub możliwej do zidentyfikowania osoby fizycznej
  - przetwarzanie danych – jakiekolwiek operacje wykonywane na danych osobowych, takie jak zbieranie, utrwalanie, przechowywanie, opracowywanie, zmienianie, udostępnianie i usuwanie
  - zabezpieczenie danych w systemie informatycznym – wdrożenie i eksploatacja stosownych środków technicznych i organizacyjnych zapewniających ochronę danych przed ich nieuprawnionym przetwarzaniem

Ochrona danych osobowych – zasady przetwarzania na uczelni

- Rektor uczelni jest Administratorem danych
- Przetwarzanie danych w uczelni wynika z realizacji zadań zawartych w Prawie o szkolnictwie wyższym
  - nie jest wymagana zgoda osoby na przetwarzanie
  - nie ma konieczności rejestrowania zbioru danych w GIODO (nie dotyczy to systemu rekrutacyjnego)
  - postępowanie rekrutacyjne jest jawne (nie oznacza to braku ochrony danych osobowych!)
  - przetwarzanie danych wrażliwych (stan zdrowia) na wniosek osoby – np. stypendium dla osób niepełnosprawnych
    (nie jest przetwarzaniem danych wrażliwych informacja, że kandydat potrzebuje pomocy podczas procesu rekrutacyjnego ze względu na niepełnosprawność)
- Osoba dopuszczona do przetwarzania danych musi uzyskać upoważnienie do ich przetwarzania

Ochrona danych osobowych – zasady przetwarzania na uczelni (2)

Zarządzenie Rektora UMK nr 58/2004, załącznik nr 1: Wzór udzielenia upoważnienia

Uniwersytet Mikołaja Kopernika w Toruniu

L. dz. [skrótjednostki]/1218/[numer]-U/[rok] Toruń, dnia [\DataWystawienia] r.

UDZIELENIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Pan [\ImieJed] [\ImieDwa] [\Nazwisko], nr PESEL: [\PESEL], zatrudniony w: [\JednostkaOrganizacyjna], jest upoważniony do przetwarzania danych osobowych w systemie: **Uniwersytecki System Obsługi Studiów – USOS**, w roli: [\Rola].

Upoważnienie jest ważne od dnia [\OdDnia] r. do dnia [\DoDnia] r.

(podpis)

([\Upoważniający])

Toruń, dnia [\DataZłożeniaOświadczenia] r.

OŚWIADCZENIE UPOWAŻNIONEGO

Oświadczam, że są mi znane obowiązki i odpowiedzialność wynikające z udzielonego mi jak wyżej upoważnienia.

(podpis)

([\ImieJed] [\ImieDwa] [\Nazwisko])

Otrzymują:

1. aa.
2. [\ImieJed] [\ImieDwa] [\Nazwisko]
3. Administrator Bezpieczeństwa Informacji
4. Dział Spraw Pracowniczych
5. administrator systemu: Uniwersytecki System Obsługi Studiów – USOS

Zarządzenie Rektora UMK nr 58/2004, załącznik nr 2: Wzór odwołania upoważnienia

Uniwersytet Mikołaja Kopernika w Toruniu

L. dz. [skrótjednostki]/1218/[numer]-O/[rok] Toruń, dnia [\DataWystawienia] r.

ODWOŁANIE UPOWAŻNIENIA DO PRZETWARZANIA DANYCH OSOBOWYCH

Z dniem [\DataOdwołania] r. ustaje udzielone Panu [\ImieJed] [\ImieDwa] [\Nazwisko], nr PESEL: [\PESEL], zatrudnionemu w [\JednostkaOrganizacyjna], upoważnienie nr [skrótjednostki]/1218/[numer]-U/[rok] do przetwarzania danych osobowych w systemie **Uniwersytecki System Obsługi Studiów – USOS**, w roli: [\Rola].

(podpis)

([\Upoważniający])

Otrzymują:

1. aa.
2. [\ImieJed] [\ImieDwa] [\Nazwisko]
3. Administrator Bezpieczeństwa Informacji
4. Dział Spraw Pracowniczych
5. administrator systemu: Uniwersytecki System Obsługi Studiów – USOS

Ochrona danych osobowych – zasady przetwarzania na uczelni (3)

- Nadzór nad bezpieczeństwem przetwarzania danych w systemach informatycznych uczelni może zostać powierzony Administratorowi Bezpieczeństwa Informacji (ABI)
- Główne zadania ABI
  - przygotowanie i uaktualnianie polityki bezpieczeństwa
  - przygotowanie i uaktualnianie instrukcji dla systemów informatycznych, w których przetwarza się dane osobowe,
  - prowadzenie ewidencji osób upoważnionych do przetwarzania danych osobowych w systemach informatycznych, która zawiera
    - imię i nazwisko osoby upoważnionej
    - datę nadania i ustania oraz zakres upoważnienia
    - identyfikator
  - wydawanie odpowiednich zaleceń w przypadkach stwierdzeniu nieakceptowalnego ryzyka związanego z przetwarzaniem danych osobowych i niezwłoczne powiadamianie o tych sytuacjach

Ochrona danych osobowych – zasady przetwarzania na uczelni (4)

- Obowiązki wynikające z UODO mogą zostać powierzone osobom, zwanym lokalnymi administratorami danych osobowych
  - dziekanom – w zakresie dotyczącym pracowników i studentów wydziałów
  - dyrektorom/kierownikom jednostek ogólnouczelnianych i międzywydziałowych – w zakresie podległych im pracowników
  - dyrektorowi administracyjnemu – w zakresie podległych mu jednostek
- Lokalni administratorzy danych osobowych zobowiązani są do przestrzegania przepisów UODO, w szczególności przez
  - udzielanie i odwoływanie upoważnień do przetwarzania danych osobowych i uzyskiwanie od nich oświadczeń
  - wdrażanie i nadzorowanie przestrzegania instrukcji zarządzania systemami informatycznymi służącymi do przetwarzania danych osobowych
  - stwarzanie w podległych im jednostkach warunków organizacyjnych i technicznych umożliwiających spełnianie wymogów wynikających z UODO

Ochrona danych osobowych – zasady przetwarzania na uczelni (5)

- Osoby upoważnione do przetwarzania danych są zobowiązane zachować w tajemnicy te dane oraz sposoby ich zabezpieczeń
- Nie można udostępniać przechowywanych w systemie danych osobowych, w szczególności danych wrażliwych osobom nieupoważnionym
  - umożliwienie dostępu do danych osobowych osobom nieupoważnionym jest karalne
- Przez udostępnianie danych należy rozumieć
  - przekazywanie ustne
  - za pośrednictwem poczty elektronicznej
  - na jakichkolwiek nośnikach elektronicznych bądź w postaci dokumentów drukowanych
- Członkowie rodzin studentów nie są upoważnieni do otrzymywania informacji z systemu
- Udostępnianie danych innym podmiotom odbywa się tylko za zgodą Rektora

Przetwarzanie danych osobowych w systemach informatycznych uczelni

- System powinien zapewniać automatyczne odnotowanie:
  - daty pierwszego wprowadzenia danych do systemu
  - identyfikatora użytkownika wprowadzającego dane osobowe do systemu
    - (nie dotyczy) Źródła danych, w przypadku zbierania danych, nie od osoby, której one dotyczą
    - (nie dotyczy, jeśli dane nie przetwarza inny podmiot) Informacji o odbiorcach, w rozumieniu art. 7 pkt 6 ustawy, którym dane osobowe zostały udostępnione, dacie i zakresie tego udostępnienia, chyba że system informatyczny używany jest do przetwarzania danych zawartych w zbiorach jawnych;
    - (nie dotyczy, jeśli nie przetwarzamy danych w celach marketingowych) sprzeciwu, o którym mowa w art. 32 ust. 1 pkt 8 ustawy.

4. Bezpieczeństwo systemu i danych

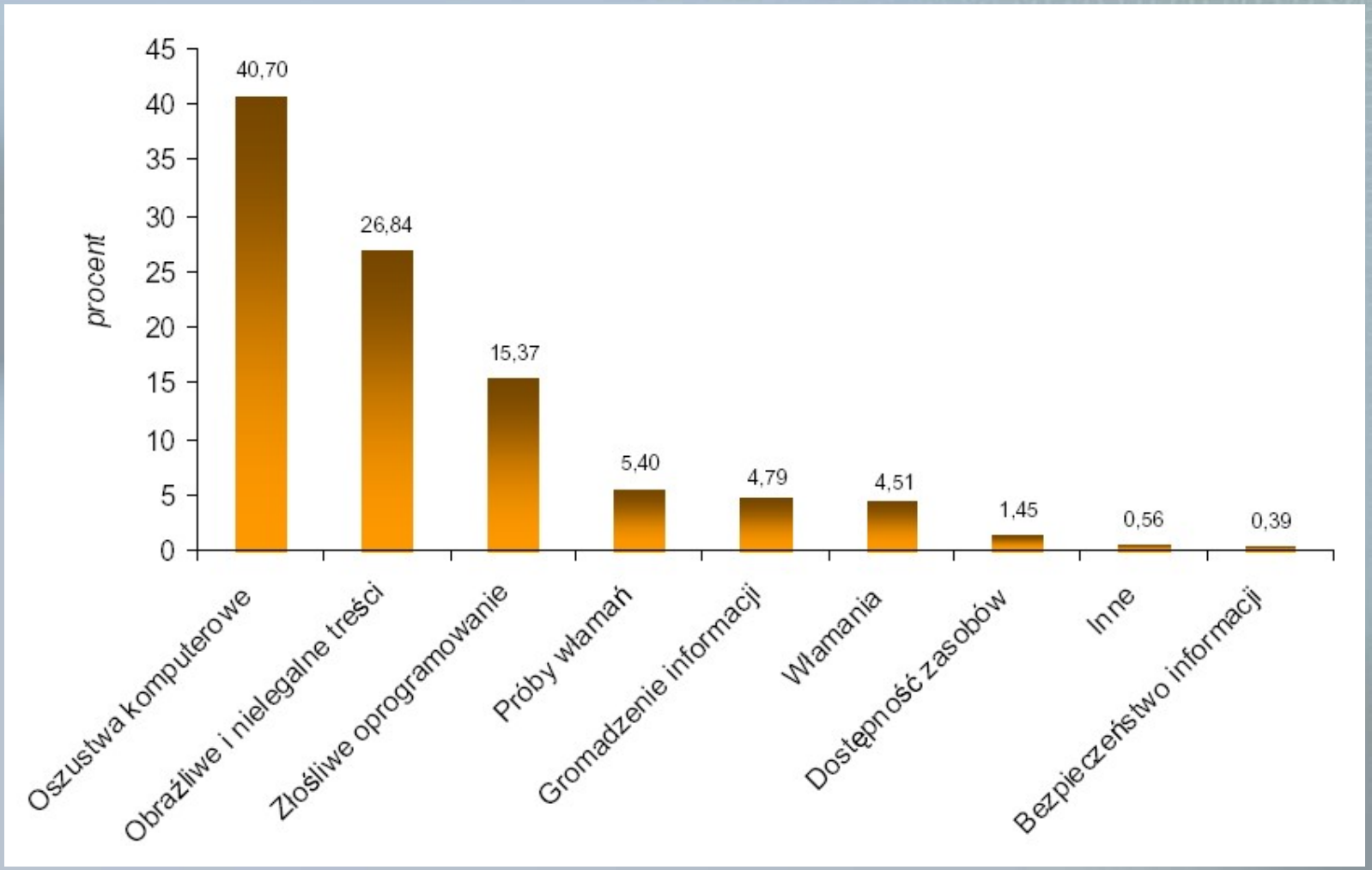
Stan bezpieczeństwa

- System zabezpieczeń jest tak silny, jak jego najsłabsze ogniwo
- Większość incydentów związanych z bezpieczeństwem informacji ma swoje źródło wewnątrz organizacji
- Badania firmy doradczej Ernst & Young (Global Information Security Survey, 2008)
  - 85% managerów wyższego szczebla docenia wpływ incydentów bezpieczeństwa na markę i renomę firmy
  - następuje poprawa bezpieczeństwa dzięki realizacji wymogów regulacyjnych (70% organizacji dysponuje procedurami obsługi naruszeń bezpieczeństwa)

Identyfikacja zagrożeń

- Zagrożenia pasywne (nie są skutkiem celowego działania)
  - naturalne katastrofy
  - zawodność sprzętu (awarie)
  - zawodność infrastruktury (telekomunikacyjnej, energetycznej, informatycznej)
- Zagrożenia aktywne (np. wynikające z działań nieuprawnionego użytkownika)
  - błąd ludzki (niedbalstwo, nieprawidłowe stosowanie mechanizmów bezpieczeństwa)
  - działania złośliwe (włamania do systemów, złośliwe oprogramowanie – sniffer, spoofing, koń trojański, wirus)
  - inżynieria społeczna, której skutkiem może być kradzież informacji

Główne typy incydentów zgłoszonych w 2008 r.



Źródło: CERT Polska (Computer Emergency Response Team)

Rozpoznanie incydentu zagrażającego bezpieczeństwu

- Modyfikacje w ustawieniach systemu
  - zmiany w rejestrach lub plikach konfiguracyjnych
  - obecność złośliwego oprogramowania lub nieznanych programów w katalogach systemowych
  - uruchomienie nieznanych procesów
  - wzrost zużycia zasobów czy załamanie systemu
- Aktywność użytkowników
  - nietypowe (zaskakujące) pory aktywności
  - obecność nieznanych kont użytkowników
  - użycie uśpionego konta
- Powiadomienia dokonane przez
  - pracowników o nietypowym zachowaniu systemu czy ataku
  - system wykrywania wtargnięć (monitoring)
  - partnerów, hakerów, MEDIA

Podatność systemu informatycznego na zagrożenia

- Zawodność oprogramowania – dysfunkcja programu
  - nieautoryzowane źródła oprogramowania
  - wady oprogramowania niskopoziomowego (związanego ze sprzętem)
  - złożoność oprogramowania – wady projektowe programu (asymetria polityki bezpieczeństwa i zabezpieczeń)
  - ewolucja oprogramowania – stosowanie przestarzałego środowiska programowania
  - testowanie oprogramowania
  - zarządzanie zmianami
- Niepoprawne wdrożenia
  - domyślna instalacja, łatwiejsze zarządzanie i administracja systemem
  - błędy konfiguracyjne (prymat funkcjonalności systemu)
- Nadużycia w wykorzystaniu oprogramowania – „innowacyjność” (zastosowanie niezgodne z przeznaczeniem)
- Wykrycie podatności następuje zwykle w wyniku analizy incydentu dokonywanej po ataku

Środki bezpieczeństwa stosowane w systemie informatycznym

- Każdy użytkownik posiada niepowtarzalny identyfikator
- Identyfikator użytkownika, który utracił uprawnienia do przetwarzania danych, nie może być przydzielony innej osobie
- Dostęp do danych jest możliwy wyłącznie
  - po wprowadzeniu identyfikatora i dokonaniu uwierzytelnienia
    - dotyczy osób, ale również procesów, programów
    - służy uzyskaniu jednoznacznego potwierdzenia, że podmiot jest tym za kogo się podaje
  - otrzymaniu autoryzacji na podstawie systemu ról i uprawnień
- Hasło składa się z co najmniej 8 znaków, zawiera małe i wielkie litery oraz cyfry lub znaki specjalne, a jego zmiana następuje nie rzadziej niż co 30 dni

Środki bezpieczeństwa stosowane w systemie informatycznym (2)

- Urządzenia, dyski lub inne elektroniczne nośniki informacji, zawierające dane osobowe, przeznaczone do
  - likwidacji – pozbawia się wcześniej zapisu tych danych, a w przypadku gdy nie jest to możliwe, uszkadza się w sposób uniemożliwiający ich odczytanie
  - przekazania podmiotowi nieuprawnionemu do przetwarzania danych – pozbawia się wcześniej zapisu tych danych, w sposób uniemożliwiający ich odzyskanie
  - naprawy – pozbawia się wcześniej zapisu tych danych w sposób uniemożliwiający ich odzyskanie albo naprawia się je pod nadzorem osoby upoważnionej przez administratora danych

Środki bezpieczeństwa stosowane w systemie informatycznym (3)

- Dane osobowe przetwarzane w systemie informatycznym zabezpiecza się przez wykonywanie kopii zapasowych zbiorów danych oraz programów służących do przetwarzania danych
- Kopie zapasowe
  - przechowuje się w miejscach zabezpieczających je przed nieuprawnionym przejęciem, modyfikacją, uszkodzeniem lub zniszczeniem
  - usuwa się niezwłocznie po ustaniu ich użyteczności
- Stosuje się
  - monitorowanie i rejestrowanie działań (dziennik zmian)
  - środki kryptograficznej ochrony wobec danych wykorzystywanych do uwierzytelnienia, które są przesyłane w sieci publicznej
  - ochronę antywirusową

Inne sposoby zwiększenia poziomu bezpieczeństwa

- Audyt – analiza zapisów działań użytkowników pozwalająca na wykrycie działań nieuprawnionych
- Przymus stosowania zasad bezpieczeństwa
  - precyzyjnie określony i przejrzysty
  - wdrożony w całej jednostce
  - uświadomienie bezpieczeństwa
    - uprawnienia
    - zakres odpowiedzialności
    - system kar i nagród

Część II
Pierwsze kroki wdrożenia

5. Zespół wdrażający

Pułapki wdrożenia

- Złożoność struktury uczelni, autonomia jej jednostek oraz ugruntowana tradycja ewolucyjnych zmian są czynnikami utrudniającymi wdrożenie
- Brak kontynuacji ze strony kolejnych władz
- Od początku musi istnieć zespół posiadający odpowiednie umocowanie, ze ściśle określonymi zadaniami, harmonogramem i budżetem, rozliczany z kolejnych etapów

Zespół wdrożeniowy

- Kierownik Zespołu – przedstawiciel Zamawiającego
- Konsultanci Wykonawcy (w tym jeden wiodący) – o ile dostawca oprogramowania uczestniczy we wdrożeniu
- Użytkownicy kluczowi ze strony Zamawiającego (właściciele kluczowych procesów)
- Przedstawiciele działu informatyki Zamawiającego

Wsparcie ze strony władz uczelni

- Powołanie prorektora ds. informatyzacji, którego jednym z obowiązków będzie wdrożenie systemu
- Powołanie pełnomocnika rektora, prodziekana czy wydziałowego koordynatora w zakresie wdrożenia systemu
- Ustanowienie w pionie administracji centralnej uczelni osoby dysponującej dużymi uprawnieniami odpowiedzialnej za wdrożenie

Kompetencje zespołu

- Uprawnienia do podejmowania decyzji o rozpoczęciu, zakończeniu poszczególnych etapów prac czy innych kluczowych rozstrzygnięć
- Wiedza merytoryczna w zakresie:
  - wdrażanego systemu
  - przebiegu procesów w uczelni
  - obsługi finansowej usług edukacyjnych
  - uwarunkowań prawnych
- Możliwości komunikacji i mediacji między zespołem wdrażającym a użytkownikami wdrażanego systemu

Budżet zespołu

- Należy zabezpieczyć środki na:
  - udział w szkoleniach dotyczących wdrażanych rozwiązań i technologii informatycznych
  - udział w warsztatach, panelach, seminariach związanych z procesami zarządzania uczelnią
  - udostępnienie literatury fachowej oraz zakup specjalistycznego oprogramowania wspomagającego administrowanie systemem
  - premiowanie dodatkowego nakładu pracy oraz zwiększonej dyspozycyjności
- Być może należy na czas wdrożenia zwolnić członków zespołu z innych obowiązków na uczelni
- Środki finansowe będą dodatkowym argumentem dla tej grupy wykwalifikowanych i doświadczonych osób na skuteczną ochronę przez zmianą pracodawcy

Ogólny plan wdrożenia

- Plan wdrożenia jest pochodną założonego modelu wdrożenia:
  - funkcjonalny – uszeregowanie modułów funkcjonalnych wg. priorytetów, wdrażanie modułu we wszystkich jednostkach równocześnie
  - jednostkowy – wdrożenie pełnej funkcjonalności w wybranej jednostce, a następnie w kolejnych
  - przyrostowy – objęcie obsługą funkcjonalną lub jednostkową wszystkich studentów realizujących pewien etap studiów, a z upływem czasu przyrostowo kolejne etapy studiów

Ogólny plan wdrożenia

- W ramach przygotowywania harmonogramu należy podzielić proces wdrażania na etapy, a w nich określić:
  - działania, które muszą zostać podjęte
  - wykonawców działań
  - szacowany czas wykonania
  - warunki pozytywnego zakończenia etapu

Zapewnienie spójności działań

- Spójność działań dotyczy:
  - wyboru metody wdrożenia
  - ustalenia właściwej kolejności wdrażania modułów lub wyboru jednostek uczelni
  - przygotowania harmonogramu prac i wykonawców działań
  - terminowości podjętych działań
  - jakości przeprowadzenia szkoleń przyszłych użytkowników
- Częste zmiany w którymkolwiek zakresie powodują wzrost niechęci do nowego systemu

6. Kody, słowniki

Wspólny system kodowania

- Ustalenie wspólnego systemu kodowania powinno poprzedzić wszystkie inne prace związane z wprowadzaniem danych do systemu
- Opracowanie systemu kodowania jest czynnością jednorazową, ale należy zapewnić ciągłość jego stosowania
- Powinna być dziełem osób z dużym doświadczeniem (prorektor, prodziekan, ...)

Cel jednolitego systemu kodowania

- Jednoznaczne odzwierciedlenie struktury organizacyjnej uczelni
- Możliwość łatwej wymiany danych między wieloma systemami funkcjonującymi w uczelni
- Powiązanie oferty dydaktycznej z jednostkami uczelni, które ją realizują
- Przypisanie studentów, pracowników oraz innych osób do jednostek uczelni
- Kontrolę dostępu do danych wg kryteriów przypisania do jednostek
- Problem: zmiana struktury organizacyjnej w czasie (co drugi senat; archiwum UW – dane od 1915 roku)

Przykłady

- UW

  Zarządzenie Rektora UW w sprawie wprowadzenia zasad kodowania struktury organizacyjnej

  Projekt kodów przedmiotów dla Wydziału Matematyki, Informatyki i Mechaniki UW

- UMK

  Zarządzenie Rektora UMK w sprawie kodowania rodzajów i systemów studiów oraz struktury organizacyjnej

  (numeracja w systemie kodowania programów studiów została dodatkowo wykorzystana do generowania indywidualnych numerów kont bankowych dla wpłat za usługi edukacyjne)

Słowniki

- Rodzaje słowników
- Kto ma uprawnienia do wypełniania i aktualizacji
- Jak wypełnić – ręcznie, automatycznie, import z innych baz
- Jak aktualizować – ręcznie, automatycznie (skrypty od dostawcy)
- Czy dane słownikowe mają naturalne kody (kody pocztowe a słownik szkół średnich)
- Zmiany w danych słownikowych mają zawsze duży wpływ na funkcjonowanie systemu (por. kody pocztowe a kontrola danych adresowych)

Słowniki ogólnopolskie

- Banki krajowe i zagraniczne
- Urzędy skarbowe
- WKU
- Kody i urzędy pocztowe
- Szkoły średnie
- Uczelnie wyższe (krajowe i zagraniczne)
- Waluty
- Obywatelstwa, języki
- Kody Erasmus

Słowniki lokalne

- Organizacyjne (jednostki uczelni, kampusy, budynki, sale)
- Pracownicze (formy zatrudnienia, stanowiska, pełnione funkcje, tytuły, urlopy, zniżki pensum)
- Socjalne (rodzaje stypendiów, algorytmy obliczające kwoty, potrącenia)
- Dydaktyczne (stosowane skale ocen, typy protokołów, rodzaje: zajęć, praktyk, punktów, cykle dydaktyczne i kalendarz akademicki, terminy zajęć, kierunki i specjalności, programy studiów oraz ich etapy)
- Finansowe (źródła wpłat, rodzaje należności, stawki odsetek, subkonta jednostek, kody kasowe, cenniki opłat)

7. Import i konwersja danych ze starych baz

Problem starych baz

- Często zawierają wiele danych kluczowych z punktu widzenia ciągłości funkcjonowania uczelni
- Często dane te nie mają unikatowych kluczy i ich uporządkowanie może wymagać dużo pracy
- Potencjalne problemy:
  - brak PESEL-i w danych osobowych
  - brak strukturalizacji adresu
  - brak słowników lub duże zmiany w ich zawartości
  - brak specjalistów znających strukturę starej bazy
  - brak narzędzi do eksportu danych ze starej bazy w postaci nadającej się do importu do nowej

Zadania zespołu wdrażającego

- Przeprowadzenie analizy źródeł danych, z których będzie możliwe pozyskanie danych w formie elektronicznej
- przygotowanie wymagań związanych z importem i konwersją danych, a także harmonogramu prac do wykonania w tym zakresie
- opracowanie formularzy do pozyskania i weryfikacji danych lub przygotowanie skryptów/procedur do ich importu

8. Instalacja testowa i kontrola gotowości systemu do wdrożenia produkcyjnego

Instalacja testowa

- Przed wdrożeniem produkcyjnym systemu informatycznego zalecana jest przygotowanie instalacji testowej, która może pełnić następujące funkcje
  - kontrolne – sprawdzenie pracy systemu
  - szkoleniowe dla przyszłych użytkowników
- Instalacja testowa może zawierać
  - wypełnione słowniki umożliwiające wprowadzanie ‘bieżących’ danych
  - wypełnione danymi tabele, parametry itp. niezbędne do modelowania obsługi procesów, których system będzie dotyczył
  - zanonimizowane (zaszumione) dane osobowe pełniące funkcję ‘wypełniacza’

Instalacja testowa (2)

- Funkcje kontrolne
  - sprawdzenie czy system posiada funkcjonalności zgodne z dokumentacją lub szczegółami kontraktu/umowy (testy funkcjonalne)
  - przeprowadzenie analizy wydajnościowej i obciążeniowej
    - dla założonych w specyfikacji obciążeniach są spełnione wymogi wydajnościowe
    - dla zwiększanych obciążeń sprawdzana jest efektywność
    - testy w różnych etapach życia systemu: wdrożenie i eksploatacja
  - kontrola stosowanych zabezpieczeń
    - zgodność z przepisami prawa w zakresie bezpieczeństwa, politykami bezpieczeństwa
    - zabezpieczenie przed skutkami awarii systemu (testy procedur składowania i odzyskiwania danych)
- Funkcje szkoleniowe
  - symulacja funkcjonalności systemu
  - przełamanie oporu i obaw związanych z użytkowaniem nowego systemu i utratą danych na skutek błędnie wykonanych czynności

Kontrola gotowości systemu do wdrożenia produkcyjnego

- Scenariusz wykonywanych testów
  - podział na testy cząstkowe
  - przygotowanie raportów wynikowych
- Klasyfikacja błędów wykrytych w testach
  - krytyczne – są to błędy, które uniemożliwiają funkcjonowanie systemu oraz blokujące pracę użytkowników
  - ważne – to błędy co prawda umożliwiające zakończenie procesu testowania danego scenariusza, ale będące błędami znaczącymi, np. błędy logiczne lub takie, które mają duży wpływ na poprawne działanie systemu
  - drobne – wszystkie błędy nie będące błędami krytycznymi i ważnymi – błędy które nie mają wpływu na funkcjonowanie systemu

Kontrola gotowości systemu do wdrożenia produkcyjnego (2)

- Kryteria uniemożliwiające przejście do wdrożenia produkcyjnego systemu:
  - występowanie błędów 'krytycznych' do czasu zakończenia testów poprawności działania
  - występowanie błędów 'ważnych' do czasu zakończenia cząstkowych testów poprawności działania, w określonej liczbie dla danego scenariusza testowego
- Finalne testy akceptacyjne realizowane w ramach końcowego przeglądu jakości nie dopuszczają występowania błędów ważnych i krytycznych – dopiero gdy ich nie ma można przystąpić do instalacji produkcyjnej ☺

Część III
System działa produkcyjnie

9. Uprawnienia użytkowników

System uprawnień

- Realizacja ustawy o ochronie danych osobowych
  - Autoryzacja dostępu do danych
  - Ochrona przed niepowołanym dostępem do danych i ich użyciem
- Uprawnienia
  - systemowe – zezwalają użytkownikowi na wykonanie w bazie operacji określonego typu np.
    - create table, drop any view, execute any procedure, create session
  - obiektowe – zezwalają użytkownikowi na wykonanie określonych operacji na konkretnym obiekcie bazy danych
    - tabela, perspektywa, sekwencja, pakiet
  - zalecane zasady stosowania:
    - minimalizacja przywilejów
    - granulacja uprawnień

Typy nadawanych uprawnień

- SELECT – pozwala na czytanie danych z tabeli lub perspektywy oraz na pobieranie wartości z sekwencji
- INSERT – pozwala na wstawianie rekordów do tabeli lub perspektywy; uprawnienie to można określić dla poszczególnych kolumn tabeli lub perspektywy
- UPDATE – pozwala na modyfikowanie rekordów w tabeli lub perspektywie; uprawnienie to można określić dla poszczególnych kolumn tabeli lub perspektywy
- DELETE – pozwala na usuwanie rekordów z tabeli lub perspektywy,
- EXECUTE – pozwala na wykonywanie pakietów
- ALTER – pozwala na wydawanie poleceń ALTER dla tabeli, perspektywy, sekwencji

System ról

- Uprawnienia mogą być kontrolowane przy pomocy ról, które stanowią nazwane zbiory uprawnień
- Role upraszczają zarządzanie uprawnieniami dla dużych zbiorów użytkowników o podobnej charakterystyce (np. pracownicy działu kadr, dziekanatu)
- System ról może przewidywać wykorzystanie parametrów, który zmniejsza liczbę ról i ogranicza koszty administrowania systemem
- Zmieniając uprawnienia należące do roli, zmienia się uprawnienia wszystkich użytkowników do niej przypisanych

Przykłady metatypów ról w systemie obsługującym tok studiów

- Modyfikacja Danych Osobowych (MDO)
  - wprowadzanie, zmiana danych osobowych studentów, doktorantów, słuchaczy studiów podyplomowych, pracowników
  - prowadzenie toku studiów
  - rozliczanie z osiągnięć przedmiotowych i łączenie ich (podpinanie) z realizowanym programem studiów
  - obsługa podań studenckich i decyzji na temat wymagań programowych
  - przedłużanie ważności legitymacji elektronicznych
  - prowadzenie procesu uzyskania dyplomu
  - drukowanie wszelkich zaświadczeń, kart okresowych osiągnięć

Przykłady metatypów ról w systemie obsługującym tok studiów (2)

- Pomoc Materialna (PM)
  - obsługa systemu pomocy materialnej udzielanej studentom i doktorantom
  - rejestracja podań o pomoc materialną
  - wprowadzanie średnich dochodów, numerów kont bankowych
  - obsługa rankingów do obliczania średniej na potrzeby stypendium za wyniki w nauce
  - wykorzystanie algorytmów do przyznawania stypendiów
  - ewidencja jednorazowych zapomóg
  - przygotowanie decyzji i raportów

Przykłady metatypów ról w systemie obsługującym tok studiów (3)

- Finanse (F)
  - obsługa systemu płatności za usługi edukacyjne
  - proponowanie należności
  - ustalanie sposobu płatności (rozbijanie na raty)
  - rozliczanie wpłat, które nie zostały rozliczone automatycznie lub dokonanie zmiany tego rozliczenia
  - wprowadzanie opłat manipulacyjnych
  - przygotowanie ponagleń do zapłaty

Przykłady metatypów ról w systemie obsługującym tok studiów (4)

- Oferta Dydaktyczna (OD)
  - prowadzenie oferty dydaktycznej jednostki
  - utrzymanie katalogu przedmiotów
  - definiowanie wymagań przedmiotowych do realizacji na programach studiów
  - uruchomienie zajęć i grup w cyklu dydaktycznym
  - określenie prowadzących grup, miejsc i terminów
  - dodanie uczestników zajęć lub
  - zdefiniowanie i przeprowadzenie rejestracji elektronicznych na zajęcia
  - wygenerowanie protokołów zaliczających zajęcia
  - przeprowadzenie elektronicznych badań ankietowych
  - rozliczanie pensum pracowników

10. Szkolenia, dokumentacja

Przeprowadzenie szkoleń

- Szkolenie pracowników jest procesem ciągłym, nie kończy się w momencie pełnego wdrożenia systemu. Wynika to z następujących czynników:
  - system jest rozbudowywany o nowe funkcje lub są modyfikowane istniejące
  - trwa rotacja pracowników
- Przygotowanie infrastruktury szkoleniowej
  - korzystanie z bazy testowej
  - dostęp do dedykowanej pracowni komputerowej
    - zwiększenie efektywności (pozytywna rywalizacja użytkowników)
    - wymiana doświadczeń między użytkownikami
    - zmniejszenie kosztów

Harmonogramy szkoleń

- Ustalenie
  - terminów spotkań i ram czasowych
  - tematyki
  - uczestników (najlepsze efekty w grupach do 20 osób)
- Tematyka szkoleń
  - całościowe (ogólne) funkcjonowanie systemu (początkowy okres wdrożenia)
  - prezentacja szczegółowa poszczególnych modułów systemu (końcowy okres wdrożenia/pełne funkcjonowanie systemu/aktualizacje systemu)
- Szkolenia mogą stać się także okazją do spotkań z osobami odpowiedzialnymi za funkcjonowanie uczelni, np. kwestorem, pracownikami działu nauczania itp.

Dokumentacja i materiały szkoleniowe

- Uczestnikowi szkolenia będzie dużo łatwiej zapamiętać i zrozumieć przekazywane treści, jeśli otrzyma choćby schematyczny spis poruszanych zagadnień
- Przygotowanie zestawu materiałów zawierających większość omawianych kwestii zwiększy koncentrację uczestników i umożliwi jedynie dodawanie własnych uwag zamiast sporządzania notatek
- Umożliwienie korzystania z pełnej (szczegółowej) dokumentacji poruszanych zagadnień np. za pomocą wydzielonego portalu edukacyjnego
- Wbudowanie w system pomocy kontekstowej
- E-podręczniki
- A może kursy w systemie zdalnego nauczania?

Kontakt z użytkownikami

- Wsparcie techniczne nie tylko w początkowej fazie wdrożenia wzmacnia w użytkownikach zaufanie do systemu
- Przykłady możliwych metod komunikowania się z użytkownikami
  - komunikaty systemowe – pojawiające się w określonym miejscu systemu, należy je traktować jako sposób szybkiego przekazania krótkich ogłoszeń
  - strony WWW zawierające odnośniki do dokumentacji oraz inne informacje ważne z punktu widzenia administratorów systemu
  - adresy e-mail, na które użytkownicy będą mogli wysyłać wiadomości do administratorów systemu
  - listy dyskusyjne, które ułatwiają przekazywanie informacji do wszystkich zainteresowanych
  - kontakty telefoniczne – podanie numerów telefonicznych, pod którymi można uzyskać pomoc w zakresie obsługi i działania systemu

11. Integracja systemów uczelnianych

System zintegrowany czy integracja systemów?

- Nieustannie rośnie złożoność rozwiązań w zakresie technologii informatycznych stosowanych w uczelniach
- Zakup jednolitego standardowego systemu zintegrowanego, zaspokajającego wszystkie potrzeby informacyjne, pozostaje ciągle wyłącznie ideą
- Na systemy informatyczne patrzy się więc jak na zestaw dostępnych komponentów, a nie jak na jednolite całościowe rozwiązanie
- Platformy integracyjne mają ułatwić budowę systemu z dostępnych na rynku lub własnych komponentów
- W ramach platformy definiuje się zestawy konektorów do każdego z systemów udostępniające funkcje innym elementom platformy

Cele i metody integracji systemów

- Celem integracji jest łączenie ze sobą różnorodnych aplikacji w celu automatyzacji pewnych zadań
- Integracja może odbywać się na różnych poziomach (aplikacji, procesów, danych)
- Dostawcy oprogramowania oferują profesjonalne platformy i narzędzia integracyjne oraz usługi
- Istnieje wiele darmowych narzędzi i technologii, które umożliwiają samodzielną integrację stosunkowo tanim kosztem

Przykłady

Architektura systemów informatycznych na Uniwersytecie Warszawskim

(to tylko fragment całości)

Przykład 1

- Automatyczna synchronizacja danych między bazą kadrową i bazą toku studiów
  - Skrypty w języku Progress 4GL pobierają dane (osobowe, adresowe, informacje o zatrudnieniach i pełnionych funkcjach) z bazy kadrowej i zapisują do łącza nazwanego.
  - Program w Javie, uruchamiany na serwerze, na którym zostały umieszczone wyniki działania skryptów, dokonuje korekty danych. Wynik działania programu jest umieszczany w jego lokalnych strukturach danych.
  - Program w Javie wywołuje procedury pakietu bazodanowego w języku PL/SQL. Ich zadaniem jest aktualizacja danych w bazie toku studiów.
- Wykonywana w nocy mniej więcej raz na tydzień
- Dlaczego to takie skomplikowane?

Przykład 2

- Automatyczna synchronizacja danych między bazą toku studiów i serwerem pocztowym, serwerem platformy do zdalnego nauczania, repozytorium identyfikatorów i haseł
  - pośrednik pełniący rolę klienta lub serwera XML-RPC odczytuje/zapisuje dane do bazy
  - dostęp do obu baz ograniczony tylko do ściśle określonego interfejsu
  - logowanie zdarzeń
- Wykonywana na bieżąco

Przykład 3

- Automatyczna synchronizacja danych między bazą toku studiów i bazami aplikacji webowych, LDAP, systemu bibliotecznego i wielu innych
  - automatyczny, generyczny migrator synchronizujący ściśle określone dane między bazami (rola pliku konfiguracyjnego i widoków bazodanowych)
  - działa metodą przyrostową (kluczowa rola daty ostatniej modyfikacji)
- Wykonywana cyklicznie, zależnie od potrzeb aplikacji (od 1 do 4 razy dziennie)

Przykład 4 i 5

- Wymiana danych na temat wyników matur między systemem rekrutacyjnym a Krajowym Rejestrem Matur (KReM)
  - Usługi sieciowe (ang. *web-services*)
  - Człowiek i pliki tekstowe
- Wymiana danych między bazą toku studiów a systemem bankowym (analogicznie dla systemu rekrutacyjnego) – usługi płatności masowych
  - Człowiek i pliki tekstowe

Przykład 6

- Wymiana danych dotyczących umów międzynarodowych i mobilności studentów między systemami informatycznymi uczelni europejskich współpracujących w ramach programu Erasmus
  - usługi sieciowe
- Na dzisiaj raczej w sferze marzeń, choć są prowadzone pilotażowe prace przez UW i firmę wytwarzającą oprogramowanie dla konsorcjum uczelni włoskich

12. Monitorowanie, konserwacja, rozwój

Monitorowanie działania systemu

- Pielęgnacja bazy danych
  - dbanie o jakość danych
  - usuwanie danych tymczasowych
  - przeliczanie indeksów
  - zwiększanie rozmiaru przestrzeni tabel
- Testy wydajnościowe, identyfikowanie wąskich gardeł
- Skalowalność i planowanie zmian
- Kłopoty użytkowników z określonymi częściami systemu powinny być sygnałem do uruchomienia szkoleń i/lub wykonania zmian w systemie

Konserwacja systemu

- Warunki umowy serwisowej
- Zarządzanie błędami
- Instalowanie nowych wersji dystrybucyjnych
- Aktualizacja oprogramowania systemowego i bazodanowego

Zmiana wymagań i rozwój systemu

- Dodatkowe raporty, statystyki, dane dla władz uczelni (warto aby uczelniani informatycy znali strukturę danych w bazie)
- Wytwarzanie nowych modułów (to tutaj mogą być ukryte koszty)
- Prace integracyjne

13. Czynniki decydujące o powodzeniu wdrożenia

Wsparcie ze strony władz uczelni

- Czynne i demonstrowane wsparcie ze strony najwyższych władz uczelni
- Kontynuacja polityki przez kolejne kadencje
- Dostosowanie uregulowań prawnych (Regulamin Studiów, rozporządzenia Rektora, Dziekana, Rady Wydziału)
- Zapewnienie budżetu dostosowanego do zaplanowanych zadań
- Wysokie umocowanie kierownika wdrożenia

Powszechna akceptacja

- Zabiegać o powszechną akceptację projektu ze strony osób bezpośrednio zaangażowanych w prace wdrożeniowe
  - określić misję i cele
  - zapewnić odpowiedni program szkoleń
  - **usprawniać i racjonalizować procesy**
  - wprowadzać rozwiązania zwiększające satysfakcję z wykonywanej pracy
  - motywować finansowo
- Nie lekceważyć działań PR-owych, rozmawiać, wyjaśniać, tłumaczyć, wsłuchiwać się w głosy użytkowników (uczelniana administracja, nauczyciele akademiccy, studenci)

Sprawna realizacja projektu

- Sprawny organizacyjnie i zaangażowany kierownik projektu (człowiek z pasją)
- Dobrze dobrany zespół wdrożeniowy
- Prawidłowe przygotowanie przedsięwzięcia
- Egzekwowanie terminowej realizacji kolejnych etapów wdrożenia
- Efektywne wykorzystanie zasobów
- Integracja systemu z innymi systemami na uczelni

Świadomość zagrożeń

- Nawet najlepszy system w początkowej fazie opóźnia a nie przyspiesza pracę, osiągnięcie przez nowy system pełnej funkcjonalności starego systemu może wymagań wielu miesięcy
- Zmiany uregulowań prawnych (suplement do dyplomu, ELS, nowe regulaminy studiów)
- Odejście osób kluczowych w procesie wdrożenia

Warto przeczytać

- Dokumentacja wdrożeniowa USOS
- Wdrożenie Zintegrowanego Informatycznego Systemu Wspomagającego Zarządzanie Uczelnią na Uniwersytecie Śląskim w Katowicach
- Projekt wdrożenia SAP na UMCS w Lublinie
- Projekt SOSNA (System Obsługi Studiów, Nauki i Administracji) na Politechnice Warszawskiej
- Sapiens – zintegrowany system zarządzania uczelnią na Uniwersytecie Jagiellońskim